# Aff Addendum

## \*\*Vaccines\*\*

### 2AC Vaccines Add-On

#### China and Russia use information warfare exploit pandemics and slow foreign response

Bachmann et al 20 – [Sascha-Dominik Dov Bachmann, Doowan Lee, and Andrew Dowse; Sascha-Dominik Dov Bachmann - Canberra Law School; NATO SHAPE; Swedish Defence University (FHS). Doowan Lee - Government of the United States of America - Naval Postgraduate School. Andrew Dowse - Edith Cowan University. “COVID Information Warfare and the Future of Great Power Competition,” The Fletcher Forum of World Affairs Vol.44:2 Summer 2020, 11-16-2020, accessed through SSRN.]

COVID-19 AND GREAT POWER COMPETITION COVID-19 (or coronavirus) has ushered in a new era of heightened competition among major powers. The pandemic’s impact has far exceeded national security and public health. In addition to COVID-19 as a global health emergency, we see increasing weaponization1 of the pandemic by both the Kremlin and the CCP to achieve strategic goals. Unfortunately, our own resilience to oppose such aggressive acts remains under-matched. One of the key components of the CCP’s strategy concerns operations in the information sphere, per the so-called ‘Three Warfares’2 which is discussed later in the article. Below the threshold of armed conflict and taking place in the ‘grey zone’, such information operations manifest as either influence operations and/or ‘strategic preconditioning’3 for any later action, both with and without the use of force.

INFORMATION WARFARE DURING COVID-19 Great Power competition of today is evident in Western relations with both the Kremlin and the CCP. The CCP appears determined to shape the world to a strategic vision where it will safeguard its economic, strategic, and security interests in Asia, the Pacific, Europe, and the Arctic for generations to come.4 Russia—its strategic partner—aims to rebuild Russia as a ‘Great Power’ and player on the international scene with twin foci on Europe and on where opportunities may arise for it to weaken Western influence and interests. It should be noted that both the Kremlin and the CCP are using concepts which we describe as either hybrid warfare and/or grey-zone warfare, examples of which are best provided by contemporary Russian warfare approaches.5 Responding to the use of irregular strategies employed by the CCP and the Kremlin, the U.S. has included the concept of Great Power competition in its national security strategy. Great Power competition entails the distribution of relative gains with no finite terminal objectives. In this context, it is not hard to see how information warfare plays a critical role in shaping how the great powers are competing in key issue areas where major powers use weaponized narratives to sow internal discord and distrust,6 rendering their adversaries unable to focus on external threats. In other words, the information environment has thus become one of the main battle spaces of Great Power competition. The need to approach information warfare from a full-spectrum perspective is more acute than ever. While disinformation mitigation is a critical component of information statecraft, it is only a necessary component, not the sufficient whole. Both revisionist states use digital media platforms and other information warfare capabilities not only to consolidate their authoritarian rule, but also to undermine and disrupt the liberal international order that the United States and its allies have buttressed.7 Drawing on this inspiration, other autocrats are emulating the CCP and the Kremlin to exploit the information environment and undermine the strategic interests of the United States.8 Authoritarian regimes further seem determined to weaponize digital media and information technology from domestic population control mechanisms to foreign policy tools.9 Emulating the Kremlin, the CCP seems poised to weaponize the cyber domain, as well as publicly available information (PAI) as tools of disruption and coercion.10 For example, the CCP has aggressively promoted patently false narratives about the origin of the coronavirus. In addition, it has actively promoted the Party’s public health ‘leadership’ using automated accounts, bots, and trolls, despite numerous frauds and defects noticed in several countries.11 The CCP’s COVID aid to other countries has further been riddled with frauds, to say nothing of its explicit use for propaganda purposes.12 Similarly, the Kremlin is exploiting the pandemic to highlight how the European Union is failing its mandates.13 While this is consistent with the Kremlin’s information operations as we saw in the 2016 election, it has palpably escalated its propaganda efforts during the COVID pandemic by intentionally propping up radical right conversations that promote the dissolution of the EU

Foreign disinformation campaigns decrease vaccination rates. We need to implement the plan now

Wilson and Wiysonge 2020 — [Steven Lloyd Wilson and Charles Wiysonge - politics, Brandeis University, Waltham, Massachusetts, USA and Cochrane South Africa, South African Medical Research Council, Cape Town, South Africa, “Social media and vaccine hesitancy,” BMJ Global Health, 11-17-2020 https://gh.bmj.com/content/5/10/e004206.full, accessed 7-21-2022]

Meaning of the study Foreign disinformation campaigns are robustly associated with declines in mean vaccination rates. The use of social media to organise offline action is highly associated with an increase in public belief in vaccines being unsafe. Both of these findings suggest that combating disinformation and misinformation regarding vaccines online is critical to reversing the growth in vaccine hesitancy around the world. These findings are especially salient in the context of the COVID-19 pandemic, given that the vaccines under development will require deployment globally to billions of people in the next year. Policymakers need to begin planning now for ways to work against the patterns found in this study. While public outreach and education about the importance of vaccines will likely be the cornerstone of any COVID-19 vaccine deployment, we argue that the findings in this paper show that such efforts are empirically not sufficient even if clearly necessary. Based on our findings, we argue for an additional two-pronged strategy explicitly targeting foreign disinformation campaigns and the use of social media by anti-vaccination groups. First, governments must mandate that social media companies are responsible for taking down antivaccination content (whether originating from genuine domestic actors or foreign propaganda operations). This is obviously easier said than done and involves both legal and technical hurdles. However, authoritarian states provide an ironic roadmap despite the chilling implications for free speech: they have consistently been successful at pressing technology companies into policing speech on their behalf within their borders. Where there is political will, there is the capacity for removing content damaging public health. Second, foreign disinformation campaigns should be addressed at their source. A preponderance of such campaigns amplifying anti-vaccination content originate from within Russia or via pseudo-state actors informally associated with Russia. The utilisation of information warfare on the internet is a broad issue that has little hope of general resolution. However, given the global nature of the COVID-19 crisis and the fact that pushing anti-vaccination propaganda will tangibly cause civilian deaths around the world—and in Russia—there is a chance that, with sufficient pressure and incentivisation, diplomacy could produce a ceasefire of sorts with regard to this specific genre of disinformation. We urge policymakers to take the time before a COVID-19 vaccine is available for mass distribution as an opportunity for action against social media factors contributing to vaccine hesitancy.

#### Specifically, misinformation about vaccines cause vaccine hesitancy – studies prove

Garett and Young ’21 — [Renee Garett; 1ElevateU, Irvine, CA, USA. 2Department of Emergency Medicine, University of California, Irvine, CA 92697, USA.3University of California Institute for Prediction Technology, Department of Informatics, University of California, Irvine, CA, USA, Sean D. Young; University of California Institute for Prediction Technology, Department of Family Medicine, University of California, Los Angeles, 10880 Wilshire Blvd., Ste. 1800, Los Angeles, CA, 90024, USA “Online misinformation and vaccine hesitancy,” OUP Academic, 9-16-2021, https://academic.oup.com/tbm/article/11/12/2194/6371221?login=false, accessed 7-10-2022]

Online misinformation on websites can also negatively impact people’s willingness to take vaccines. According to the Pew Research Center, 55% of Americans with access to the internet sought health or medical information online with some reporting that the information they obtained influenced their health behaviors. Unfortunately, content on health websites varies in accuracy and quality with approximately 6% of those examined containing incorrect information [[21](javascript:;)]. Anti-vaccination websites take many forms from activism to natural health sites to general news and blogging sites, with some sites receiving 1.5 million unique visitors per month [[22](javascript:;)]. This is unsurprising since researchers found that 43% of websites propagated during a web search for “vaccination” and “immunization” comprised of anti-vaccination websites [[15](javascript:;)]. Once led to websites, readers may be bombarded with information that questions scientific integrity, use emotive appeals for civil liberties, and concern for the health and welfare of children. Anti-vaccination persuasion centers on creating a community affected by vaccines and vaccine-related practices [[23](javascript:;)]. Main themes used by anti-vaccine champions include safety and effectiveness, alternative medicine, freedom and rights, conspiracy theories, and morality [[14](javascript:;)].

SOCIAL MEDIA

One of the most efficient methods of spreading vaccine misinformation online is through social media. A report by the Centre for Countering Digital Hate (CCDH) found that social media accounts by anti-vaccination proponents gained 7.8 million followers since 2019, with 31 million Facebook users following anti-vaccination accounts and 17 million YouTube users subscribing to similar accounts [[24](javascript:;)]. In examining vaccine chatter on Facebook, researchers found that though anti-vaccination clusters were fewer in numbers than pro-vaccination clusters, they nevertheless had very high presence and were well entangled with undecided clusters [[25](javascript:;)]. One study found that public use of social media to organize action was associated with the belief that vaccines were unsafe and that foreign disinformation campaigns on social media were associated with lower vaccination rates and negative discourse/posts on social media [[26](javascript:;)]. Another study examined coverage of the human papilloma virus (HPV) vaccine in social media and state-level HPV vaccine coverage. Results showed that exposure to information on social media explained a higher proportion of the variance in vaccine coverage compared to socioeconomic factors, and that vaccine coverage was lower in states with higher exposure to misinformation, conspiracy theories, and safety concerns [[27](javascript:;)].

COVID-19 VACCINE-RELATED MISINFORMATION

During the current COVID-19 pandemic, it is especially important to be aware of the prevalence and role that online misinformation is having on people’s attitudes and behaviors as this affects willingness to get the COVID-19 vaccine. News of the availability and near dissemination of the recently developed and tested vaccines began to circulate in headlines and social media posts. Subsequently, misinformation and conspiracies about the COVID-19 vaccine gained traction [[28](javascript:;), [29](javascript:;)]. Investigators who examined media consumption and reliance on specific institutions regarding COVID-19 found that reliance on certain news formats and sources was associated with knowledge, misinformation, and prejudice [[30](javascript:;)]. The amount of misinformation online surrounding the vaccine has been labeled as a second pandemic and has fueled the mistrust surrounding the handling of the pandemic, which can undermine efforts to vaccinate [[31](javascript:;)]. Surveys of adults about getting the COVID-19 vaccine showed reluctance in doing so. The report by CCDH noted that one in six British would get vaccinated for COVID-19 [[24](javascript:;)] and an even higher number of Americans, four in ten, stated they definitely or probably would not get the COVID-19 vaccine [[32](javascript:;)]. In a randomized control study, participants who were exposed to snippets of social media posts containing COVID-19 misinformation had a decrease in intent to obtain the vaccine compared to controls who were exposed to factual COVID-19 information [[33](javascript:;)].

#### Vaccines are also crucial to stopping future pandemics—but reassuring the public about their safety is crucial:

Julie L. Gerberding, M.D., M.P.H., and Barton F. Haynes, M.D., 2/4/2021 (New England Journal of Medicine, “Vaccine Innovations — Past and Future,” <https://www.nejm.org/doi/full/10.1056/nejmp2029466>, Retrieved 8/2/2021)

Vaccination is a powerful method of disease prevention that is relevant to people of all ages and in all countries, as the Covid-19 pandemic illustrates. Vaccination can improve people’s chances of survival, protect communities from new and reemerging health threats, and enhance societal productivity. But achieving the promise of vaccination requires much more than the vaccines themselves. It requires appropriate incentives to encourage the timely discovery and development of innovative, effective, safe, and affordable products; effective financing and delivery programs; and credible scientific leaders who can provide evidence-based policy recommendations and reassure the public about the value of the vaccines. Since its inception 50 years ago, the National Academy of Medicine (NAM), previously known as the Institute of Medicine (IOM), has been an authoritative resource on medical issues, including vaccination, and a global leader in vaccine-policy development. FDA Licensure Dates for Selected Innovative Vaccines since 1970. It’s hard to overstate the benefits that innovative vaccines deployed in the past five decades have had on morbidity and mortality (see timeline).1 The incidence of vaccine-preventable diseases among U.S. children has decreased dramatically, an achievement that is attributable in part to high vaccine-coverage rates. By the 2018–2019 school year, coverage rates among kindergarteners exceeded 90% in all but two states, according to data from the Centers for Disease Control and Prevention (CDC). Four vaccine-preventable illnesses have been eliminated from the Americas: smallpox in 1971, poliomyelitis in 1994, and rubella and congenital rubella syndrome in 2015 (one of us is an executive vice president at Merck, which produces vaccines for rubella, among other vaccines). Moreover, between 2011 and 2020, immunization programs in low-income countries saved an estimated 23.3 million lives.2 Perhaps the most notable immunization-related accomplishment during the past half century was the eradication of smallpox, which was verified by the World Health Organization (WHO) in 1980. In addition, global cases of paralytic polio have decreased by 99.95% from the estimated 350,000 cases in 1988,3 when the global polio-eradication program was announced, and two of the three wild-type polioviruses, WPV types 2 and 3, have been eradicated. Other important achievements during this period include the 1986 approval of the first vaccine based on recombinant technology, a hepatitis B vaccine that not only has reduced rates of the infection in many countries but was also the first vaccine to reduce cancer risk. In 1987, the first polysaccharide-protein conjugate vaccine was licensed; since then, the incidence of invasive Haemophilus influenzae type b disease among children has fallen dramatically. In 2009, a vaccine for Neisseria meningitidis group A became the first licensed vaccine specifically designed for certain people in low-income countries. Achieving broad population health benefits associated with vaccination requires effective policies that create incentives for vaccine development, ensure financing of vaccines, and improve access. After a measles outbreak in 1989–1991, the U.S. Vaccines for Children Program was authorized in 1993 to ensure that eligible children would have free access to all CDC-recommended vaccines. To address remaining gaps, the IOM in 2000 issued a landmark report that recommended policy and programmatic improvements to strengthen U.S. immunization programs. One outcome of this effort was the requirement included in the 2010 Affordable Care Act that plans provide first-dollar coverage (coverage without copayments or other cost sharing) for vaccines recommended by the CDC’s Advisory Committee on Immunization Practices for children and adults up to age 26. Policy advances have also enhanced the effects of vaccination globally. The WHO launched the Expanded Program on Immunization in 1974 to increase access to vaccines. Beginning in 2000, the benefits of this program were greatly enhanced by the creation of Gavi, the Vaccine Alliance, an international public–private partnership that provides financial and programmatic support to ensure that children in the poorest countries have access to vaccines. In 2017, with the support of the NAM and other organizations, this model was used as a framework for the creation of the Coalition for Epidemic Preparedness Innovations to fund innovative vaccines and other countermeasures against pathogens that cause devastating public health consequences, such as the Ebola virus and now SARS-CoV-2. Because vaccines are usually administered to healthy people, maintaining the highest safety standards isn’t only an ethical imperative but is also essential to sustaining public trust. The story of vaccine progress has been punctuated by both real and misguided safety concerns for as long as vaccines have been in use. Such concerns have included adverse events associated with vaccination itself, quality lapses in the manufacturing process, and false alarms regarding vaccine safety. The potential for financial gain has fueled liability suits related to putative safety concerns. The NAM has conducted ongoing objective assessments of vaccine safety to help address concerns. Between 2000 and 2004, its Immunization Safety Review Committee evaluated evidence pertinent to various vaccine-safety topics and set a new standard for independent scientific review that remains relevant as the NAM contributes to coronavirus-related policies. Vaccine confidence depends on trust in the safety and efficacy of the products themselves, trust in vaccine manufacturers and the clinicians who administer vaccines, and trust in policymakers who assess the scientific evidence and promulgate vaccination recommendations. Failures in any of these areas can have substantial long-term public health consequences, as was the case with misinformation about measles vaccines. Enduring mistrust stemming from a discredited study that associated childhood vaccination with autism has been linked to recent outbreaks of measles in the United States. Sustaining both vaccine safety and trust in vaccination will become increasingly complex. Vaccines continue to be approved, and more vaccines have become accessible in resource-limited countries, but safety surveillance systems are less evolved in many low-income regions than in high-income regions. Similarly, vaccines are being manufactured in regions where regulatory oversight isn’t always optimal, and counterfeit vaccines remain a threat. Emerging infections may require rapid availability of new vaccines before comprehensive safety studies are complete. Perhaps most important, the speed and reach of communication on social media platforms have created unprecedented opportunities for users to amplify misinformation and flame the fears of parents and other stakeholders in the immunization ecosystem. Moving forward, vaccines against a range of infectious agents will need to be developed. New and reemerging pathogens, such as SARS-CoV-2 and new influenza strains, regularly appear. Viruses that are capable of spreading by vector or airborne routes — one of the most important pandemic threats — continue to emerge. More than 1.5 million as yet unknown viruses are estimated to exist in animals worldwide, and 38 to 50% of them are candidates to spread to humans.4 Global-surveillance and virus-discovery programs are therefore important, and they may be able to predict pandemics. In 2011, the IOM commissioned the development of a strategic multiattribute ranking tool for vaccines to facilitate evaluation of new vaccine targets and help guide decisions about prioritizing vaccine-development efforts. When pandemics emerge, rapid responses are necessary. Vaccines aren’t the only available tool: passive administration of antibodies for prevention or treatment of infectious diseases has been used for many years. The Pandemic Prevention Platform program of the Defense Advanced Research Projects Agency aims to develop a new form of passive antibody protection that can slow viral epidemics starting within 60 days after identification of the pathogen and until a vaccine can be made. Thanks to new technology, the vaccine-development process is also being condensed. Experimental vaccines were developed and ready for phase 1 clinical trials in 20 months for SARS after the epidemic began in 2003 and in slightly more than 3 months for Zika virus in 2016. The response to the Covid-19 pandemic is a prime example of how rapidly new vaccines can now be designed. By the time the WHO declared Covid-19 a pandemic on March 11, 2020, at least 37 groups from biotechnology companies and academic institutions were working on vaccine candidates.5 These candidates include live attenuated, inactivated, DNA, messenger RNA, viral vector, and spike-protein–based vaccines. Less than 1 year later, the first Covid-19 vaccine-efficacy trials have now been completed, and the first vaccines are authorized for emergency use. Many approved vaccines, such as those against measles and polio, were made using attenuated or killed versions of the virus without detailed knowledge of viral pathogenesis. In contrast, current strategies for vaccine design rely on new technologies that lead to a deeper understanding of the immune system and of host–pathogen interactions. For new experimental HIV and respiratory syncytial virus (RSV) vaccines, a detailed structural understanding of antibody interactions with the HIV envelope or the RSV prefusion form of the fusion (F) protein is needed. Vaccines remain the most effective tool for preventing infectious diseases and improving global health. Remarkable progress has been made with the use of vaccines, including the eradication of smallpox and the control of childhood diseases such as measles, mumps, rubella, and polio. New insights into the functioning of the immune system on a cellular and molecular level have made possible the rapid development of new vaccines. Difficulties facing vaccinologists include predicting the type and timing of the next pandemic; developing vaccines to combat rapidly changing pathogens such as HIV-1, influenza, and multidrug-resistant bacteria; and establishing rapid-response strategies to control emerging and reemerging infectious diseases. The future holds great promise for vaccine-mediated control of global pathogens, but providing affordable access to effective vaccines for everyone who could benefit from them remains an important challenge.

#### Future pandemics cause extinction

Eleftherios P. **Diamandis 21** (works for the Department of Pathology and Laboratory Medicine, Mount Sinai Hospital, Toronto, Canada; Lunenfeld-Tanenbaum Research Institute, Mount Sinai Hospital, Toronto, Canada; Department of Laboratory Medicine and Pathobiology, University of Toronto, Toronto, Canada. “The Mother of All Battles: Viruses vs. Humans. Can Humans Avoid Extinction in 50-100 Years? 4/13/21 https://www.preprints.org/manuscript/202104.0397/v1)//conway

The recent SARS-CoV-2 pandemic, which is causing COVID 19 disease, has taught us unexpected lessons about the dangers of human extinction through highly contagious and lethal diseases. As the COVID 19 pandemic is now being controlled by various isolation measures, therapeutics and vaccines, it became clear that our current lifestyle and societal functions may not be sustainable in the long term. We now have to start thinking and planning on how to face the next dangerous pandemic, not just overcoming the one that is upon us now. Is there any evidence that even worse pandemics could strike us in the near future and threaten the existence of the human race? The answer is unequivocally yes. It is not necessary to get infected by viruses of bats, pangolins and other exotic animals that live in remote forests in order to be in danger. Creditable scientific evidence indicates that the human gut microbiota harbor billions of viruses which are capable of affecting the function of vital human organs such as the immune system, lung, brain, liver, kidney, heart etc. It is possible that the development of pathogenic variants in the gut can lead to contagious viruses which can cause pandemics, leading to destruction of vital organs, causing death or various debilitating diseases such as blindness, respiratory, liver, heart and kidney failures. These diseases could result n the complete shutdown of our civilization and probably the extinction of human race. In this essay, I will first provide a few independent pieces of scientific facts and then combine this information to come up with some (but certainly not all) hypothetical scenarios that could cause human race misery, even extinction. I hope that these scary scenarios will trigger preventative measures that could reverse or delay the projected adverse outcomes.

### Vaccine Extensions

#### Misinformation affects underserved communities the most

**Scheufele and Krause 18** — [Dietram A. Scheufele; Department of Life Sciences Communication, College of Agricultural and Life Sciences, University of Wisconsin–Madison, Madison, WI 53706., Nicole M. Krause; Department of Life Sciences Communication, College of Agricultural and Life Sciences, University of Wisconsin–Madison, Madison, WI 53706 “Science audiences, misinformation, and fake news,” PNAS, 11-9-2018, https://www.pnas.org/doi/full/10.1073/pnas.1805871115, accessed 7-11-2022, Rachel]

A last area with a dearth of systematic empirical work are mechanisms to reach audiences that are often underserved by traditional channels for science communication. Newspapers, science television, or even science museums, for instance, tend to reach more educated and higher-income audiences ([11](https://www.pnas.org/doi/full/10.1073/pnas.1805871115#core-r11)). Furthermore, from work dating back to the 1970s on widening knowledge gaps, we also know that citizens with higher socioeconomic status (levels of education and income) are able to learn more efficiently from new information than their peers. As a result, quality scientific information is not only more likely to reach more educated and higher-income audiences, but, when it does, the ability of citizens with higher socioeconomic status to process new information more efficiently can further widen existing gaps between the already information-rich and the information-poor.

Our inability to reach all segments of the population equally well with high-quality scientific information is particularly troubling, given that the need for antidotes to misinformation might be particularly pronounced among certain groups of the public. One indicator of this problem is the educational and income gaps related to seeing fake news as a problem in the first place. In a 2016 Pew survey after the US presidential election ([28](https://www.pnas.org/doi/full/10.1073/pnas.1805871115#core-r28)), almost three in four Americans (73%) with a household income over $75,000 thought that completely made-up news caused “a great deal” of confusion. Comparatively, fewer than three in five (58%) respondents with a household income of $30,000 shared that concern. However, socioeconomic gaps also emerge with respect to people’s confidence in their own ability to spot fake news in the first place. A 2018 US survey commissioned by *The Economist* asked respondents about their ability to distinguish real and fake news ([96](https://www.pnas.org/doi/full/10.1073/pnas.1805871115#core-r96)); 83% of respondents with a family income of at least $100,000 felt “very confident” or “somewhat confident” that they could “tell real news from fake news.” Among respondents with an income of less than $50,000, that number dropped to 63%.

#### misinformation abt vaccines high now - covid proves

**Terry-21** (Ken Terry is an expertise in health care and health IT, an award winning journalist, webmd, 11/10/2021 Most Americans Have Been Duped by COVID Misinformation: Survey, <https://www.webmd.com/lung/news/20211110/americans-duped-by-covid-misinformation>)

Nearly 8 in 10 U.S. S adults either believe or aren't sure about at least one of eight false statements about the COVID-19 pandemic or the COVID-19 vaccines, according to a new Kaiser Family Foundation (KFF) survey. Unvaccinated adults and Republicans are among those most likely to hold these misconceptions, the nationally representative poll shows. Overall, 78% believed at least one piece of misinformation. Nearly two-thirds of unvaccinated adults (64%) believe or are unsure about at least half of the eight false statements, compared with 19% of vaccinated adults. Forty-six percent of Republicans believe or are unsure about at least half of the statements, 3 times the share of Democrats in that category (14%). Independent voters were not factored into the survey results.

The topline results show: Sixty percent of adults say they've heard that the government is exaggerating the number of COVID-19 deaths by counting deaths due to other factors and either believe it to be true (38%) or aren't sure if it's true (22%). Four in 10 (39%) respondents say they've heard that pregnant women should not get the COVID-19 vaccine and believe it to be true (17%) or aren't sure if it's true (22%). Three in 10 (31%) say they've heard that the vaccine has been shown to cause infertility and either believe it (8%) or aren't sure if it's true (23%). Thirty-five percent of respondents say they've heard that the government is hiding deaths from the COVID-19 vaccine; 18% believe it, and 17% say they're not sure if it's tru. Other statements attract less but substantial support: Twenty-eight percent of respondents have heard that the antiparasitic drug ivermectin is a safe and effective treatment for COVID; 14% believe it, 14% are not sure if it's true. Twenty-four percent of Americans have heard that you can get COVID from the vaccine; 14% believe that to be true, while 10% are unsure. Twenty-four percent of respondents have heard that the vaccines contain microchips; 7% believe it, 17% say they've heard that but don't know if it's true. Twenty-one percent of Americans have heard claims that the vaccine can change DNA or don't know if it's true. Misinformation by News Source. The report notes that "people's trusted news sources are correlated with their belief in COVID-19 misinformation." At least a third of those who trust information from CNN, MSNBC, NPR, and local and network TV news do not believe any of the eight false statements. Depending on their mix of these news sources, only 11%-16% of this group believe or are unsure about at least four of the eight false statements. In contrast, 36% of people who trust Fox News, 37% of those who trust One America News, and 46% of those who trust Newsmax say they believe or are unsure about at least half of the eight false statements. It's also notable that 44% of people who trust NPR, 48% of those who trust MSNBC, 50% of those who trust network news, and 49% of those who trust CNN believe or are unsure about one to three of the false statements. While larger shares of people who trust COVID information from conservative news sources believe misinformation, according to the Kaiser Family Foundation, the researchers say the survey cannot explain those beliefs. "Whether this is because people are exposed to misinformation from those news sources, or whether the types of people who choose those news sources are the same ones who are pre-disposed to believe certain types of misinformation for other reasons, is beyond the scope of the analysis," they write. The poll results show the role partisanship plays in which networks are trusted. Democrats trust COVID-19 information from network (72%) and local (66%) television, CNN (65%), MSNBC (56%), and NPR (51%). Republicans' most trusted news sources for COVID-19 information are Fox News (49%), local (34%) and network (25%) news, and Newsmax (22%). Few adults say they trust social-media sources for COVID-19 information, such as YouTube (13%), Facebook (9%), Twitter (6%), and Instagram (5%). However, the researchers write that the groups influenced by information they see on those platforms may be larger than these percentages indicate, as previous KFF surveys have found that nearly as many adults get information about COVID-19 vaccines from social media as from cable, network, and local TV news. Partisan COVID Mortality Gap. Wherever people get their news, misinformation that determines their attitudes about COVID-19 and the vaccines has likely had real-world consequences. According to a recent article in The New York Times, a gap between the higher COVID death tolls in more Republican areas and lower death tolls in more Democratic areas of the country has developed in 2021 — with an association emerging between attitudes toward the COVID vaccines and the resulting willingness to be vaccinated between those regions. In October, the Times reports, 25 out of every 100,000 residents of counties that voted heavily for Donald Trump in the last presidential election died from COVID. That's 3 times higher than the mortality rate in counties that strongly supported Joe Biden (7.8 per 100,000).

#### Herd immunity key to keep disease in control

**Randolph and Barreiro ‘20** — [Haley E. Randolph, Genetics, Genomics, and Systems Biology, University of Chicago, Chicago, IL, USA; Luis B. Barreiro; Genetics, Genomics, and Systems Biology, University of Chicago, Chicago, IL, USA Department of Medicine, Section of Genetic Medicine, University of Chicago, Chicago, IL 60637, USA Committee on Immunology, University of Chicago, Chicago, IL 60637, USA; “Herd Immunity: Understanding COVID-19,” Immunity; Volume 52, Issue 5, 5-19-2020, https://www.sciencedirect.com/science/article/pii/S1074761320301709, accessed 7-10-2022, Rachel]

[Acquired immunity](https://www.sciencedirect.com/topics/immunology-and-microbiology/adaptive-immune-system) is established at the level of the individual, either through natural infection with a pathogen or through immunization with a vaccine. Herd immunity ([Box 1](https://www.sciencedirect.com/science/article/pii/S1074761320301709" \l "tbox1)) stems from the effects of individual immunity scaled to the level of the population. It refers to the indirect protection from infection conferred to susceptible individuals when a sufficiently large proportion of immune individuals exist in a population. This population-level effect is often considered in the context of vaccination programs, which aim to establish herd immunity so that those who cannot be vaccinated, including the very young and immunocompromised, are still protected against disease. Depending on the prevalence of existing immunity to a pathogen in a population, the introduction of an infected individual will lead to different outcomes ([Figure 1](https://www.sciencedirect.com/science/article/pii/S1074761320301709" \l "fig1)). In a completely naive population, a pathogen will propagate through susceptible hosts in an unchecked manner following effective exposure of susceptible hosts to infected individuals. However, if a fraction of the population has immunity to that same pathogen, the likelihood of an effective contact between infected and susceptible hosts is reduced, since many hosts are immune and, therefore, cannot transmit the pathogen. If the fraction of susceptible individuals in a population is too few, then the pathogen cannot successfully spread, and its prevalence will decline. The point at which the proportion of susceptible individuals falls below the threshold needed for transmission is known as the herd immunity threshold ([Anderson and May, 1985](https://www.sciencedirect.com/science/article/pii/S1074761320301709" \l "bib1)). Above this level of immunity, herd immunity begins to take effect, and susceptible individuals benefit from indirect protection from infection ([Figure 1](https://www.sciencedirect.com/science/article/pii/S1074761320301709#fig1)B).

#### Widespread diseases like a covid variant will be devastating

**Mooney 21**— [Tom Mooney; Senior Communications & Advocacy Manager, CEPI, “Preparing for the next “Disease X” – CEPI,” CEPI, 2-1-2021, https://cepi.net/news\_cepi/preparing-for-the-next-disease-x/, accessed 7-11-2022, Rachel]

We also know that beta coronaviruses that cause SARS and MERS are associated with case fatality rates of 10-35% (25-88 times worse than COVID-19) and that coronaviruses circulate widely in animal reservoirs. The emergence of a coronavirus variant combining the transmissibility of COVID-19 with the lethality of SARS or MERS would be utterly devastating. We must minimise this threat as a matter of urgency. One way to do this in the long-term would be to develop a vaccine that provides broad protection against coronaviruses in general.

#### A new pandemic will cause severe economic failure

IMF, 20 — [IMF The International Monetary Fund (IMF) is an international organization that promotes global economic growth and financial stability, encourages international trade, and reduces poverty, “World Economic Outlook Update, June 2020: A Crisis Like No Other, An Uncertain Recovery,” 6-24-2020 https://www.imf.org/en/Publications/WEO/Issues/2020/06/24/WEOUpdateJune2020, accessed 7-11-2022, Rachel]

Downside risks, however, remain significant. Outbreaks could recur in places that appear to have gone past peak infection, requiring the reimposition of at least some containment measures. A more prolonged decline in activity could lead to further scarring, including from wider firm closures, as surviving firms hesitate to hire jobseekers after extended unemployment spells, and as unemployed workers leave the labor force entirely. Financial conditions may again tighten as in January–March, exposing vulnerabilities among borrowers. This could tip some economies into debt crises and slow activity further. More generally, cross-border spillovers from weaker external demand and tighter financial conditions could further magnify the impact of country- or region-specific shocks on global growth. Moreover, the sizable policy response following the initial sudden stop in activity may end up being prematurely withdrawn or improperly targeted due to design and implementation challenges, leading to misallocation and the dissolution of productive economic relationships. Some of these aspects are featured in the Scenario Box, which presents growth projections under alternative scenarios. Beyond pandemic-related downside risks, escalating tensions between the United States and China on multiple fronts, frayed relationships among the Organization of the Petroleum Exporting Countries (OPEC)+ coalition of oil producers, and widespread social unrest pose additional challenges to the global economy. Moreover, against a backdrop of low inflation and high debt (particularly in advanced economies), protracted weak aggregate demand could lead to further disinflation and debt service difficulties that, in turn, weigh further on activity.

### NATO key

#### NATO key to countering disinformation---multiple warrants

Tomasz Chłoń, 5/16; Chłoń was the ambassador of Poland to Estonia (2005-2010) and to Slovakia (2013-2015), and the director of NATO Information Office Moscow (2017-2020); “NATO and Countering Disinformation The Need for a More Proactive Approach from the Member States”, GLOBSEC, 16-05-2022, [https://www.globsec.org/wp-content/uploads/2022/05/NATO-and-Countering-Disinformation-ver1-spreads.pdf /](https://www.globsec.org/wp-content/uploads/2022/05/NATO-and-Countering-Disinformation-ver1-spreads.pdf%20/) chuo

===[last part also talks about cohesion key!] Russian disinfo is high now b/c of the war & false narratives they’ve spread in the past, so it’s up to NATO’s cohesion (and coordinating capabilities), credibility, expertise, guidance, financial support, mandates, and the ability for them to create a global snowball to organizations and nations to counter it.

One of the founding myths of Russian foreign policy (developed below) relates to a betrayal by the West. Many in Russia are either unwilling or too scared to challenge the veracity of this tale since it has become national dogma. As the freedom of speech constitutes one of the fundamental and respected rights of democracies, this myth is also widely spread throughout the West. Moreover, the West’s culture of open debates, which respects differing points of view, puts Russian masterminds of false narratives in a privileged position when it comes to influencing Western societies and their decision-making processes. **It also renders NATO and EU countries increasingly vulnerable to influence from pro-Kremlin propagandists spurred on by an unbridled sense of initiative and combined with active measures as well as armed conflicts.** The matrix of the myth of Western betrayal and Russian self-victimisation is the “broken promise of not enlarging NATO to the East”. The Kremlin has also used this myth to justify the full-scale invasion of Ukraine on 24 February 2022 – a move that has potentially incalculable consequences for European and even global security. This new stage in Russia’s confrontational policy has been further solidified with support from the increasingly belligerent Belarusian dictator although Alyaksandr Lukashenka’s standing has also been weakened through his complete dependence on Russia. Minsk, assisted in turn by Moscow, created a migration crisis on the Belarusian border with Poland, Lithuania and, to a lesser extent, Latvia, thereby opening an additional hybrid front. **Increased tension on NATO’s entire eastern flank and the war waged by Russia against Ukraine have been exacerbated by Russian and Belarusian hostile disinformation activities, which are unprecedented in terms of scope, intensity and toxicity.** In both Russia and Belarus, the highest political authorities, diplomats, state-controlled media, special services and their proxies have been **actively involved in spreading familiar but intensified false narratives as well as new concoctions that are particularly harmful to the public** in the Russian-language, state-controlled information environment. **Unfortunately, some of these narratives fall on fertile ground in certain circles in the West and are cynically exploited in local political struggles.** The goal of disinformation is to **undo the cohesion of the transatlantic community, undermine the credibility of NATO and EU members and, ultimately, derail the existing rules-based international order.** **The “new-old” story is that: Russia, and now Belarus, are surrounded by foes, and the heightened security crisis is the fault of the West, which had been allegedly pushing Ukraine towards war.** Having rejected the Minsk agreements, Ukraine had been preparing to launch military operations against the inhabitants of Donbas, occupied Crimea and regions in Russia itself; to this end, Kyiv had been concentrating its forces and resources (including weapon systems received from NATO countries) in the east of the country. Polish and American mercenaries were also operating and preparing armed provocations in the east of Ukraine; this means that not only Ukraine but also the West itself had been preparing to attack the Russian Federation and Belarus. Ukraine had been mobilising troops on the border with Belarus, against which Poland has been making territorial claims. Finally, Vladimir Putin justified his illegal assault on Ukraine with the need to demilitarise and denazify Ukraine. He did so despite the fact that the Ukrainian nation lost 8 million people in World War II fighting Nazi Germany and is a country led by a Jewish president who won the popular vote in a free, fair and democratic election; an election which showed the Ukrainian neo-Nazi parties having less support than probably anywhere else in Europe.

Although it is not easy to measure, the pernicious nature of Russian disinformation and interference abroad has been “tested” positively in several cases, with prime examples including the attacks against Ukraine, the U.S. and French presidential elections, as well as the Brexit referendum. The extent to which social polarisation and internal political fights are causal effects of Russian (and others) meddling in the West could be discussed elsewhere, but what is of importance for this paper is that such **frictions are certainly being exploited and amplified by the opportunistic organisers of external disinformation.** In any case, the cumulative result can be seen, for example, in Slovakia where a significant part of the society blames the Alliance for the current Russian crisis (at least that had been the case before the full-scale war against Ukraine started) or in Croatia where the president has been questioning the Alliance’s Eastern policy. The actions of candidates for the highest political positions in France who propagate anti-NATO slogans are even more concerning. Sympathy for the Russian regime is shown by representatives of ruling or co-ruling parties in NATO and EU member states, including Fidesz in Hungary and Podemos in Spain (which should be particularly sensitive to disinformation following the Kremlin’s interference in the Catalan independence question). Moscow uses other tools to exert its influence in Western countries, but their effect may be more prevalent in countries with elected parties that have pro-Kremlin inclinations (e.g., AfD in Germany). Russia has been known to drive political corruption, use blackmail tactics and even resort to acts of terrorism. The growing popularity of conspiratorial and pro-Kremlin narratives in Germany, France and Spain that are spread through encrypted social channels linked to Moscow have become a fact of everyday life. While it is challenging to fully assess how effective countermeasures to tackle foreign interference have been, examples from countries that have taken them up with determination show that the fight against foreign meddling can have a genuine impact. Most ways and means of counteracting disinformation in this political warfare fall under the responsibility of sovereign states (and the European Union due to its legislative prerogatives). It is predominantly their responsibility to build resistance to disinformation and to respond to it with both deterrence and punishment. NATO’s role in this regard is limited. At the same time, the Alliance – as an organisation at the centre of false accusations and hostile propaganda – knows how to defend itself, which is evidenced by the overall high level of public support for NATO among its members. Nevertheless, it seems that the **Alliance’s potential to combat disinformation is not fully utilised by its individual members, which could benefit from NATO’s expertise and coordinating capabilities to a greater extent than they have thus far.**

Tackling disinformation remains an essential part of NATO’s communication strategies and day-to-day operations, which includes media monitoring, analysis of the information space and proactive communication in a coordinated and fact-based manner. **Its goal is to inoculate or “pre-bunk” the mediasphere rather than debunk each false claim, i.a. through “Setting the Record Straight” narratives and activities which counter the Kremlin’s myths about NATO.** In 2019, NATO adopted an updated and systematic package of appropriate objectives and measures to combat disinformation. The following year, NATO’s Response to Disinformation on COVID-19 became realised in an Action Plan issued to Allies by the Secretary General. This document sought to bring together multiple strands of work on countering hostile disinformation surrounding COVID-19. In 2021, NATO’s Toolbox for Countering Hostile Information Activities was created; it reflects the Alliance’s twin-track model to respond to hostile information activities: “understand” and “engage”, underpinned by “coordination”. The document aims to provide Allies with a toolbox to assess hostile information activities, including disinformation, and to assist in determining possible courses of action. Furthermore, NATO IS staff holds biweekly briefings on Russian and other disinformation activities at various relevant committees. Within the Civil Emergency Planning Committee, as part of a long-term effort, and covering resilience baselines – spanning across many domains including communications – Allies share information about how prepared they are to face various key civil security challenges, including disinformation. **The organisation supports member and partner states by providing guidance as well as co-financing for social and scientific projects that strengthen their resilience to disinformation.** Rapid-reaction teams have been made available to member states as part of NATO’s strategy to fight hybrid threats. The organisation is also cooperating more closely with the European Union to ensure that NATO benefits from the EU’s Rapid Alert System set up to counter disinformation.

At the same time, the West has yet to prepare a coherent, comprehensive and coordinated response to Russian disinformation. It is up to nations to fully utilise NATO’s potential. A response practice has been developed and seen partial success within some states and Euro-Atlantic institutions, but it has not yet been translated into a real common policy or strategy. At national levels, political declarations and agreed action plans are still not fully implemented in too many instances. Western states approach disinformation in varied ways due to differences in history, regional security, wealth, education, media quality, political and legal culture and – most importantly – the current state of their relations with Russia. As a rule, some states prefer bilateral approaches that safeguard national prerogatives. This may change now following the Russian invasion of Ukraine. Nevertheless, the challenge of disinformation has begun to attract higher political attention. In the European Union, this has transpired through the adoption of the European Democracy Action Plan and the presentation of new regulations on digital services in December 2020. These regulations aim to address the core issue of the business model developed by disinformation organisers who instrumentalise social media platforms. The report by the Special Committee on Foreign Interference in all Democratic Processes in the EU, including Disinformation (INGE), has also promised that other means of influence will be addressed5 . In an effort to combat disinformation, the Digital Services Act (DSA) is a breakthrough legal instrument that will fundamentally change the rules of the game for the information environment in the European Union, member states and partner countries; it will also have an impact on national approaches worldwide. The DSA will impose numerous legal obligations on operators of online platforms that are more demanding than the previous voluntary commitments outlined in the Code of Practice for Fighting Disinformation. Companies will be obliged to cooperate with independent researchers and allow them to access their data. They will also participate in complaint and appeal procedures regarding content moderation and dispute resolution. The DSA will provide for the companies’ obligatory consultations, including with civil society organisations. It will also introduce the institution of trusted whistle blowers, who, among other things, will notify the companies about suspected crimes online. The act will correspondingly establish a European Digital Services Council and advisory body made up of national digital service coordinators responsible for implementing legislation at the national level. It will impose specific additional duties on exceptionally large online platforms with more than fortyfive million users per month. These obligations will include assessing systemic risks resulting from their services, identifying actions to reduce such risks, conducting independent audits, setting appropriate conditions for algorithmic recommendations of user content and ensuring additional transparency in advertising (including political ads). Among international organisations and institutions, the European Union plays a leading role in counteracting disinformation and introducing new effective measures against it. The future regulations on transparency in financing political parties and election campaigns gives hope for limiting corruption and external influence in the affairs of the member states. NATO and the EU share similar membership compositions and were created based on comparable value systems, so it is reasonable to assume that counteracting disinformation will be more prominently reflected in NATO’s new Strategic Concept. A need for this has been suggested by the authors of the NATO2030 expert group report prepared ahead of the Madrid Summit in June 2022. As a result, **countering disinformation could be given a more visible place on the agenda of NATO ministerial meetings and summits, and more proposals with clear commitments by member states to tackle disinformation may be unveiled. NATO also has the opportunity to strengthen the mandates of existing committees to better coordinate national efforts.**

In light of the current security environment in Europe and worldwide, traditional threats are still a priority, and collective defence will remain one of NATO’s core missions, even more so than in the 2010 document. Among the tasks supporting this existing mission, there will also be development of a full range of instruments aimed at neutralising new risks, including disinformation. As experience has shown, threats evolve in terms of intensity, goals, methods and means. The challenge for the negotiators of NATO’s new Strategic Concept will therefore be to provide for adequate flexibility when crafting current and future countermeasures that will guide the Alliance’s activities for years to come. Overall, NATO’s (and the West’s) coherent response and efforts against foreign disinformation, both nationally and internationally, should focus on: (i) their civic resilience, (ii) their offensive capabilities as much as their defensive ones and (iii) minimising the differences in how individual Western countries approach disinformation in practice. In other words, deterrence must be pursued through both punishment and denial. The following recommendations apply specifically to NATO but also to other organisations that can cooperate more with the Alliance as well as the member states themselves, for which **NATO can act as a catalyst in the development of national policies and practices.**

Therefore, where appropriate, **Allies should overcome any remaining reluctance and uncooperative tendencies that limit the role of NATO in combating new threats,** especially hybrid ones. First, tackling disinformation should gain greater political attention among all Allies. National countermeasures undertaken in some member states (e.g., France, Germany, the Baltic States and the UK) or partner countries (e.g., Finland and Sweden) testify to the importance they attach to the problem of falsehoods in international politics. When allowed, **NATO could better serve as a coordinator and multiplier of good practices** (of which these countries are, to a significant extent, a model). Second, there is no need to reinvent the wheel. The work ahead can be built on the existing acquis and institutions without substantial additional resources, which is important given budgetary constraints. Third, **there is clearly more scope and possibility for NATO to foster synergies with other organisations** – most notably the EU – in helping each other and partner countries to fight foreign disinformation. Overall, NATO and the West must take a more offensive approach in tackling this ever more dangerous scourge.

#### Increased information guarding with NATO’s resources is the linchpin of countering Russian, Chinese, and COVID disinformation

Dale F. Reding and Bryan Wells, 22, Reding and Wells are from the office of the chief scientist, NATO headquarters; “Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies”, Springer, 05-04-2022, https://link.springer.com/content/pdf/10.1007/978-3-030-94825-2\_2.pdf/chuo

===can be used as not just NATO key but also the actions they do---if the warrants & solutions the card mentions aligns w/ the aff then this card can be used

===definitely not the best card (unless the strat specifically focuses on the cognitive warfare side of things) but talks about NATO’s strategy in the past and how NATO can work on this w/ disinformation increasing moving forwards

As NATO moves towards the future, it finds itself confronting the challenges of a changing world. As noted in the NATO2030 process (Maizière et al., 2020; NATO, 2021a), NATO will need to address a host of returning and emergent challenges such as Russia’s aggressive actions, the threat of terrorism, cyber-attacks, emerging and disruptive technologies, the security impact of climate change, and the rise of China. **The solutions to these challenges require a delicate blend of political and military action married with the deep collective wisdom contained within the Alliance.** Within the three core missions specified by NATO’s 2010 strategic concept (collective defence, crisis management and cooperative security) (NATO, 2020d), the Alliance is focused on five operational imperatives: cognitive superiority, layered resilience, influence and power projection, cross-domain command, and integrated multi-domain defence (NATO, 2021c). These imperatives and the overarching challenges outlined in NATO2030 have led NATO to expand its operational domains from three (air, land, sea) to include cyber (NATO, 2019) and space (NATO, 2021b). However, a school of thought exists that has strongly advocated that the cognitive domain should be given equal importance and noting that it is an area where Alliance nations are particularly vulnerable (Cole & Le Guyader, 2020). Recent examples of the ever-growing threat presented by disinformation, misinformation, and propaganda, including actions taken during the COVID-19 crisis, would support such an assertion.

NATO’s approach, honed over seventy-two years of information conflict, is based on a traditional approach of **highlighting concrete actions, verifiable facts and credible communication**. This approach relies on clear and consistent narratives passed through conventional mass media, public engagements and social media. Such an approach is based on the Alliance’s ideals and core values. Trust, once broken, is hard to regain, so clarity and consistency are central aspects of this approach. For example (NATO, 2020b), in support of the Alliance and its partners, “NATO and Allied armed forces have played a key role in supporting civilian efforts to fight COVID-19, with some 350 flights delivering hundreds of tons of critical supplies, the construction of almost 100 field hospitals, and almost half a million troops across the Alliance securing borders, transporting patients and helping with testing [and vaccine delivery].” It has also built over twenty-five field hospitals, provided over twenty-five thousand beds to the Allied nations, and supports sharing medical supplies and logistics through the NATO Euro-Atlantic Disaster Response Coordination Centre (EADRCC) (Ozawa, 2020).

Responding to specific attacks, NATO provides **widely available refutations, briefings, talking points, statements, and corrections**. In response to the COVID-19 infodemic, NATO **intensified its communications across a wide range of platforms and media, engaged in an increasing number of online engagements with a broad range of audiences**. Also, it expanded outreach within Russia through various media products. However, **this has not been enough**, and NATO has reached out to academia, industry, NGOs, think tanks, and media watch organisations to encourage discussion. This can reduce the susceptibility to disinformation and support a more resilient society. An engaged, independent, and empowered fourth estate is a necessary part of this resilience. Only by constant engagement with old and new media across the Alliance, partners and where possible, social groups/countries that are the sources can one hope to ensure that disinformation is successfully countered.

The response to disinformation has been coordinate through the Strategic Communication Task Force, led by the NATO Public Diplomacy Division (PPD). An example of NATO’s approach may be found in its straightforward debunking of Russian myths on NATO and COVID-19 (NATO, 2020a). This strategy faces the recurring issues raised in Russian disinformation efforts and attempts to answer the accusations in a forward-leaning fashion.

In the end, NATO has faced the COVID pandemic in two ways (Ozawa, 2020). The first is by leveraging the power of the military Alliance to support a global medical emergency, and the second by addressing the infodemic head-on. The efforts of the S&T community have successfully been brought to bear on both issues.

No single strategy will work all the time, nor will counter-narrative strategies be universally successful, as exemplified by the continuing existence of “flat earth” societies despite irrefutable evidence to the contrary. NATO’s engagement strategy, therefore, relies on proactive and rapid communication, highlighting flawed reasoning (debunking), identifying familiar sources and methods of disinformation, countering disinformation on the platform or via the media on which it is found, adapting to the evolution of such disinformation, being selective in which attacks to counter and consistent in overall messaging. Not all disinformation can be countered, if for no other reason than the sheer volume of such occurrences, so selecting those attacks that can do the most harm or are starting to gain significant attention is a critical step. Earning the trust of Alliance societies through **consistent communication and provision of information will help slow or marginalise the remainder**.

Fourth, NATO needs to better adapt to hybrid, grey zone and cognitive warfare. The battleground of today and the future includes the sixth operational domain, the cognitive or, more generally, the human, domain. Russian and Chinese approaches to disinformation have been successful to some degree, impacting the lives of citizens in the Alliance and with allies. In a manner consistent with the values and ethics that underlie the Alliance, mastering this domain will be essential to maintaining the Alliance’s effectiveness and reducing the risk of strategic errors with potentially disastrous repercussions.

## \*\*Biodiversity\*\*

### 2AC Biodiversity Add-On

#### Disinformation wrecks public confidence in science which undermines solutions to climate change and diseases---plan is key to solve

T. V. Gerbina, 22, Gerbina is from an Institute for Scientific and Technical Information from Russia; “Science Disinformation: On the Problem of Fake News”, Springer, 2-25-2022, <https://link.springer.com/article/10.3103/S0147688221040092/chuo>

This article is devoted to an important socio-cultural phenomenon that undermines public confidence in science, that is, fake science news. The term fake news is analyzed and data on the dissemination of fake news on social networks is provided. Information sources for science news and fake science news are identified. Special attention is paid to the dissemination of fake science news during the COVID-19 pandemic.

According to the Oxford English Dictionary, the 2016 word of the year was post-truth. According to the definition of British linguists, this concept means circumstances in which objective facts have less influence on the formation of public opinion than emotions or personal beliefs [1]. This phenomenon arose due to the influence of the media: by manipulating society, they create a different reality. One of the main reasons for the post-truth era is the abundance of fake news that the audience is unable to recognize.

The growing influence of fake news is fueled by a loss of trust in the authorities, as well as in the media and the journalistic profession in general. **Fake news fills the vacuum for people or communities offering instant solutions to various problems.** In their discourse, knowledge, science, facts, evidence, and rationality are swept aside as the sophistry of the elite. With the development of Internet technologies, anyone can become an author of fake news and begin to **spread it instantly**; any attempt to refute these false facts is useless. **Emotions take over rationalism**, i.e., people believe what they want to believe. **All this fully applies to science news.**

Development of the Internet provides an excellent opportunity to promote scientific knowledge, as well as to educate and disseminate research results. If it is credible, science news can be an influential vehicle for drawing public attention to important issues of our time; otherwise, **such news undermines the credibility of scientific information and science in general**.

The **scientific news problem has been aggravated by the COVID-19 pandemic and the information wave that followed**. Disinformation about the new disease spread faster than the pandemic, resulting in the emergence of the phenomenon of infodemic, i.e., an overabundance of both reliable and inaccurate information, which makes it difficult for people to identify reliable sources. Infodemic has exacerbated the problem of fake science news, since almost any message about COVID-19 relates to science, in particular, to medicine and biology.

In our time, **science is more relevant than ever for society, given such important problems of our time as climate change, the energy supply, and the global spread of viral infections**. Science news is a key resource for helping the public understand new scientific knowledge and the latest technological advances. The media, including social media, mediate relationships between people and technological development and help them to understand the new world by playing the role of a science conduit. According to the reach of the audience, the main channels for the receipt of science news can be divided into sources for professionals (scientists) and sources for society as a whole (Fig. 5). Accordingly, professional sources of information (mostly scientific articles) are the main channels for obtaining information for popular scientific publications and news agencies. It is difficult to judge the quality of scientific articles, but an article in a scientific journal is most likely to be peer reviewed, which makes it a more reliable source of news. However, this is compounded by the fact that the quality of scientific journals can vary significantly and some journals publish research without peer review. [figure omitted]

The most popular science fake news over the years has been vaccine manufacturer conspiracy theories and denial of man-made climate destruction. Vaccines are considered one of the most important inventions ever made for the benefit of humanity. The World Health Organization estimates that vaccines save 2–3 million lives every year. However, a **fabricated scientific article that claimed that the measles, mumps, and rubella vaccine causes autism [26] led to widespread dissemination of this misinformation**, especially through social media. This, in turn, led not only to record levels of measles incidence in Europe in 2018, but also expanded the range of so-called anti-vaxxers [27].

**The denial of anthropogenic climate change, which is dismissed as fake science without any evidence, has led to universal acceptance of the international agreement on climate change being lost, and its impact on global warming is likely to be disastrous around the world** [28].

One of the most widely replicated fakes is the so-called flat Earth theory. Tens of thousands of videos, social media accounts, podcasts, and websites are devoted to this absurd theory [29, 30]. Today, when space probes are exploring the planets of the solar system, such “scientific” information can only cause confusion.

In general, the coronavirus pandemic has spawned a host of **conspiracy theories and fake science news**, which can be roughly divided into the following categories:

• the origin of the SARS-CoV-2 virus (bat soup, a laboratory leak, creation of the virus by Bill Gates or the US Government);

• racial theory (for example, only Asians are infected with the virus);

• the spread of coronavirus (5G networks);

• treatment and prevention of coronavirus (alcohol consumption; rinsing with chlorine dioxide; bleach injections; swimming in a pool with chlorinated water; eating garlic, ginger, sesame oil, bananas; using cocaine; washing hands and rubbing surfaces with baby urine; warming up the nose with a hairdryer; taking baths with granite);

• politics (governments hiding the real deaths from coronavirus and falsifying vaccinations; the increase in the incidence in Europe is caused by illegal migrants);

• epidemiology and statistics (overestimated/ underestimated statistics on morbidity and mortality);

• vaccines and vaccinations (death after vaccination; mass vaccination for the sake of obtaining superprofits by corporations; the contents of heavy metals in the vaccine).

Most readers probably found this news funny, but there are examples where such messages caused serious harm to health and even led to death. As an example, by the end of March 2020, over 2100 Iranians had been poisoned by oral methanol. Iran, as an Islamic country, has strict restrictions on alcohol consumption, but in this case patients said that, according to information on social networks, SARS-CoV-2 infection can be prevented with alcohol. As a result, almost 900 patients poisoned with illegal alcohol were admitted to the intensive care unit and 296 of them died [36].

With the development of science and technology, there has been a clear increase in interest in science and scientific research. On the one hand, society is aware of the dependence of progress on the development of scientific research; on the other hand, **it perceives science as something that carries potential threats**. The digital revolution contributed to the replacement of vertical models of dialogue between science and society with horizontal models [43]. An important subject of the dialogue between society and science is the diversity of scientific knowledge in the information environment. The transition of scientific knowledge into knowledge for all is ensured by the popularization of science, which gives knowledge a form accessible to the general public.

**The massive dissemination of fake science news can be seen as a crisis of the political system and science journalism and as a new propaganda tool, where fake scientific information is deliberately disseminated on social networks in a viral manner with the aim of quickly impacting the audience.** There are many motives for creating fake science news, the most obvious being financial gain and ideological beliefs.

Preventing the deliberate creation of false information is very difficult, and, in democratic societies that operate on the principles of free speech and freedom of expression, it is even more difficult. Thus, instead of looking for ways to prevent the creation of misinformation, the **primary focus should be on limiting the spread of fake news and minimizing the damage it can cause**.

#### Specifically, misinformation devastates biodiversity through misplaced conservation

Ford et al, 21, Ford is the associate professor at the department of biology at the University of British Columbia; the articles they write focus mainly on conservation. “Understanding and avoiding misplaced efforts in conservation”, FACETS, 2021, [https://www.facetsjournal.com/doi/pdf/10.1139/facets-2020-0058 /](https://www.facetsjournal.com/doi/pdf/10.1139/facets-2020-0058%20/)chuo

===5 main reasons (misallocating resources, misinforming supporters, alienating partners, delegitimizing evidence, & other one is direct---an action intended to enhance biod has a direct, negative impact on a wild population) why disinformation/misinformation (same effect so it’s the same here) is bad for biodiversity & conservation (problem of “misplaced conservation”)

Recent social trends have seen rising polarization in political affiliations and on key issues (Bail et al. 2018), along with the amplification of misinterpreted or false information in public discourse (Lazer et al. 2018). These two trends may have negative effects on many aspects of health, politics, science, and the conservation of biodiversity. For example, as early as the 1940s, and for decades after, the spread of misinformation overwhelmed scientific evidence suggesting a link between tobacco smoking and cancer (Proctor 2012). Today, similar misinformation regarding the efficacy of vaccinations (Lazer et al. 2018) or responses to the public health orders (e.g., the use of masks to reduce the spread of COVID-19) foments polarization and threatens public health (Paes-Sousa et al. 2020). The mere suggestion of human-caused climate change has become polarizing, impeding actions that could minimize harm to human health, livelihoods, and biodiversity (Biddle and Leuschner 2015). Polarization threatens cooperative approaches to problem solving and decision-making (Barber and McCarty 2015; Maher et al. 2018), while misinterpreted or false information distracts the public and decision-makers from acting upon pressing needs and may waste resources in doing so (Oreskes and Conway 2011; Barnes et al. 2018). The conservation of biodiversity is a globally significant challenge, and inherently **requires cooperation and evidence to be successful**. However, success in conservation can be influenced by actions that **undermine cooperation and evidence**—i.e., **polarization and misinformation**. To better understand how polarization and misinformation affects biodiversity, we define the term **“misplaced conservation”**, which occurs when actions increase the scientific, financial, political, or social resources required to achieve a positive outcome for biodiversity in the present or future. Misplaced conservation is distinct from other human activities that are also direct threats to biodiversity, such as habitat loss or overexploitation. The concept of misplaced conservation focuses on activities where conservation resources are expended on an improper, unsuitable, or unworthy activity and the intended outcome of such activity was: (i) to maintain or restore biodiversity, but this outcome is impeded by lack of cooperation and evidence and (ii) to intentionally impede the use of cooperation and evidence in the context of doing conservation. For these reasons, misplaced conservation arises from the combined underlying influences of polarization and misinformation on conservation activities. By articulating the concept of misplaced conservation (Fig. 1), we hope to provide a framework to help overcome barriers to more effective conservation actions. At its most benign, misplaced conservation may arise from genuine motivations to conserve biodiversity. These motivations may quickly give rise to incremental actions that appear as “baby steps” or “raising awareness”. Too often, the success of these actions is not supported with evidence of their positive effect on biodiversity and may instead be distracting or otherwise placating people into a false sense of success (Hagmann et al. 2019). For example, “nudging” is a concept that alters the architecture of choice or the context in which choices are made to provide options that have smaller benefits, with lower costs, with quicker pay offs (Thaler and Sunstein 2009). While nudging has proven effective in many circumstances (Sunstein 2017), it can also lead to complacency that undermines support for more impactful policies and decision-making. Using an experimental approach, Hagmann et al. (2019) found that people overestimated the effectiveness of small gains in environmental policy, when a more costly but more effective alternative was presented. Similarly, simply “raising awareness” does not always lead to positive changes for conservation. In a behavioral experiment, Dunn et al. (2020) found that after watching a documentary about marine conservation, people increased their subject matter knowledge, but they did not change their behaviour with respect to ocean pollutants. While many impactful environmental movements began with smaller, incremental successes, nudges, and awareness campaigns, it should not be assumed that these are effective tools for conservation. The effectiveness of such interventions needs to be evaluated against the potential costs incurred by the fomentation of complacency. Misplaced conservation also occurs when actions are intended to impede successful conservation. This malicious intent could, for example, involve attacking the credibility of an opposing scientist when competing lines of evidence are part of a conflict between stakeholders (Horton et al. 2016; Harvey et al. 2018; Loss and Marra 2018). For example, Hmielowski et al. (2014) found that when the mainstream media work to deliberately decrease trust in scientists, it increases uncertainty that global warming is happening. Giving equal weight to dissenting views, often a hallmark of journalism, without consideration of expertise may further exacerbate the credibility of science (Brown and Havstad 2017) and lead to policies that are inconsistent with the best available evidence to solve problems (Anderegg et al. 2010). [fig. 1 omitted] Whether people are motivated by truly benign outcomes and happen to be misguided or ignorant in their execution of conservation actions or they are motivated to be deliberately malevolent or negligent, we consider all of these intents to be part of misplaced conservation. The outcomes, rather than intentions, help determine misplaced conservation. Here, we describe some of the key actions that create misplaced conservation, supported by case studies to demonstrate this concept. We begin by describing five nonexclusive actions and then discuss solutions to better understand and resolve it—a critical step towards biodiversity conservation in an era of polarization and lies. Broadly speaking, there are direct (1) and indirect (4) pathways through which the actions of people lead to misplaced conservation (Fig. 1). Direct misplaced conservation has a proximate, negative impact on a wildlife population or biodiversity. In contrast, indirect, misplaced conservation impedes the ability of the public, conservation practitioners, stakeholders, or scientists to do conservation. The indirect impacts of misplaced conservation arise from (i) misallocating of resources, (ii) misinforming supporters, (iii) alienating partners, and (iv) delegitimizing evidence. These actions are not mutually exclusive and can combine to influence conservation outcomes (Table 1). For example, this misallocating resources can lead to a direct loss of biodiversity (Bottrill et al. 2008; Gilbert et al. 2020) or the misuse of evidence can entrench alienization of potential partners (Hodgson et al. 2019). Misplaced conservation can arise when an action intended to enhance biodiversity has a direct and negative impact on a wild population, species, or ecological community (Table 1). For example, domestic sheep (Ovis aries) were removed from a private ranch ahead of the area’s forthcoming designation as Patagonia National Park, Chile (Wittmer et al. 2013). A primary motivation to create this protected area was to conserve populations of huemul deer (Hippocamelus bisulcus). However, by removing an important prey item (i.e., sheep) for local carnivores (Vulpes spp. and Puma concolor), predation rates on native deer species increased. The well-intentioned action of creating a more “pristine” environment to benefit huemel deer accelerated their decline. In another case of direct harm, members of the public planted a species of milkweed to help provide habitat for monarch butterflies (Wade 2015). However, some people used a milkweed species that is not native to the temperate species range of monarch butterflies. As a result, monarchs interrupted their migration and were exposed to higher rates of egg parasites. Exposure to this non-native milkweed created a direct threat to monarchs (Satterfield et al. 2015). Lastly, kokanee salmon (Oncorhynchus nerka) stocks in Okanagan Lake, British Columbia, were declining through the 1950s (Shepherd 1999). The planned introduction of the exotic mysid shrimp (Mysis relicta) in 1966 was intended to provide productive forage for the native salmon with the intention of bolstering the fishery. However, shrimp were able to escape predation from salmon through diel migration through the water column and then compete with juvenile kokanee for plankton. As a result, the introduction of mysid shrimp reduced forage for juvenile salmon, reducing recruitment, and directly hastening the decline of the salmon fishery. Consequently, there have been calls for the application of additional, costly control measures to lower mysid numbers (Shepherd 1999). **The well-intentioned but misplaced effort to conserve biodiversity may exacerbate declines.** Efforts to bolster evidence through pilot studies and adaptive management and to improve the uptake of evidence in policy through cooperative approaches in decision-making are needed to minimize the prevalence of direct misplaced conservation. It is a common experience for people working in conservation to operate with under-supported resources. These resources include funding, time, volunteer effort, media attention, or social or political capital. Misplaced conservation occurs when such **fixed and limited resources are misallocated to issues that have minimal gains for biodiversity** (Table 1). This **misallocation of resources** makes it more difficult to act upon higher priority action because fewer resources are then available. [table 1 omitted] Misallocating resources has often occurred when conservation agencies decide which species to prioritize for recovery or enhanced management. Species recovery efforts are often targeted at a subset of species under threat—this subset may have a higher “profile” (i.e., is more charismatic) and a lower threat profile than other species. Consequently, species with a lower public profile are underresourced (Donaldson et al. 2016). In some cases, habitat protection for less-charismatic species can be far more cost-effective approach to restoring biodiversity than efforts focused exclusively on high-profile species (Neeson et al. 2018). Similarly, the rise of individually focused conservation outcomes, or “compassionate conservation” (Ramp and Bekoff 2015) pulls resources away from more proximate causes of species or population decline to serve the welfare outcomes of individual animals, usually from a limited subset of large charismatic species (Hayward et al. 2019; Oommen et al. 2019). While animal welfare is embodied in many aspects of wildlife management and research, it is often unstated how attention given to the fate of individuals elevates the conservation of a species, population, or community. For example, many people were upset when “Cecil” the lion was killed by a hunter in 2015, yet policy reforms to support lion conservation have moved little since that time (Carpenter and Konisky 2019). Still, the legacy of Cecil’s death remains a rallying cry for some conservation groups (Darimont et al. 2020). Efforts to address the negative impacts of habitat loss, invasive species, or human–wildlife conflict through compassionate conservation approaches would make unavailable some of the most cost effective and successful tools developed to preserve and restore biodiversity (Callen et al. 2020). To minimize the misallocation of resources, there either needs to be better use of existing allocations, or more resources, and preferably both (Bonebrake et al. 2019). To improve use of existing allocations, conservationists have put forward prioritization schemes to quantify tradeoffs in decision-making (Martin et al. 2018). In some cases, such priority allocation could lead to the loss of some components of biodiversity, but preserve a larger, more valued component (Gilbert et al. 2020). This so-called “conservation triage” has been hotly contested (Bottrill et al. 2008), but until resources are enhanced, there will likely remain a need to prioritize allocations in a world of finite resources. While we argue there is no “most correct” conservation action that inherently deserves priority resource allocation, a more transparent, evidence-based and cooperative decision-making process should at least reveal tradeoffs in resource use. Questions of whose priority matters the most are critical to resolving allocation in a just and equitable manner. As such, the underlying human dimensions of conservation governance are central to mobilizing cooperative approaches to evidence-based decision-making (Decker et al. 2016). **Misplaced conservation outcomes can arise when the public is misinformed about which threats are most pressing, which species are a priority for action, and (or) which actions are most beneficial for biodiversity** (Table 1). A misinformed public also diverts resources away from actions that benefit conservation. For example, in the 2010s, a series of amateur-made online petitions to ban shark finning in Florida (USA) attracted tens of thousands of signatures. However, shark finning was banned in Florida in 1994, such that these petitions cannot possibly achieve their stated goal. These “finning” campaigns also contribute to the misunderstanding of threats facing sharks by incorrectly suggesting that the shark fin trade is the only threat these animals face (Shiffman and Hueter 2017). In contrast, government-sponsored (e.g., National Oceanographic and Atmospheric Administration (NOAA), a Federal agency that houses the National Marine Fisheries Service agency (NMFS)) **petitions that would lead to tangible policy directions receive little attention**. For example, three recent and evidenced-based proposals aimed to improve the sustainability of fisheries: an 2016 NMFS proposal to modify recreational angling regulations for threatened dusky sharks (81 FR 71672), a 2017proposal to alter the US-Atlantic coast shark fishing season (82 FR 55512), and a 2017 proposal to require tuna fishing vessels to release threatened sharks that they capture (82 FR 56177). None of these petitions received substantial public support or commentary (only 87, 13, and 1 comment(s) were posted, respectively). Similar to the case of using non-native milkweed to help monarch butterflies, recent awareness of pollinator conservation has focused largely on campaigns to “save the bees”. However, confusion over how to best do this has been impeded by the conflation of native pollinators and managed, non-native bees (Dicks 2013). Managed bees contribute to the decline of native biodiversity via pathogen spillover and competition for floral nectar (Colla and MacIvor 2017). Broadscale policies to conserve pollinators, such as the US-based Pollinator Partnership Action Plan, focus on land uses and pesticide bans that will benefit non-native honey bees at the expense of native bumblebee species (Nicholls et al. 2020). While wild honey bee conservation is a concern within its native range (Requier et al. 2019), misinformed support for such “insect livestock” and feral, non-native species across North America threatens native pollinators which are truly at risk of extinction (Dicks 2013). Ocean plastics have emerged as a central issue in marine conservation. For example, “straw shaming”—even at the cost of infringing on the needs of people experiencing physical disabilities— is one extreme outcome of the plastic pollution response (Krueger 2019). However, technological solutions to remove ocean garbage (i.e., through surface skimming) may not target the areas of the ocean where most pollution occurs (i.e., at depth) (Stafford and Jones 2019). Like the nudging of decarbonization policy (Hagmann et al. 2019), contemporary approaches to plastic pollution may have created a “convenient truth to distract environmental policy from more serious and urgent threats” (Stafford and Jones 2019). Overcoming these distracting discourses in conservation will not only require effective science but also effective communication of knowledge to support behavioral changes. As with the other dimensions of misplaced conservation, supporters become misinformed when evidence is not communicated clearly or used appropriately. Such misinformed support can be the outcome of conservation leadership failing to “do their homework” for how to best focus the efforts of people invested in positive outcomes for biodiversity. Efforts to better connect conservation biology and conservation social science (including communication science) are critical to channeling clear and accurate information to supporters (Kareiva and Marvier 2012; Bennett et al. 2017). **Misplaced conservation can occur when the partners (groups or individuals) become alienated from a shared vision of success that was caused by, or results, in greater polarization.** Alienation occurs when short-term gains are elevated over long-term benefits and when individual gains are elevated over collective benefits, giving rise to conservation social dilemmas (Cumming 2018) or conservation conflict (Redpath et al. 2013). While alienation may result from different value systems held by conservation partners and the perceptions of inequity (i.e., superiority) in those value systems relative to others (Saunders et al. 2006; Manfredo et al. 2017), the outcome is disrupted partnerships. For example, hunting, animal welfare, and conservation organizations may not share the same ethical, instrumental, or utilitarian values towards wildlife, yet all of these groups advocate for better conservation outcomes for wildlife (Butler et al. 2003; Treves 2009; Dickman et al. 2019). When these groups are pitted against one another over a subset of values (e.g., consumptive use of wildlife; evidence vs. anecdote; science vs. emotion), it generates conflict and weakens their collective ability to affect change on commonly shared values (e.g., the persistence of wildlife populations) (Redpath et al. 2017). Given the importance of partnerships in achieving conservation success (McNeely 1995; Cooke et al. 2020), efforts that disrupt partnerships can have dire and long-lasting consequences. One common way alienation manifests is through geopolitical structures that are decoupled from diverse value systems and worldviews. As in many countries, people in rural Sweden had a more favorable view of lethal approaches to human–wildlife conflict than people in urban areas (Gangaas et al. 2013). Urban populations can influence policy on human–wildlife conflict policy without facing the proximate consequences of loss of safety, interruption of livelihood, or damage to property (Ericsson and Heberlein 2003). Rural residents may therefore act outside of regulations (Gangaas et al. 2013) unless given more appropriate tools and resources to resolve conflict with wildlife (König et al. 2020). Similarly, Indigenous perspectives in conservation often are alienated by colonial governments. Recently, The Tahltan Nation in British Columbia offered bounties for grizzly bear and wolf harvest following a province-wide ban on grizzly bear hunting—which the Tahltan had vocally opposed (Simmons 2020). The persistence of stakeholder conflict, unregulated actions, and centralized or colonial decision-making makes it more difficult to conserve biodiversity for rural, urban, and Indigenous people. The emergence of alienated partners speaks clearly to the role of cooperation as an antidote to polarization. In some cases, evidence can help support or bring together groups in a cooperative manner and reduce polarization (Baynham-Herd et al. 2020; Williams et al. 2020). However, science can also become “weaponized” by all sides in public debate, such that more information will not always generate better decisions (Peery et al. 2019). Instead of conflating conservation with a “data gap” per se, efforts to improve processes that lead to better decisions (i.e., in a manner the improves stakeholder or public support) may be needed to overcome the alienation of partners and increase the success of conservation actions. **Misplaced conservation can arise [or] when the products (i.e., facts) and generators (i.e., scientists) of evidence are delegitimized in the political or decision-making realm** (Table 1). Here, we refer to evidence in the context of biological and social “western science”, and recognize that there are other systems that create, hold, and share knowledge (e.g., Indigenous knowledge) that make important contributions towards conservation (Garnett et al. 2018) and also face delegitimization. Delegitimization may arise when scientists representing different world views, or interpretations of data, come into debate over a policy. The perception of scientific uncertainty is then exploited to undermine conservation outcomes. When decision-makers or the public perceive a lack of scientific consensus, it undermines the value of evidence and confidence in evidence-based decision-making (Lewandowsky et al. 2013). For example, special interest groups may inflate perceptions of uncertainty, via doubt mongering, in a practice that has been seen in polar bear conservation (Harvey et al. 2018), the impact of free ranging cats on biodiversity (Loss and Marra 2018), and responses to climate change (Oreskes and Conway 2011). In some cases, delegitimization may arise from competing interests in the uptake of certain types of information, rather than a lack of information per se. “Whose science matters” becomes central to these debates and evidence may reinforce, rather than neutralize, polarization among groups (Hodgson et al. 2019). Such debates have been documented in raptor conservation (Hodgson et al. 2019), deer management (Freddy et al. 2004), bear hunting (Maji´c et al. 2011), and climate change (Hayhoe 2018). Peery et al. (2019) described the challenge of agenda-driven science in conservation: “because conservation conflicts in an increasingly polarized world might tempt some to engage in agenda-driven science to win a conflict.” Finally, scientists may delegitimize their own contributions to positive conservation outcomes. Unlike fundamental scientific disciplines, conservation sciences actively encourage the blending of curiosity-driven, basic research with mission-oriented applied research and advocacy (Horton et al. 2016; Smol 2018). Conservation scientists often engage in public discourse and play an important role in disseminating facts to the public, stakeholders, and decision-makers (Chan 2008; Smol 2018). However, conservation scientists risk depleting the credibility of the research community in general if values and facts are conflated (Horton et al. 2016; Redpath et al. 2017). Indeed, as Baynham-Herd et al. (2020) showed, trustworthiness of intervenors is seen as a key predictor of cooperation in conservation with integrity ranking as a key dimension of how trust is built. For this reason, transparency in the facts (i.e., scientific consensus) vs. the expressed values of the scientist require clear articulation. As Chan (2008) argued, conservation scientists must clearly communicate where the facts stop and where their own values begin, or they risk abusing goodwill and trust towards science and its practitioners. To avoid or mitigate misplaced conservation efforts, we recommend that more effort be made to adopt an intentional, transparent process of decision-making that accounts for the gains and losses to both cooperation and biodiversity (Saunders et al. 2006). While this effort may at first appear to be conservation dictum, we underscore that cooperation has too often taken a back seat to short-term gains in biodiversity. Finding pathways cooperation, in spite of knowledge gaps and differences in attitudes or beliefs, remains an essential and yet understudied tool in formal conservation education and training (Cinner 2018). Rather than try to change or undermine the values of potential partners, it is usually more effective to find alignment with the existing values of conservation partners (Decker et al. 2016; Manfredo et al. 2017; Hayhoe 2018). Seeing conservation efforts as a push towards better cooperation and use of evidence is one way to suppress the negative effects of polarization and misinformation. Scientists and managers should invest in (and be supported to do so) efforts to monitor the outcomes of conservation action, then interpret, share, and respond adaptively to evidence as it accrues. Such an “adaptive management” approach is often discussed in conservation but not clearly executed (Keith et al. 2011). For example, recent efforts to ban (British Columbia, Canada in 2017) or restore (in Wyoming, USA) grizzly bear hunting have focused on ethics and individual welfare; however, there has been little or no advocacy by conservation groups to create processes that quantify the impacts of these policy changes on bear populations and the people who must co-exist with them. Adaptive management as a means of understanding and solving conservation problems is vulnerable to many of the same challenges faced in misplaced conservation writ large, with self interest, conflicts, and deliberate overconfidence in data serving to undermine management goals (Walters 1997). Reducing uncertainty is a central goal of evidence-based decision-making, yet progress in science is often nonlinear and unpredictable. Debate and paradigm shifts are a normal and important part of the scientific process (Kuhn 2012). Conservation science is no different, with some debates unresolved after decades of research (Young et al. 2010). As such, we do not suggest that conservation scientists should abandon productive and civil debates about science generally or conservation specifically, but we hope that such debates will focus on critical and transparent analysis of data, analyses, techniques, and interpretations, rather than a critique of scientists or the inferred motivations or values of potential conservation partners. Conservation actions often are motivated by perceptions of scarcity and imbue a sense of urgency— the time to act is “now”. However, **the risks that come from passionate, but misinformed, people advocating for preferred policy outcomes that misalign with evidence can be high**. Cooperation, as antidote to extinction, needs to transcend the roles played by people concerned with biodiversity, of which scientists are but a limited sector. Many groups (e.g., public, experts, scientists, governments, and conservation organizations) are responsible for promoting the importance of biodiversity and acting to averting loss. For this reason, it is not necessary for every concerned member of the public to know every technical detail and nuance of complex environmental problems, nor the policies that can help address them. Nonexperts can help by joining, or working to amplify the message of, expertled and evidence-based conservation campaigns. Nonexperts can also volunteer their time or help raise funds for expert-driven campaigns, or they can write to decision-makers expressing support for (or opposition to) policies as recommended by experts. Ultimately, people should consider that without specific knowledge, training, or experience, that there are real risks to people and biodiversity if ineffective solutions are promoted to resolve complex problems. [table 2 omitted] In addition to cooperation across levels of “expertise”, efforts to promote cooperation across backgrounds and identities has demonstrated positive outcomes for science. Conservation actions stemming from diverse and inclusive processes that include a variety of views and experiences should produce the best outcomes. For example, greater gender diversity on research teams leads to more productive scientific outcomes, in addition to the benefits of creating more equitable workspaces (Nielsen et al. 2017). Likewise, integrating local and macro-scale institutions is a critical step towards recognizing the diversity of power, scope, and governance structures that affect biodiversity (Berkes 2007; Popp et al. 2019). Including local peoples in decision-making increases their agency over resources and should increase acceptance of any changes to their daily lives that come from conservation actions. An important vehicle for cooperation is open, transparent, and respectful communication with all relevant partners (Lundquist and Granek 2005). Stakeholders and rights holders who believe that regulations were developed in a reasonable, fair manner that incorporates collective priorities are more likely to follow resulting regulations and laws (Kennedy 2010; Dressel et al. 2020). Likewise, when stakeholders feel like they and their concerns are being ignored, they are more likely to ignore the resulting regulations (Suman et al. 1999; Freddy et al. 2004). Shiffman (2020) documented how strategically communicating key scientific facts and science-based policy solutions resulted in passing new environmental regulations while minimizing inter-stakeholder conflicts. Social media has transformed how people communicate with one another, a transformation that has important implications for both environmental advocacy and for conservation scientists who wish to engage in public outreach (Parsons et al. 2014; Lamb et al. 2018; Smol 2018). This transformation may not always result in positive gains for biodiversity (i.e., via the spread of misinformation; Vosoughi et al. (2018)); nonetheless, social media is a powerful form of intervention and feedback. When used well, social media also has the potential to infuse public discourse with expert-supported approaches to conservation and pushback on misinformation (Thaler and Shiffman 2015; Shiffman 2020). In addition, scientists can now hear the concerns people are expressing on social media about biodiversity-related policies and this, in turn, can help design more cooperative approaches to conservation and nuanced communication strategies. This insight needs to be contextualized of course, as the media channels available to a scientist are constructed through the same biased algorithms as the information leading from the scientist to the public. As much as there are positive steps people can take to reduce misplaced conservation, acting poorly can make a bad situation worse. There is a need for conservation scientists to acknowledge that people trying to help is not the same as helping, and good intentions do not excuse easily foreseen or managed harm. Case studies of misplaced conservation often highlight people who wanted to help but may have not foreseen the myriad outcomes of their actions. However, conservation decisions affect the existence of species, peoples’ livelihoods, or the intactness of cultures—the onus on better decision-making leaves little room for error (Foote and Wenzel 2009). Misplaced conservation asks scientists and stakeholders to acknowledge that outcomes—rather than intentions—are the arbitrator of conservation success. Society has enshrined into law the concept of negligence to help guide responsible behaviour when the outcomes were reasonably anticipated. For example, driving while intoxicated is against the law in many places because it is a known and well-established risk to public safety—the intentions of the driver (e.g., to get home) are not at issue. There often are no explicit laws to protect against misplaced conservation (i.e., excluding environmental regulations) and this is unlikely to occur. However, there is a need to better hold people involved in making conservation decisions accountable for their role in promoting polarization and misinformation. The benefits of cooperative and evidence-based approaches to conservation are well described and are generally regarded as essential for achieving conservation gains (Keith et al. 2011). These approaches build policy with evidence and integrate wholistic dimensions of conservation practice—including the roles of governance, politics, social justice, and fundamental ecology. Yet, the adoption of these concepts is far from universal practice. There is a need to better understand and then address the practices that run counter to the body of knowledge that has described pathways to effective conservation practice (Table 2). Society is witnessing one of the largest and most rapid mobilizations of scientific focus and public policy in history in response to the COVID-19 pandemic. Along with the urgency and scope of this crisis, lessons are quickly emerging about the critical role of scientific integrity and accountability and the need for accurate communication between science, policy, and the public (Piller 2020). Conservation science will benefit from these lessons as society continues to cope with accelerating global extinctions. Articulating the mechanisms of, and solutions, to misplaced conservation will help ensure that efforts to restore and protect biodiversity are successful.

**Biodiversity loss cascades and is existential**

**Torres, 16** - founding director of the X-Risks Institute, an affiliate scholar at the Institute for Ethics and Emerging Technologies, and author of the forthcoming Morality, Foresight, and Human Flourishing: An Introduction to Existential Risks ( Phil, ‘Biodiversity loss: An existential risk comparable to climate change’, April 11 2016, <https://thebulletin.org/2016/04/biodiversity-loss-an-existential-risk-comparable-to-climate-change/> )//hecht

**Catastrophic consequences for civilization**. The consequences of this rapid pruning of the evolutionary tree of life extend beyond the obvious. There could be surprising effects of biodiversity loss that scientists are unable to fully anticipate in advance. For example, prior research has shown that localized ecosystems can undergo abrupt and irreversible shifts when they reach a tipping point. According to a 2012 paper published in Nature, there are reasons for thinking that we may be approaching a tipping point of this sort in the global ecosystem, beyond which the consequences could be catastrophic for civilization. As the authors write, a planetary-scale transition could precipitate “substantial losses of ecosystem services required to sustain the human population.” An ecosystem service is any ecological process that benefits humanity, **such as food production and crop pollination**. If the global ecosystem were to cross a tipping point and substantial ecosystem services were lost, the results could be “**widespread social unrest, economic instability, and loss of human life**.” According to Missouri Botanical Garden ecologist Adam Smith, one of the paper’s co-authors, **this could occur in a matter of decades**—**far more quickly than most of the expected consequences of climate change, yet equally destructive**. **Biodiversity loss is a “threat multiplier”** that, by pushing societies to the brink of collapse, will exacerbate existing conflicts and introduce entirely new struggles between state and non-state actors. Indeed, **it could even fuel the rise of terrorism**. (After all, climate change has been linked to the emergence of ISIS in Syria, and multiple high-ranking US officials, such as former US Defense Secretary Chuck Hagel and CIA director John Brennan, have affirmed that climate change and terrorism are connected.) The reality is that **we are entering the sixth mass extinction** in the 3.8-billion-year history of life on Earth, and the impact of this event could be felt by civilization “in as little as three human lifetimes,” as the aforementioned 2012 Nature paper notes. Furthermore, the **widespread decline of biological populations could plausibly initiate a dramatic transformation of the global ecosystem on an even faster timescale: perhaps a single human lifetime**. The unavoidable conclusion is that **biodiversity loss constitutes an existential threat in its own right**. As such, it ought to be considered alongside climate change and nuclear weapons as one of the most significant contemporary risks to human prosperity and survival.

## \*\*Warming\*\*

### 2AC Warming Add-On

#### Science disinformation hinders solutions to existential crises---climate change and vaccines

ALLEA, 21, ALLEA is the European Federation of Academics of Sciences and Humanities, representing more than 50 academies from over 40 countries in Europe; “Fact or Fake? Tackling Science Disinformation”, ALLEA, 05-2021, https://allea.org/wp-content/uploads/2021/04/Fact-or-Fake-Discussion-Paper.pdf/chuo

===tbh this card is kind of similar to Gerbina but is better lol; not specific to undermining trust though this is about just wrong information makes people do the wrong things

The overall success of the scientific method also means that when someone wants to make claims that go against established scientific knowledge and are not grounded in the scientific method, they must seek to undermine the trustworthiness of the scientific method or scientists per se. Thus, paradoxically, scientific language is often adopted at the same time as scientific activities themselves are being questioned. An extreme and particularly harmful form of anti-scientific activity appears in the form of conspiracy theories with notable examples in the three areas chosen for analysis in this discussion paper: climate change, vaccines, and pandemics.3

**Science disinformation is one of the major challenges of our times, with consequences for society at large and for (trust in) science.**4, 5 This paper sheds light on the characteristics and mechanisms of science disinformation and discusses what scientists, science communicators and policymakers can do about it.

While science disinformation and misinformation is common in many different areas, we have chosen to focus on three that strike us as particularly important: climate change, vaccine safety and pandemics.

Climate change in the form of global warming resulting from human activities was first predicted more than a century ago. Continuous monitoring of various physical and chemical parameters shows that the process of warming has accelerated during recent decades. Signs of global warming include melting glaciers, thawing permafrost, and rising sea levels. These changes are caused by growing concentrations of greenhouse gases in the atmosphere. Findings in many areas of research are almost unanimously interpreted to mean that the large number of humans and their activities have prominent roles in these developments.6

Major concerns are now if the increase in carbon dioxide levels and temperatures mean that **efforts to break the rising curves will come too late**. Models predict rising sea levels and **flooding of large coastal area**s, thereby **reducing areas for human settlements and food production**. This is predicted to **displace hundreds of millions of people**, resulting in an **increased population density and raising the potential for violent conflicts**. Together, these processes will **extinguish habitats for many species of organisms and exacerbate the ongoing mass extinction**.

Despite overwhelming scientific evidence, politically motivated refusal to accept anthropogenic global warming (increasing temperatures due to human influence) has been intense and has used both ‘cherry-picking’ and conspiracy theories in order to counter widely accepted scientific evidence. This resistance has received strong financial support from business interests, further amplified by certain sections of the media. **If the facts of climate change and its causes are countered with false claims about cause-and-consequence relationships, this will delay actions to reduce global warming, potentially with disastrous consequences.**

**Vaccines are considered one of the most important inventions ever for the benefit of humankind.** The World Health Organization has estimated that vaccines save 2-3 millions of lives every year, especially children, and prevent unimaginable suffering.7 High immunity at the population level arising from vaccinations leads to reduced transmission of an infectious disease and may even eliminate it completely. Those who have been vaccinated will serve as a protective barrier by not transmitting the disease to those who have not been vaccinated (so called ‘herd immunity’).

Nevertheless, opposition towards vaccination has existed since vaccination programmes were introduced. The reasons for this resistance have varied over time and have at times been based on valid doubts as to the vaccine’s efficacy. However, some vaccines have been used for decades and all vaccines are consistently monitored to ensure a high ratio of benefits over risks. In addition, high standards for the approval of new vaccines have been implemented worldwide. Nevertheless, public resistance to vaccines prevails in some pockets of our societies, sometimes keeping vaccination uptake below the threshold required for herd immunity.

**False information, exaggerated/unjustified claims about side effects, or conspiracy theories regarding underlying objectives for global vaccination programmes may ultimately lead to an insufficient rate of vaccination and therefore inadequate levels of immunity at the population level.** Vaccine hesitancy can not only lead to unnecessary disease outbursts, but also puts those at risk who have not yet been vaccinated, especially infants, and those who cannot be vaccinated, such as individuals with immune deficiencies. **Misinformation that increases vaccine hesitancy may cause more people to suffer from an epidemic, more people to show severe symptoms, and more people to die.**

The origin and spread of the pandemic have been the subject of much speculation, some of which has involved fanciful conspiracy theories such as linking the pandemic to 5G mobile phone technology or suggesting the virus was man made and introduced into the population on purpose. In addition, there have been numerous cases of fraudulent marketing of health care products, ranging from face masks to ventilators. Even political leaders in several countries have promoted regimens that completely lacked clinical or biological evidence. Those who complied may have caused themselves unnecessary harm and/or felt unduly safe and have displayed more risky behaviour, either by exposing themselves to individuals infected with the virus or by ignoring their own symptoms and thereby exposing others. This ‘infodemic’ coined by the WHO may have contributed to the spreading of the pandemic and may have **increased the number of patients with severe symptoms requiring intensive care, as well as the number of deaths.**

Generating disinformation can be incited by different motivations in different actors and in numerous combinations. The most apparent motivations are financial profit and ideological conviction. Both can at times deviate from norms of rationality and moral standards when individuals ignore or are unable to recognise harmful consequences for others. In other instances, the aim of **disinformation is to deliberately cause confusion, instability, or mistrust for political purposes.**

Deliberate construction of false information is very difficult to prevent. When lies are generated wilfully, the responsible individuals have already committed themselves to fraud. Likewise, it may also be hard to convince those who knowingly disseminate existing misinformation to change their behaviour. In open societies with strong protective individual rights and freedom of expression, it is difficult to stop disinformation at its roots, except by appealing to humanitarian values and hoping that those who produce and spread disinformation will consider with empathy the consequences for other people and then stop themselves and change their behaviour. Instead of finding ways to prevent disinformation from being generated in the first place, **efforts will have to focus on limiting the spread of disinformation and minimising the damage it may cause**.

Policymakers have at least four ways to prevent the spread of misinformation: They can regulate content directly, provide someone with the authority for regulating content, redesign the structures (platforms) in which content is generated and distributed, or support the creation of instruments that can raise citizen awareness and enable them to identify and prevent the dangers of misinformation.30

One way forward is to ask public regulators of news media to intensify their regulation of social media platforms and websites. Web services are often sources of news and information while also financed by advertising agencies. This leads to an obvious conflict of interest that needs to be examined and constantly regulated.

However, search engines and social media platforms should not be viewed as a threat to our democracy per se. We should act in an enlightened manner to nurture and guide the rich value of diverse commercial sources of digital information, as we do with newspapers and television channels. We need to regulate them in a manner that allows us to access the accurate information and exploit emerging information technologies, e.g. automated factchecking and recommender systems.

Last but not least, **governments have the option of strengthening incentives for empowering recipients of information to identify and cope with mis- and disinformation, either themselves or with the help of machine learning systems**. (Digital) media literacy is crucial here for evaluating the content and context of information and ultimately detecting its accuracy. Several endogenous cues (content) and exogenous cues (context) can help **test the validity of information**.31 However, such cues to disinformation and their uptake for regulation remain largely underexplored.

**Urgent action on a global scale is necessary to mitigate these processes.** However, many political leaders and large proportions of populations still deny the factual observations, the observed or inferred causes, and the predicted consequences. This causes necessary decisions to be insufficient both in extent and time. Thus scientists and science communicators are facing an immense challenge to explain the chains of causal events, the ongoing global warming and the predicted future consequences.

#### Extinction.

Kareiva 18, Ph.D. in ecology and applied mathematics from Cornell University, director of the Institute of the Environment and Sustainability at UCLA, Pritzker Distinguished Professor in Environment & Sustainability at UCLA, et al. (Peter, “Existential risk due to ecosystem collapse: Nature strikes back,” *Futures*, 102)

In summary, six of the nine proposed planetary boundaries (phosphorous, nitrogen, biodiversity, land use, atmospheric aerosol loading, and chemical pollution) are unlikely to be associated with existential risks. They all correspond to a degraded environment, but in our assessment do not represent existential risks. However, the three remaining boundaries (climate change, global freshwater cycle, and ocean acidification) do pose existential risks. This is because of intrinsic positive feedback loops, substantial lag times between system change and experiencing the consequences of that change, and the fact these different boundaries interact with one another in ways that yield surprises. In addition, climate, freshwater, and ocean acidification are all directly connected to the provision of food and water, and shortages of food and water can create conflict and social unrest. Climate change has a long history of disrupting civilizations and sometimes precipitating the collapse of cultures or mass emigrations (McMichael, 2017). For example, the 12th century drought in the North American Southwest is held responsible for the collapse of the Anasazi pueblo culture. More recently, the infamous potato famine of 1846–1849 and the large migration of Irish to the U.S. can be traced to a combination of factors, one of which was climate. Specifically, 1846 was an unusually warm and moist year in Ireland, providing the climatic conditions favorable to the fungus that caused the potato blight. As is so often the case, poor government had a role as well—as the British government forbade the import of grains from outside Britain (imports that could have helped to redress the ravaged potato yields). Climate change intersects with freshwater resources because it is expected to exacerbate drought and water scarcity, as well as flooding. Climate change can even impair water quality because it is associated with heavy rains that overwhelm sewage treatment facilities, or because it results in higher concentrations of pollutants in groundwater as a result of enhanced evaporation and reduced groundwater recharge. Ample clean water is not a luxury—it is essential for human survival. Consequently, cities, regions and nations that lack clean freshwater are vulnerable to social disruption and disease. Finally, ocean acidification is linked to climate change because it is driven by CO2 emissions just as global warming is. With close to 20% of the world’s protein coming from oceans (FAO, 2016), the potential for severe impacts due to acidification is obvious. Less obvious, but perhaps more insidious, is the interaction between climate change and the loss of oyster and coral reefs due to acidification. Acidification is known to interfere with oyster reef building and coral reefs. Climate change also increases storm frequency and severity. Coral reefs and oyster reefs provide protection from storm surge because they reduce wave energy (Spalding et al., 2014). If these reefs are lost due to acidification at the same time as storms become more severe and sea level rises, coastal communities will be exposed to unprecedented storm surge—and may be ravaged by recurrent storms. A key feature of the risk associated with climate change is that mean annual temperature and mean annual rainfall are not the variables of interest. Rather it is extreme episodic events that place nations and entire regions of the world at risk. These extreme events are by definition “rare” (once every hundred years), and changes in their likelihood are challenging to detect because of their rarity, but are exactly the manifestations of climate change that we must get better at anticipating (Diffenbaugh et al., 2017). Society will have a hard time responding to shorter intervals between rare extreme events because in the lifespan of an individual human, a person might experience as few as two or three extreme events. How likely is it that you would notice a change in the interval between events that are separated by decades, especially given that the interval is not regular but varies stochastically? A concrete example of this dilemma can be found in the past and expected future changes in storm-related flooding of New York City. The highly disruptive flooding of New York City associated with Hurricane Sandy represented a flood height that occurred once every 500 years in the 18th century, and that occurs now once every 25 years, but is expected to occur once every 5 years by 2050 (Garner et al., 2017). This change in frequency of extreme floods has profound implications for the measures New York City should take to protect its infrastructure and its population, yet because of the stochastic nature of such events, this shift in flood frequency is an elevated risk that will go unnoticed by most people. 4. The combination of positive feedback loops and societal inertia is fertile ground for global environmental catastrophes Humans are remarkably ingenious, and have adapted to crises throughout their history. Our doom has been repeatedly predicted, only to be averted by innovation (Ridley, 2011). However, the many stories of human ingenuity successfully addressing existential risks such as global famine or extreme air pollution represent environmental challenges that are largely linear, have immediate consequences, and operate without positive feedbacks. For example, the fact that food is in short supply does not increase the rate at which humans consume food—thereby increasing the shortage. Similarly, massive air pollution episodes such as the London fog of 1952 that killed 12,000 people did not make future air pollution events more likely. In fact it was just the opposite—the London fog sent such a clear message that Britain quickly enacted pollution control measures (Stradling, 2016). Food shortages, air pollution, water pollution, etc. send immediate signals to society of harm, which then trigger a negative feedback of society seeking to reduce the harm. In contrast, today’s great environmental crisis of climate change may cause some harm but there are generally long time delays between rising CO2 concentrations and damage to humans. The consequence of these delays are an absence of urgency; thus although 70% of Americans believe global warming is happening, only 40% think it will harm them (http://climatecommunication.yale.edu/visualizations-data/ycom-us-2016/). Secondly, unlike past environmental challenges, the Earth’s climate system is rife with positive feedback loops. In particular, as CO2 increases and the climate warms, that very warming can cause more CO2 release which further increases global warming, and then more CO2, and so on. Table 2 summarizes the best documented positive feedback loops for the Earth’s climate system. These feedbacks can be neatly categorized into carbon cycle, biogeochemical, biogeophysical, cloud, ice-albedo, and water vapor feedbacks. As important as it is to understand these feedbacks individually, it is even more essential to study the interactive nature of these feedbacks. Modeling studies show that when interactions among feedback loops are included, uncertainty increases dramatically and there is a heightened potential for perturbations to be magnified (e.g., Cox, Betts, Jones, Spall, & Totterdell, 2000; Hajima, Tachiiri, Ito, & Kawamiya, 2014; Knutti & Rugenstein, 2015; Rosenfeld, Sherwood, Wood, & Donner, 2014). This produces a wide range of future scenarios. Positive feedbacks in the carbon cycle involves the enhancement of future carbon contributions to the atmosphere due to some initial increase in atmospheric CO2. This happens because as CO2 accumulates, it reduces the efficiency in which oceans and terrestrial ecosystems sequester carbon, which in return feeds back to exacerbate climate change (Friedlingstein et al., 2001). Warming can also increase the rate at which organic matter decays and carbon is released into the atmosphere, thereby causing more warming (Melillo et al., 2017). Increases in food shortages and lack of water is also of major concern when biogeophysical feedback mechanisms perpetuate drought conditions. The underlying mechanism here is that losses in vegetation increases the surface albedo, which suppresses rainfall, and thus enhances future vegetation loss and more suppression of rainfall—thereby initiating or prolonging a drought (Chamey, Stone, & Quirk, 1975). To top it off, overgrazing depletes the soil, leading to augmented vegetation loss (Anderies, Janssen, & Walker, 2002). Climate change often also increases the risk of forest fires, as a result of higher temperatures and persistent drought conditions. The expectation is that forest fires will become more frequent and severe with climate warming and drought (Scholze, Knorr, Arnell, & Prentice, 2006), a trend for which we have already seen evidence (Allen et al., 2010). Tragically, the increased severity and risk of Southern California wildfires recently predicted by climate scientists (Jin et al., 2015), was realized in December 2017, with the largest fire in the history of California (the “Thomas fire” that burned 282,000 acres, https://www.vox.com/2017/12/27/16822180/thomas-fire-california-largest-wildfire). This catastrophic fire embodies the sorts of positive feedbacks and interacting factors that could catch humanity off-guard and produce a true apocalyptic event. Record-breaking rains produced an extraordinary flush of new vegetation, that then dried out as record heat waves and dry conditions took hold, coupled with stronger than normal winds, and ignition. Of course the record-fire released CO2 into the atmosphere, thereby contributing to future warming. Out of all types of feedbacks, water vapor and the ice-albedo feedbacks are the most clearly understood mechanisms. Losses in reflective snow and ice cover drive up surface temperatures, leading to even more melting of snow and ice cover—this is known as the ice-albedo feedback (Curry, Schramm, & Ebert, 1995). As snow and ice continue to melt at a more rapid pace, millions of people may be displaced by flooding risks as a consequence of sea level rise near coastal communities (Biermann & Boas, 2010; Myers, 2002; Nicholls et al., 2011). The water vapor feedback operates when warmer atmospheric conditions strengthen the saturation vapor pressure, which creates a warming effect given water vapor’s strong greenhouse gas properties (Manabe & Wetherald, 1967). Global warming tends to increase cloud formation because warmer temperatures lead to more evaporation of water into the atmosphere, and warmer temperature also allows the atmosphere to hold more water. The key question is whether this increase in clouds associated with global warming will result in a positive feedback loop (more warming) or a negative feedback loop (less warming). For decades, scientists have sought to answer this question and understand the net role clouds play in future climate projections (Schneider et al., 2017). Clouds are complex because they both have a cooling (reflecting incoming solar radiation) and warming (absorbing incoming solar radiation) effect (Lashof, DeAngelo, Saleska, & Harte, 1997). The type of cloud, altitude, and optical properties combine to determine how these countervailing effects balance out. Although still under debate, it appears that in most circumstances the cloud feedback is likely positive (Boucher et al., 2013). For example, models and observations show that increasing greenhouse gas concentrations reduces the low-level cloud fraction in the Northeast Pacific at decadal time scales. This then has a positive feedback effect and enhances climate warming since less solar radiation is reflected by the atmosphere (Clement, Burgman, & Norris, 2009). The key lesson from the long list of potentially positive feedbacks and their interactions is that runaway climate change, and runaway perturbations have to be taken as a serious possibility. Table 2 is just a snapshot of the type of feedbacks that have been identified (see Supplementary material for a more thorough explanation of positive feedback loops). However, this list is not exhaustive and the possibility of undiscovered positive feedbacks portends even greater existential risks. The many environmental crises humankind has previously averted (famine, ozone depletion, London fog, water pollution, etc.) were averted because of political will based on solid scientific understanding. We cannot count on complete scientific understanding when it comes to positive feedback loops and climate change.

## \*\*Morale\*\*

#### Ukraine loses now, and Russia victory causes LIO collapse

Defeat causes:

-Collapses ICJ credibility

-Triggers EU and NATO shattering

-Cyberattacks

-European Prolif

Simon **Tisdall** is a foreign affairs commentator. He has been a foreign leader writer, foreign editor and US editor for the Guardian4-1-20**22**, "The awful truth is dawning: Putin may win in Ukraine. The result would be catastrophe," Guardian, <https://www.theguardian.com/world/2022/apr/24/the-awful-truth-is-dawning-putin-may-win-in-ukraine-the-result-would-be-catastrophe>

This gaping disconnect is doubly disturbing. It suggests lack of coordination between the UN chief and a permanent member of the UN security council on how best to proceed. It also [highlights a wider problem](https://carnegieeurope.eu/strategiceurope/86948): diverging, sometimes opposing, occasionally self-serving, approaches to the crisis by western leaders who have hitherto trumpeted their unity of purpose.

The outrage in western countries sparked by Putin’s 24 February invasion is starting to fade. Likewise the burst of optimism that followed Ukraine’s success in repelling the Russian advance around Kyiv. Now, as Moscow begins a huge, [slow-motion offensive](https://www.theguardian.com/world/2022/apr/21/ukraine-access-weapons-determine-fate-donbas-offensive) in the east, concern grows that this conflict has no end-point and that the enormous economic and human damage that results may be permanent – and global.

Johnson supports a free, independent Ukraine but, like other alliance leaders, appears to lack a thought-through, long-term plan to achieve it

Johnson, typically, is not looking much beyond the present moment. The UK and Nato, he said, would just “keep going with the strategy” of imposing sanctions on Russia and supplying weapons to Kyiv. Johnson supports a free, independent Ukraine but, like other alliance leaders, appears to lack a thought-through, long-term plan to achieve it. What if Ukrainian forces start losing? What if [the country is partitioned](https://www.thetimes.co.uk/article/ukraine-war-revitalised-russia-can-still-win-western-intelligence-warns-fvwc9cz0n), or nears collapse?

The price of failure – the true cost of a Putin victory – could be staggering. It is potentially unsupportable for fractious western democracies and poorer countries alike, beset by simultaneous post-pandemic security, energy, food, inflation and climate crises. Yet out of myopic self-interest over issues such as Russian oil and gas imports, and from [fear of wider escalation](https://www.theguardian.com/world/2022/apr/21/german-report-casts-doubt-on-scale-of-its-weapons-support-for-ukraine), western leaders duck the tough choices that could ensure Ukraine’s survival and help mitigate such ills.

The past week furnished a grim glimpse of the future that awaits if Putin is able to continue to wage war with impunity, commit more heinous crimes, threaten nuclear and chemical blackmail and trash the UN charter. Drastically downgrading its growth forecasts due to the conflict, the International Monetary Fund predicted global[economic fragmentation, rising debt and social unrest.](https://www.theguardian.com/business/2022/apr/19/imf-cuts-global-growth-forecast-over-ukraine-war)

David Malpass, head of the World Bank, said a “human catastrophe” loomed as an unprecedented, estimated [37% rise in food prices](https://www.bbc.co.uk/news/business-61171529), caused by war-related disruption to supplies, pushed millions into poverty, increased malnutrition, and reduced funding for education and healthcare for the least well-off.

More than 5 million people have fled Ukraine in two months, and more will follow, exacerbating an international migration emergency that extends from Afghanistan to the Sahel. In drought-hit east Africa, the World Food Programme says 20 million people [may face starvation](https://www.aljazeera.com/news/2022/4/19/20-million-risk-starvation-as-horn-of-africa-drought-worsens-un) this year. Putin’s war did not create the drought, but the UN warns it could hurt [efforts to reduce global heating](https://www.theguardian.com/environment/2022/mar/21/ukraine-war-threatens-global-heating-goals-warns-un-chief), thereby triggering further displacement and forced migration.

The broader, negative political impact of the war, should it rage on indefinitely, is almost incalculable. The UN’s future as an authoritative global forum, lawmaker and peacekeeper is in jeopardy, as more than [200 former officials warned Guterres](https://www.theguardian.com/world/2022/apr/19/antonio-guterres-urged-to-take-lead-in-securing-peace-in-ukraine-or-risk-future-of-un) last week. At risk, too, is the credibility of the international court of justice, whose [injunction to withdraw](https://www.theguardian.com/world/2022/mar/16/un-international-court-of-justice-orders-russia-to-halt-invasion-of-ukraine) was scorned by Putin, and the entire system of war crimes prosecutions.

In terms of democratic norms and human rights, the full or partial subjugation of Ukraine would spell disaster for the international rules-based order – and a triumph for autocrats everywhere. What message would it send, for example, to China over Taiwan, or indeed to Putin as he covets [the vulnerable Baltic republics](https://www.theguardian.com/world/2022/apr/11/nato-achilles-heel-alliance-conducts-war-games-nervous-lithuania)? [Islamist terrorists](https://www.thetimes.co.uk/article/isis-urges-jihadists-to-strike-europe-and-israel-while-west-is-distracted-by-ukraine-bz0sfpf0t) who now furtively plot to exploit the west’s Ukraine distraction would relish such a victory for violence.

Failure to stop the war, rescue Ukraine and punish Russia’s rogue regime to the fullest extent possible would come at an especially high price for Europe and the EU. In prospect is a second cold war with permanent [Nato bases on Russia’s borders](https://www.politico.eu/article/nato-jens-stoltenberg-military-presence-eastern-border-army-ukraine-russia-war/), massively increased defence spending, an accelerating nuclear arms race, unceasing cyber and information warfare, endemic energy shortages, rocketing living costs, and more French-style, Russian-backed rightwing populist extremism.

In short, the dawn of a new age of instability. Why on earth would politicians such as America’s Joe Biden, [Germany’s Olaf Scholz](https://www.theguardian.com/commentisfree/2022/apr/10/germany-role-against-delusional-putin), and France’s Emmanuel Macron tolerate so fraught and dangerous a future when, by taking a more robust stand now, they might prevent much of it from materialising? By supposedly avoiding risks today, they ensure a much riskier tomorrow.

Sending weapons and best wishes is not enough. Conferring last week, [western leaders](https://www.nytimes.com/2022/04/21/us/politics/russia-ukraine-military-biden.html)debated providing security guarantees for Ukraine after the war. All well and good. But this war is happening now. Who will guarantee Ukraine’s survival in the possibly [decisive next few weeks](https://www.politico.eu/article/russia-new-offensive-west-allies-pledge-help-ukraine)? Who, if push comes to shove, will move beyond [training missions](https://www.theguardian.com/politics/2022/apr/21/uk-training-ukrainian-soldiers-weapons-equipment) and provide direct, in-country military support?

Let’s get real. For all its heroism and sacrifice, [Ukraine](https://www.theguardian.com/world/ukraine) may lose this fight. Dreadful though it sounds, Putin could win. If the west so abandons its principles and values to let that happen, the long-term price, for everyone, will be a whole new world of pain.

#### Successful US Morale Information warfare ends the war in Ukraine

Daniel **Karr et al**., Daniel Karr is an intelligence consultant at Recorded Future, an intelligence company, and a former intelligence analyst at the US Department of Defense. Jacob Ware is the research associate for counterterrorism at the Council on Foreign Relations and an adjunct professor at Georgetown University’s Edmund A. Walsh School of Foreign Service. 4-14-20**22**, "Hearts Not Minds: Morale and Inspiration in Insurgency and Territorial Defense," Modern War Institute at West Point , https://mwi.usma.edu/hearts-not-minds-morale-and-inspiration-in-insurgency-and-territorial-defense/

In war, morale always matters. The US military knows this better than most. In July 1965, Secretary of Defense Robert McNamara [requested](https://history.state.gov/historicaldocuments/frus1964-68v03/d67) additional deployments of US ground forces in Vietnam to “destroying” the morale of the Democratic Republic of Vietnam and the Viet Cong, including through the use of “informational actions.” While McNamara accurately predicted the impact of the information environment on the morale of insurgents and counterinsurgents alike, he overlooked how these deployments would affect the morale of US soldiers in Vietnam and the US public at home. Despite suffering hundreds of thousands of casualties, the North Vietnamese and Viet Cong forces held out, capturing Saigon a decade after McNamara’s request for additional forces. The relative willpower of US forces compared to that of the Viet Cong insurgents was one of [many reasons](https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG965.pdf) for this outcome.

Morale would similarly play a central role in US struggles in Afghanistan and Iraq. Although patriotic sentiment was widespread after the 9/11 attacks, US morale [waned](https://www.brookings.edu/blog/markaz/2015/06/29/iraq-afghanistan-and-the-u-s-militarys-morale-crisis/) over time, beaten down by improvised explosive devices, sniper attacks, and the knowledge that blood and sweat shed in conflicts in the Middle East and south Asia were yielding few strategic results. As one Taliban fighter is said to have [declared](https://www.newsweek.com/10-years-afghan-war-how-taliban-go-68223), “You have the watches. We have the time.” Both insurgent and counterinsurgent in Iraq and Afghanistan were well aware of one of the golden rules of guerrilla warfare, once [neatly summarized](https://www.foreignaffairs.com/articles/asia/1969-01-01/viet-nam-negotiations) in the Vietnam context by Henry Kissinger: “The guerrilla wins if he does not lose. The conventional army loses if it does not win.”

In these historical conflicts, the belligerent that successfully prioritized morale won. A wide-ranging RAND Corporation [report supports this conclusion, noting](https://www.rand.org/content/dam/rand/pubs/research_reports/RR2300/RR2341/RAND_RR2341.pdf) that “failure of will has signaled the ending of almost every military conflict in world history.” Morale, then, should be considered a critical factor as the Ukrainian crisis progresses. Predicting the outcome of this bloody conflict is a difficult task, but [one possible outcome is a protracted insurgency](https://www.washingtonpost.com/outlook/2022/03/05/russia-can-defeat-ukraine-it-cant-hold-territory/), with Russian occupiers facing a fierce Ukrainian resistance. The fate of such an insurgency would be determined by [many factors](https://www.rand.org/content/dam/rand/pubs/monographs/2010/RAND_MG965.pdf), including Russia’s [counterinsurgency strategy](https://mwi.usma.edu/dont-underestimate-the-bear-russia-is-one-of-the-worlds-most-effective-modern-counterinsurgents/), the intervention of outside powers, and the morale of both sides. On the latter point, in particular, Ukraine appears to hold a decisive advantage.

Morale in the Russia-Ukraine War

Morale has been an essential factor in the territorial defense of Ukraine. President Volodymyr Zelenskyy’s leadership has played a central role in keeping Ukrainian morale high; he has repeatedly rebuffed Russian disinformation through public appearances around Kyiv and refused offers of Western exfiltration, at one point [declaring](https://www.cnn.com/2022/02/26/europe/ukraine-zelensky-evacuation-intl/index.html), “I need ammunition, not a ride.” The media has regaled Western publics with accounts of heroism—such as the story of the troops at Snake Island who were killed (although that later proved untrue) after defying a Russian warship with the [proclamation](https://taskandpurpose.com/news/ukrainian-troops-snake-island-russian-warship/) “Russian warship, go fuck yourself”—as well as stories of plucky Ukrainian soldiers outwitting their far more powerful Russian counterparts, such as at [Kharkiv](https://www.nytimes.com/2022/03/03/us/politics/russia-ukraine-military.html), where Ukrainian ambushes repeatedly stalled a Russian advance. Civil society, meanwhile, has also stepped up, with one journalist [summarizing the atmosphere](https://coffeeordie.com/russian-invaders-ukraine-war/) as “not a climate of fear or pessimism. Rather, there was a clear strength forged by community action. A single purpose to which everyone had subscribed—victory. And in that common cause all individual anxieties seemed to fade.”

But morale will likely play an even more important role in the now-unraveling next phase, particularly if Russia ultimately succeeds in occupying parts of eastern Ukraine. Insurgency and guerrilla warfare are notoriously difficult to prosecute, and are sapping to energy and spirit—guerrillas will face food and supply shortages, adverse weather, and relentless manhunts. But the Ukrainian resistance will receive sustained financial and political support, including from [an international diaspora movement](https://www.cfr.org/event/home-and-abroad-public-forum-us-russia-relations). These are also excellent conditions for insurgency; [in the words of](https://www.csis.org/events/assessing-russian-military-campaign-ukraine) former US Under Secretary of Defense for Intelligence Michael Vickers, “Ukraine has all the conditions going for it” to wage an insurgent campaign. And Russia’s reaction—to escalate bombings against civilian infrastructure in an “[effort to break Ukrainian morale](https://twitter.com/DefenceHQ/status/1500357239428763649?cxt=HHwWgsCyxbi9q9IpAAAA)”—has only fed Ukrainian anger and patriotism. As Ben Connable notes in a [study of the will to fight on both sides](https://www.lawfareblog.com/ukrainian-and-russian-will-fight-early-war-assessment), Ukrainian morale may stay strong: “Given the existential nature of the Russian invasion and the demonstrated power of Ukrainian national identity, there is a good chance that the Ukrainians can sustain much of their will to fight through the invasion and into a long-term insurgency.”

Russian morale, meanwhile, appears to be flagging. The Defense Department has [observed](https://www.c-span.org/video/?518455-1/pentagon-ukraines-airspace-remains-contested) “indications” that Russian forces are suffering from low morale, which could be one factor [frustrating the Russian advance](https://www.nytimes.com/2022/03/03/us/politics/russia-ukraine-military.html?smid=tw-share) up to this point. There are reports of [Russian desertions](https://www.telegraph.co.uk/news/2022/03/04/russias-brave-deserters-part-noble-military-tradition/) and [sabotage of their own weaponry](https://www.nytimes.com/2022/03/01/world/europe/russia-troops-pentagon.html); many of Russia’s frontline soldiers [were not even told they were going to war](https://www.businessinsider.com/putin-lied-to-russian-soldiers-left-them-unprepared-attack-nyt-2022-3). Assassination attempts targeting Zelenskyy [have allegedly been foiled](https://www.foxnews.com/world/chechen-hit-squad-sent-murder-zelenskyy-eliminated) by Russia’s own intelligence agencies. And while Ukrainians have been galvanized into the streets by images of their battered, unshaven president defying an invading enemy, Russians [have taken to the streets](https://www.reuters.com/world/europe/more-than-64-people-detained-anti-war-protests-russia-protest-monitor-2022-03-06/) to protest the war.

Morale will grow increasingly important as the conflict drags on—and increasingly hard for Russia to sustain, as Russian soldiers continue to realize there will not be a quick return home, as their comrades head back in body bags, and as Russia’s bombing campaign [intensifies the resistance and global support for Ukraine](https://twitter.com/ColinPClarke/status/1499787082885210117).

Next Steps

Asymmetric wars are not just asymmetric in capability but also in stakes: the lesser force often faces an existential threat, and therefore summons a spirit that an invading army simply cannot match. Ukraine, as a nation seeing its right to self-determination in mortal danger, will always maintain that advantage against Moscow. But policymakers must also consider whether morale can be maintained, constructed, or cajoled.

Morale’s importance offers the West an opportunity to push the war in Ukraine’s favor. The information environment, and its intersection with cyber operations, could already be shaping morale in the ongoing conflict. So far, Russia’s use of cyber operations in its invasion of Ukraine has been limited. Despite the [discovery](https://www.cisa.gov/uscert/ncas/alerts/aa22-057a) of destructive malware targeting organizations in Ukraine in January and February, predictions that Russia would use highly destructive cyberattacks to aid in its military operations [have not come true](https://www.lawfareblog.com/cyber-realism-time-war). Rather than causing serious damage to Ukrainian critical infrastructure, cyber operations may leave a very different impact on the conflict: curbing the morale of Russian invaders. In the early days of the invasion, a Ukrainian newspaper published the personal information of 120,000 Russian troops, which was possibly obtained through cyber operations. Analysts quickly [pointed out](https://www.csoonline.com/article/3652370/purported-massive-leak-of-russian-soldiers-data-could-sink-morale-digital-security.html) how the exposure of this data could leave Russian soldiers vulnerable to targeted anti-Russian messaging, further eroding the morale of the invading forces. The leak came only days after the hacktivist group Anonymous [declared “cyber war”](https://twitter.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia) on Russia, subsequently conducted [denial-of-service attacks](https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia) against Russian government and state media websites, and [posted](https://twitter.com/Anonymous_Link/status/1498607316836536320) data allegedly belonging to the Russian Ministry of Economic Development on Twitter.

Anonymous and other groups’ hacktivism fits into the narrative that the heroic, less capable Ukrainian forces are locked in a noble struggle against the more powerful Russian aggressors. Information operations, possibly enabled by cyber operations, can further promote such narratives, complicating Russia’s counterinsurgency efforts.

As the United States [weighs](https://www.washingtonpost.com/national-security/2022/03/05/russia-ukraine-insurgency/) how to support Ukraine, it should recognize that the US military has already [created](https://www.c4isrnet.com/cyber/2021/12/29/new-us-army-cyber-unit-is-building-concepts-for-tactical-cyber-operations/) [multiple](https://www.airforcemag.com/16th-air-force-is-fully-up-and-running/) units capable of integrating and projecting military power across the information environment and the cyber domain. Should an insurgency emerge, the United States should deploy this capability to help maintain the conflict’s narrative in favor of Ukraine. Highlighting Russian atrocities, using cyber operations to expose the identities of those who target innocent civilians, and spreading messages about the heroism of the Ukrainian people are just a few options to bolster Ukrainian morale while curbing that of the Russian invaders. US military and covert operations to promote such narratives should be accompanied by complementary diplomatic messaging, as well as domestic political messaging from US leaders, to sustain the American public and private sectors’ support for pressuring Russia. Given Western unity in countering Russia up to this point, it is likely that US allies and partners will echo these messages.

Understanding the history of morale’s role in insurgencies is essential for analyzing the ongoing war in Ukraine and developing sound policy options for what could be a drawn-out conflict. But one thing seems clear: Russia will struggle to win its war in Ukraine if its troops do not want to be there.

#### Russia is using info warfare to destroy Ukrainian military readiness

-Authoritarian countries are using info warfare to spread HR violations

Zara **Abrams** has a B.A. in neuroscience and an M.A. in science journalism, both from USC., 6-1-20**22**, "The role of psychological warfare in the battle for Ukraine," American Psychological Association https://www.apa.org/monitor/2022/06/news-psychological-warfare

“The Ukrainians are fighting a 21st-century war, which is half on the internet,” said Stephan Lewandowsky, PhD, a professor of psychology at the University of Bristol who studies misinformation at the societal level. “That new approach has worked extremely well because it has preempted Russian attempts to rewrite history.”

Getting to the truth

Disinformation in war is nothing new—in fact, it’s a key part of the playbook. Leaders commonly inflate or fabricate information about everything from military might to supposed atrocities to confuse opponents or boost morale at home. Even Ukraine has [appeared to push](https://www.nytimes.com/2022/03/03/technology/ukraine-war-misinfo.html) some wartime narratives that may be false.

But with the rise of social media, propaganda can now be deployed on a much larger scale—and it has been used to garner support for genocide and other human rights violations, including those against the Uyghur population in China, the Rohingya in Myanmar, and Muslim populations in India. To describe the growing role of online media in political conflicts, Singer helped coin the term “LikeWar.”

“If you think of cyber war as the hacking of networks, LikeWar is its evil twin: the hacking of people on those networks, through our likes, shares, and sometimes lies,” said Singer, who is also a strategist and senior fellow at the nonpartisan public policy institute New America.

For years, Russia has been waging—and winning—a LikeWar against much of the world. The Kremlin has deployed tried-and-true psychological manipulation strategies via social and online media, including disparaging outgroups and rapid-fire lying, according to research by Jon Roozenbeek, PhD, a postdoctoral fellow in psychology at the University of Cambridge, who studies mis- and disinformation and media discourse in Ukraine.

Roozenbeek documented how the Kremlin stoked outgroup animosity toward Ukrainians and the Ukrainian government during the takeover of the Donetsk and Luhansk regions in eastern Ukraine, a tactic linked with high social media engagement (“[Media and Identity in Wartime Donbas, 2014–2017](https://www.repository.cam.ac.uk/handle/1810/305148),” University of Cambridge, 2019; Rathje, S., et al., [PNAS](https://www.pnas.org/doi/10.1073/pnas.2024292118), Vol. 118, No. 26, 2021).

Another ploy Russian President Vladimir Putin has used to great success is conspiracy “gish gallop,” or rapid-fire lying, said Roozenbeek, for instance around the Malaysian Airlines disaster of 2014. The Kremlin’s [constant stream of lies](https://www.irishtimes.com/opinion/combating-fake-news-the-21st-century-civic-duty-1.3739327)—that it was a Ukrainian attack, that all the passengers were dead before takeoff, that the pilot intentionally crashed the plane—is used to sow confusion and disillusionment (Paul, C., & Matthews, M., [RAND Corporation](https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf.) (PDF, 177KB), 2016).

“It’s a firehose of falsehoods that don’t even hang together,” Lewandowsky said. “They’re just saying anything, literally anything, to reinforce people’s belief that you can never get to the truth.”

The Russian leader also uses specific leadership and aggressive tactics to help justify violence, said Tin Nguyen, a research associate at the National Counterterrorism, Innovation, Technology, and Education Center who is completing his doctoral degree in industrial-organizational psychology at Penn State University (Lovelace, J. B., et al., [The Leadership Quarterly](https://doi.org/10.1016/j.leaqua.2018.08.001), Vol. 30, No. 1, 2019; James, L. R., et al., [Organizational Research Methods](https://doi.org/10.1177/1094428104272182), Vol. 8, No. 1, 2005). For example, Putin’s strategies include painting Ukraine and Western nations as evil and immoral and framing messages in terms of power dynamics. If Russia is merely a victim that other world powers are exploiting, the country has a justification for revenge.

#### Ukraine victory causes Russian collapse

Vasili **Rukhadze** is Visiting Lecturer of political science at the University of Pittsburgh, specializing in post-communist and post-Soviet politics and international relations. https://www.thedefensepost.com/2022/03/24/russia-wins-loses-ukraine/ 03-23-20**22**

Russian Defeat in Ukraine

On the other hand, a Russian defeat in Ukraine may lead to rapid defection from the regime, massive protests, and subsequent political chaos, which can contribute to Putin’s downfall.

The result can be the rise of another strongman with a more conciliatory stance towards the West or even the rise of a whole new democratic regime. It will depend on the potency of Russia’s grassroots democratic movements, which do not seem too strong at this stage.

Furthermore, the Russian defeat in Ukraine and unfolding economic crisis may even plunge the country into larger chaos and lead it to territorial disintegration, the outcome that took place in Russia twice in the 20th century: first after the 1917 Revolution and then as a result of the fall of the Soviet Union.

Such an outcome will have major geopolitical, economic, social, and cultural repercussions for Eurasia.  
**Ukraine has created energy for democratic movements but Russian victory causes populism globally**

[Andrei **Kozyrev**](https://twitter.com/andreivkozyrev) is an author and former politician who was the Russian Federation’s first foreign minister (1991–96). He was twice elected to the State Duma, where he served from 1994 to 2000. More recently, he was a distinguished fellow at the Wilson Center’s Kennan Institute (2016–17). His books include his 2020 memoir, The Firebird: The Elusive Fate of Russian Democracy. May 20**22** https://www.journalofdemocracy.org/why-putin-must-be-defeated/

Russia’s barbaric invasion of Ukraine constitutes a real and present danger to world peace and a rules-based order in Europe. But even more ominous than Russian war crimes are the neo-Stalinist ideas that the Kremlin is using to justify them. Putin’s regime is implementing these designs inside Russia and is offering them for export to the outside world in hopes of helming a new global Comintern. That new International—the Antidemocracy International—while detached from Soviet communism would still share similar aims, use similar tools to seize power, and be similarly fueled by anti-Western fury.

According to a recent Wall Street Journal [report](https://www.wsj.com/articles/vladimir-putins-20-year-march-to-war-in-ukraineand-how-the-west-mishandled-it-11648826461), German chancellor Angela Merkel (2005–21) realized at the November 2014 G-20 summit in Brisbane, Australia, that Russian president Vladimir Putin would never be open to a rapprochement with the West. During what was to have been a discussion about Ukraine—Russia had annexed Crimea earlier that year—Putin decried the decadence of democracies, citing the “spread of ‘gay culture’” as evidence. That assertion should sound painfully familiar to people in Russia and Germany, where in the 1930s such claims were used to justify the establishment of murderous dictatorships. Astoundingly, some [right-wing media commentators](https://www.forbes.com/sites/nicholasreimann/2022/02/23/these-conservatives-are-defending-russia-in-ukraine-crisis-and-trump-leads-the-way/?sh=49d2710b78cf)—rather than finding such views alarming, as anyone who had lived under Stalinism or fascism would have—have defended Putin and repeated his lies to their audiences.

Even more ominous was Putin’s statement in the same conversation with Merkel that “[Russia’s values were superior and diametrically opposed to Western decadence](https://www.wsj.com/articles/vladimir-putins-20-year-march-to-war-in-ukraineand-how-the-west-mishandled-it-11648826461).” It was Nazi Germany’s claim of racial superiority and the Stalinist Soviet Union’s claim of ideological superiority that underpinned their attacks on other nations. Poland, viewed as inferior by both, was invaded and carved up by the two powers during the Second World War in accordance with the infamous 1939 Molotov-Ribbentrop Pact, named for the Russian and German foreign ministers. The claim of superiority—of values and of national heritage (the Russian Empire and the Soviet Union)—is a key to understanding the war crimes and genocidal nature of Russia’s war on Ukraine today. To Putin, all means are justified in dealing with inferior people, who should be either forced into submission or eliminated. The appeasers in Europe, such Hungary’s Premier Viktor Orbán and Serbia’s President Aleksandar Vučić, should take note of Russia’s history and of the fact that Putin views Russia as superior not only to Ukraine but to the entire West.

At that same 2014 meeting, Putin, following Stalin, also made it clear that his contempt for the West extended beyond the cultural to the political. Leaders in democracies, in Putin’s view, will always be weak, hamstrung as they are by the need to win votes. Sergey Karaganov, a former top advisor to Putin and now honorary chair of the Moscow Council for Foreign and Defense Policy, like many Kremlin mouthpieces has stated Putin’s antidemocratic views even more plainly. In an April 2022 interview, [Karaganov said](https://www.newstatesman.com/world/europe/ukraine/2022/04/russia-cannot-afford-to-lose-so-we-need-a-kind-of-a-victory-sergey-karaganov-on-what-putin-wants) that Russia must win its war against Ukraine, but also made it clear that the real adversary in this war is the West, whose “moral foundation” is in question. Explaining the Kremlin’s strategic calculus, Karaganov said that “democracy in its present form in most European countries will not survive, because under circumstances of great tension [such as the covid-19 pandemic and the war in Ukraine], democracies always wither away or become autocratic. These changes are inevitable.” One has only to remember the British resistance to the German Blitz (1940–41) during World War II to see the obvious lie buried in his words.

Russia’s Never-Ending Battle

While Kremlin policies are no longer focused on achieving a communist victory over capitalism, they are still aimed at destroying Western democracy. A look back at the history of Russian-Western tensions shows how they escalated into political, cultural, and economic confrontation at the start of 2022, and why democracy has emerged as the key issue in that conflict.

The demise of the Soviet Union in 1991 raised hope that democracies could be established in Russia and Ukraine, along with other newly independent states. The West declared the end of the Cold War and welcomed those developments, but offered little practical support, particularly economic, to Russia’s reformers. (This must not be repeated with Ukraine today.) In the end, the old guard in Moscow allowed democratic and rebel nationalist forces to sweep away ascetic communism rather easily but were afraid of democracy. To preserve their dominance, the corrupt civil and military-security bureaucracies led by the KGB counterattacked the reformers. Most of all, the old guard worked to retain control of key natural-resource–based industries, especially oil. These holdovers were—and are—after power and money. They spent their spoils on luxuries in the democratic West and on propaganda machines and police to keep the population in check at home. This type of Russian state capitalism developed its hypocritical creed both as a cover for the corruption and plunder and as a message to the people not to protest.

I remember debating with old-guard front men during my time in government. Their line of argument sounded like an amalgam of primitive nationalism and religious and cultural clichés. The Bolsheviks, they argued, first created the Soviet Union, a superpower, and then built the Cheka (the KGB’s predecessor) to guard the USSR from internal and external challenges. But the communists failed to recognize the flaw in their ideology: If you force people to make sacrifices to achieve the unattainable—paradise on earth—sooner or later, they will become frustrated and revolt. That is exactly what happened in the Soviet Union. Since the fall of communism, the Kremlin, my opponents insisted, should preach pravoslavie (orthodoxy), which promises paradise in heaven but requires sacrifices in the name of the Russian state—the fortress, defended by the Federal Security Bureau (the KGB’s successor) and army, that stands against the infidels of the decadent West, led by the United States. And now came their ace card: Whatever one thinks about friendship between the two, Russia simply cannot afford to lose the United States as a clear enemy in the eyes of the people, the army, and the government. It needs a common enemy to unite them.

This eclectic and false blend of religion and patriotism became the postcommunist surrogate for a state ideology. It is called Pravoslavny Chekism, as odd as that might sound given that the Cheka from its inception repressed the church and religion. Pravoslavny Chekism and its proponents gradually found their way to President Boris Yeltsin (1991–99), who had played a key role in the demise of the Soviet Union and the emergence of the new Russian state in the early 1990s. A former provincial Communist Party apparatchik, he denounced communism and raised the banner of democracy in his fight for power. Yet he was hardly genuinely devoted to its implementation and, meeting resistance, began sliding back into more traditional ways of governance. Yeltsin’s choice of Vladimir Putin, a little-known St. Petersburg politician and former KGB officer, as his successor in 1999 was not accidental.

By that time, the reform process had slowed to a crawl, with the emerging free-market system leaving the Russian people with a huge bill and no means to pay it. The promised benefits of capitalism and democracy seemed nowhere in sight. At the same time, bureaucrats and crony entrepreneurs became millionaire oligarchs almost overnight. The prodemocracy forces lost credibility by continuing to support Yeltsin unconditionally and failing to act as an independent counterweight. As a result, democrats lost two free and fair parliamentary elections (in 1994 and 1995) to ultranationalists and neocommunists, who capitalized on the hardships wrought by the half-hearted reforms. None of the parties in parliament managed to provide an attractive alternative to the political and economic course—Pravoslavny Chekism and crony capitalism—ordained by Yeltsin and his bureaucracy.

Once in power, Putin and his team of former-KGB troopers doubled down on that course, solidifying control of the main industries and media. Parliament was eventually reduced to a stage show and rubber stamp for Putin’s policies, a sign that democracy was in danger. For Putin’s circle, the Cold War has never ended. The collapse of the Soviet Union was just one lost battle in an ongoing war with the West, which was to blame for Russia’s domestic failures both before and after the fall. While the prodemocracy press began withering from lack of financing under Yeltsin and especially Putin, ex-Soviet journalists at home and abroad were receiving KGB-arranged sponsorships from crony capitalists and quickly resumed churning out their traditional blame-the-West, fear-NATO headlines.

Once Putin had consolidated his grip on power in Russia, the Kremlin followed the Soviet example and went on provoking the West with daring statements, local hot wars, and disinformation and subversion campaigns. The feeble international response to their actions, especially in Crimea, the Donbas, and Syria, convinced the Kremlin that the United States and the West had, since declaring the arrival of the post–Cold War era, relaxed to the point of having lost the will to resist. Russia even tested the effectiveness of [threatening nuclear war](https://www.wilsoncenter.org/article/russias-nuclear-threats-recast-cold-war-dangers-delicate-balance-terror-revisited). Apparently, it does still work in deterring stronger Western support for Ukraine’s fight for freedom. The past seventy years of the nuclear era, however, had already proven that the only effective strategy for preventing such a war was to make unleashing it a suicidal act. Yet bowing to nuclear blackmail is also suicidal, as it opens the door for blackmailers to make endless demands.

Authoritarian Aggression Must Be Checked

The more determined democracies are to avoid war, the greater the risk that autocracies will wage it. The claim of military success helps autocrats to seize and hold power. Thus, the war in Ukraine will likely be a defining moment for Russia that will also have repercussions all over the world. If the West allows Putin to claim victory in Ukraine, antidemocracy populists everywhere will celebrate, believing that they can do whatever they want, and Putin will cement his dictatorship in Russia. Not only his acolytes in government but also a large part of the Russian populace will believe the Kremlin propaganda telling them that Putin’s leadership is amassing victories. If Russia wins this war, his agents of influence and useful idiots in the West will be singing his praises while police repression in Russia is ratcheted up even more—just to be on the safe side.

A few weeks after the beginning of the invasion, Putin pushed several laws through his puppet parliament and signed executive orders basically criminalizing all forms of dissent and the remnants of independent media. These moves, as Andrei Kolesnikov, a senior fellow at the now-shuttered Carnegie Moscow Center, [wrote](https://carnegieendowment.org/2022/04/06/how-silent-assent-made-bucha-possible-pub-86822), resemble the Nazification of German society (a process known as Gleichschaltung) after the Nazi’s seized power in 1933. Hitler sought to “coordinate” and control all political, social, cultural, and educational institutions in the name of national unity.

But Russia does not need the example of Nazi Germany, however striking the parallels may be, to serve as a roadmap. Russia has its own totalitarian legacy—Josef Stalin’s ruthless dictatorship, which Putin’s Russia is increasingly coming to resemble. For example, a new law passed in March makes public statements that contradict the Kremlin on the war in Ukraine punishable by up to fifteen years in prison. “The history of mass execution and political imprisonment in the Soviet era, and the denunciation of fellow citizens encouraged by the state . . . now looms over Russia’s deepening . . . repression,” [writes](https://www.nytimes.com/2022/04/09/world/europe/putin-russia-war-ukraine.html) Anton Troianovski. As in Soviet times, the more that ordinary people fear being suspected of disloyalty to the Kremlin, the more likely they will be to turn on each other. Repression and intimidation are key pillars of a totalitarian state that reduces citizens to an obedient population. In [the words of Bertrand Russell](https://books.google.com/books?id=qmFQlCiXZHIC&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q=herd&f=false), “collective fear stimulates herd instinct and tends to produce ferocity towards those who are not regarded as members of the herd.”

The collective fear of repression is a fierce enemy of democracy, but it is not the only driver of the herd mentality so necessary to totalitarianism. Fear of changing social dynamics—such as cultural pluralism, rapid technical development, and globalization—which many find especially hard to keep up with, also builds the herd. Putin’s base resides predominantly outside of Moscow and other major urban centers, is notably less educated, and comprises a mass of angry, struggling people. The older ones are nostalgic for the days when they were young and the grass was green, forgetting of course that they had frequently suffered under the old order. The younger ones are a mob of poorly educated malcontents looking for a strongman to transform them from the losers of modern society into its winners.

People who are afraid of change seek solace in scapegoating an “enemy,” simply defined as different, untraditional, or foreign. Putin’s propaganda succeeded in portraying Ukraine as an immediate enemy that can and should be trampled for breaking away from Mother Russia and for being the proxy of far greater and more distant adversaries—the United States and NATO. Defeating those enemies would help to keep the Russian herd under control and disprove the idea that Russia’s cousins next door could ever go it alone and choose democracy.

Putin’s full-scale aggression in Ukraine has galvanized the Antidemocracy International—from the Chinese Communist Party to the U.S. ultraright. Many [believed](https://www.washingtonpost.com/national-security/2022/05/21/russia-ukraine-victory/) that Russia would win quickly and easily. As Washington was warning of the massive Russian military buildup on the Ukrainian border, Chinese president Xi Jinping and Putin met on 4 February 2022, ahead of the Beijing Olympics. They signed a long communiqué outlining future areas of cooperation and claimed there were “[no limits](https://www.wsj.com/articles/russias-vladimir-putin-meets-with-chinese-leader-xi-jinping-in-beijing-11643966743)” to their commitments.

At about the same time, former U.S. president Donald Trump, still a leader of the Republican Party, [spoke admiringly of Putin](https://www.theguardian.com/us-news/2022/mar/26/donald-trump-georgia-republican-primary-rally) to a crowd of supporters, saying “they ask me, ‘Is Putin smart?’ Yes, Putin was smart. And I thought he was going to be negotiating. I said, ‘That’s a hell of a way to negotiate, put 200,000 soldiers on the border.’” In those awkwardly worded remarks one can recognize the Putinesque leitmotifs of mocking an elected leader for being weak and praising a dictator for using or threatening armed force, regardless of its being in violation of existing norms of civilized behavior. No wonder it came from a politician who tried to hold on to power despite having lost an election. In Russia, “smart Putin” has freed himself from such burdens by simply doctoring electoral results in his and his supporters’ favor.

Europe’s far right has had its own romance with the Russian autocrat for many years. Hungary’s Orbán has long been viewed as a potential leader of the new Antidemocracy International by [right-wing advocates](https://www.wsj.com/articles/hungary-budapest-viktor-orban-conservative-dreher-europe-eu-11649716947) in the United States. Orbán’s coalition won almost 53 percent of the vote in Hungary’s April 2022 election versus the opposition’s 34 percent. In Serbia, the unapologetically pro-Putin Aleksandar Vučić was reelected president in April 2022 by a sweeping margin. In France, Marine Le Pen, leader of the far-right National Rally, is literally [indebted to Putin](https://www.nytimes.com/2022/04/22/world/europe/le-pen-putin-france-election.html). Her party, denied financing from French banks, took out a US$12.2 million loan from a Russian bank in 2014. In the first round of France’s April 2022 presidential election, [Le Pen came in second to Emmanuel Macron for a second time](https://www.journalofdemocracy.org/a-dangerous-facade/), but by a significantly narrower margin than in 2017. (She was, however, soundly beaten in the runoff.)

European and U.S. right-wing populism is similar to that of Russia in the make-up of its political base and in its messaging. Trump, Orbán, and Le Pen voters tend to be less urban, have less formal education, and be more anxious about the rapidly changing cultural and economic landscapes. The rhetoric of these aspiring autocrats, like Putin’s, signals to their followers that the dizzying complexity of the modern world is actually nothing more than a battle between a good “us” and a bad “them,” whose ranks include foreigners and minorities as well as, in the case of Russia, the decadent West and liberals, who represent all the above. This is a sign that democracy is in danger.

The End of Ideology

Despite similarities, however, the leaders of the Antidemocracy International have no unifying or consistent set of ideas. They simply want power for themselves. It is only the rejection of democracy that brings them together. But it cannot mobilize a mass movement to the extent of self-destructive social engineering and world war in the way that messianic ideologies have. The two most portentous examples of such mass madness—Soviet communism and Nazi fascism—were defeated and discredited in the twentieth century. In the twenty-first century, Muslim fundamentalism, another potential stirrer of mass hyperdelirium, has failed to produce anything more than terrorism, thereby securing its worldwide rejection. There is an animated debate concerning the end of history, but the history of ideologies is over, at least for now.

What has emerged in their place? The now-universal ideas of a market economy and a publicly supported government. As it turns out, however, implementing them takes a lot of work. Democracy is not an ideology. But it is the best of all forms of government, all of which (including democracy) are imperfect. Autocracy, in contrast, is a bad form of government. Democracy—with its endless debates and elaborate procedures, and seemingly dominated by a globalized, overeducated elite—may appear too mundane and uninspiring to win over the doubters who are overwhelmed by modern life. They instead take refuge in dreams of reviving the past. Those dreams are what nurture and feed the populists and autocrats.

Yet for many, nothing is more inspiring than freedom. Thus the fearless Ukrainian president, Volodymyr Zelensky, was able to mobilize and unite his people to fight the Russian invaders, and has called for building Ukraine’s democracy and for [joining Europe](https://www.journalofdemocracy.org/ukraine-belongs-in-the-eu/). The international response to Putin’s aggression in Ukraine has also been encouraging. Both sides of the political aisle in the United States have supported providing assistance to Ukraine. A divided electorate in France banded together to defeat Le Pen, and after Orbán’s win at the polls, Hungary supported the EU’s decision to impose a [fifth set of sanctions](https://www.rferl.org/a/eu-sanctions-russia-ban-coal/31792723.html) on Russia. Although China and India abstained from condemning the Russian war, they have also refrained from providing Moscow with any meaningful assistance, especially military support. And even though they are clearly taking advantage of Russia’s self-imposed trading limits in the Western markets by buying Russian oil at huge discounts, Moscow’s old dream of creating an anti-Western axis with the two Asian giants remains unrealized. Putin’s friendship with Xi has proved far from limitless. Both Beijing and New Delhi understand the difference between words denouncing the existing world order and deeds able to damage it. In contrast to a declining Russia, China and India are rising and increasingly able to compete with the United State and Europe for influence on the international stage and a better place within the existing world order, amended to their taste but not destroyed.

Putin’s war on Ukraine has laid bare the critical need to defend and promote democracy in Europe, the United States, and elsewhere. But it has also demonstrated democracy’s amazing resilience. The brutality of the Russian war has reminded people everywhere of the existential danger that autocracy poses because it relies on violence at home and, in many cases, abroad. Prodemocracy forces in the West and beyond have mobilized once again. Democracy is still on the march, however treacherous the path ahead may be.

#### Russia is restraining the extent of its info warfare abilities but is brainwashing Ukrainians and Russians, current US action fails

[Alyssa **Demus**](https://www.rand.org/about/people/d/demus_alyssa.html) **and** [Christopher **Paul**](https://www.rand.org/about/people/p/paul_christopher.html) both study information warfare, influence, and other defense operations in the information environment at the nonprofit, nonpartisan RAND Don’t Sleep on Russian Information-War Capabilities ," Defense One, <https://www.defenseone.com/ideas/2022/04/dont-sleep-russian-information-war-capabilities/364050/> 04-05-20**22**

It certainly appears as though Russia’s opening portrait of the “special operation” as a quest to emancipate the people of Ukraine from [drug-addicted Nazi oppressors](https://www.businessinsider.com/putin-calls-ukraine-government-drug-addicts-neo-nazi-disinformation-2022-2) has fallen too far outside of global audiences’ existing belief systems to gain traction. At the highest levels of government, world leaders have [nearly unanimously](https://www.pbs.org/newshour/world/u-n-security-council-defeats-russia-humanitarian-resolution-on-ukraine-that-would-omit-fault) come out in support of Ukraine, even hurling a [tsunami of sanctions](https://graphics.reuters.com/UKRAINE-CRISIS/SANCTIONS/byvrjenzmve/) at Russia. On the other end of the spectrum, [blue-and-yellow flags](https://www.nytimes.com/2022/03/03/us/ukraine-flag-sales.html) now dot American neighborhoods as symbols of solidarity for Ukraine. From this vantage point, Ukraine looks to have Russia beat. But this is only part of the story.

Instead of fixating on Russia’s missteps, policymakers and analysts would benefit from studying Ukraine’s sophisticated information campaign while bearing in mind that Russia retains significant [information warfare capabilities](https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/) and [a willingness to use them](https://www.bbc.com/news/technology-60796079). Moreover, Russia is endowed with several related advantages such as a robust state-backed media apparatus, an increasingly hermetic [PB1] domestic information space, and the capacity for [wholly manufactured yarns or deliberately misrepresented half-truths](https://www.rand.org/pubs/perspectives/PE198.html). In fact, we see evidence of these capabilities, advantages, and this willingness working on some of Russia’s target audiences. In Russia and small pockets of eastern Ukraine, [anecdotal reporting](https://www.newsweek.com/russian-journalist-says-some-believe-country-fighting-hitler-ukraine-1686077) indicates that some audiences are buying the Kremlin line. [Stories](https://www.nytimes.com/2022/03/06/world/europe/ukraine-russia-families.html) of Russians refusing to believe their Ukrainian family members’ own harrowing [personal accounts of the war](https://www.bbc.com/news/world-europe-60600487) have surfaced.

Kyiv restaurateur Misha Katsurin, who posted on Instagram about his father’s refusal to acknowledge Russia’s role as the aggressor, received an outpouring of support in the form of [135,000 likes and shares](https://www.yahoo.com/entertainment/didn-t-believe-ukrainian-launches-230750845.html), and hundreds of comments by people with similar experiences. Katsurin has since established a site, [Papa pover](https://papapover.com/en/) (“Dad, believe”) designed to help Ukrainians engage family members in Russia who believe the Kremlin’s stories. The site has gathered a catalogue of disinformation narratives and suggestions about scripted responses.

In Russia, the de-Nazification narrative [is not new](https://www.theguardian.com/world/2022/mar/04/russian-soldiers-ukraine-anger-duped-into-war). Talking heads on Russian state-operated TV—which [62 percent of Russians rely on for news](https://www.levada.ru/2021/08/05/rossijskij-medialandshaft-2021/), according to recent polling—have spent the past eight years [fearmongering](https://russian.rt.com/inotv/2014-03-07/Nacisti-v-Kieve-sovershenno-ne) about this supposed [threat](https://www.npr.org/sections/parallels/2014/05/03/309006428/russia-condemns-ukraine-with-comparisons-to-nazis). Years-[long exposure](https://cognitiveresearchjournal.springeropen.com/articles/10.1186/s41235-021-00301-5) to such narratives can have a profound and durable [effect on one’s perceptions](https://www.jstor.org/stable/20445414?seq=1) and beliefs. It’s the first-mover advantage, reinforced by [repetition and familiarity](https://www.rand.org/pubs/perspectives/PE198.html). In fact, [58 percent of Russians](https://www.atlanticcouncil.org/blogs/ukrainealert/not-just-putin-most-russians-support-the-war-in-ukraine/) polled between February 28 and March 3 indicated approval for the invasion of Ukraine. This suggests that attempts to message to, influence, and/or mobilize Russian military personnel or the broader public may fall on deaf ears for much of this audience.

The claims to be rooting out supposed Nazis are but one element of Russia’s broader information campaign. Perhaps recognizing the failure of these early narratives to take root among global publics, the Kremlin has pivoted to manufacturing conspiracies on Ukrainian chemical, biological, and nuclear weapons programs. Though similarly far-fetched on their face, these stories are at least plausible, in that most industrial countries have chemical production and laboratories, and Ukraine has a history of [weapons manufacture](https://carnegieendowment.org/2014/07/30/saving-ukraine-s-defense-industry-pub-56282) dating back to the Soviet era. What’s more, the believability of this narrative is aided by the fact that it is rooted in a kernel of truth: In early March, a U.S. authority figure, Under Secretary of State Victoria Nuland, [confirmed](https://www.c-span.org/video/?518355-1/secretary-state-political-affairs-testifies-ukraine) to the Senate Foreign Relations Committee that Ukraine is home to biological research facilities, a fact which Russia has [latched onto and distorted](https://ria.ru/20220311/laboratorii-1777710523.html).

More concerning for U.S. policymakers is the fact that these narratives and others propagated by Russian officials and their proxies appear to be [gaining some traction](https://foreignpolicy.com/2022/03/10/bioweapons-ukraine-russia-disinformation/) among segments of the U.S. public. If Russia’s past propensity to [target American audiences](https://www.dni.gov/files/documents/ICA_2017_01.pdf) is any indication, more disinformation and propaganda of this nature is likely forthcoming. And Russia possesses other instruments in its informational toolkit. Within Russia, for instance, the Kremlin has tightened its grip on information with the implementation of a sweeping set of new restrictions on [journalism](https://www.amnesty.org/en/latest/news/2022/03/russia-kremlins-ruthless-crackdown-stifles-independent-journalism-and-anti-war-movement/) and [social media](https://www.npr.org/2022/03/07/1085025672/russia-social-media-ban). Meanwhile, President Biden has recently warned the nation against the increasing [likelihood of Russian cyberattacks](https://www.nbcnews.com/politics/joe-biden/evolving-intelligence-suggests-russia-may-target-us-businesses-cyberat-rcna20921). Moreover, this first month of the war in Ukraine has [demonstrated](https://www.rferl.org/a/ukraine-invasion-russia-fake-pretext/31685484.html) Russia’s willingness to use [false-flag operations](https://foreignpolicy.com/2022/02/04/false-flag-invasions-are-a-russian-specialty/) and various other [instruments of subversion](https://www.rand.org/pubs/perspectives/PE331.html) in service of political and military ends.

For its part, the evidence so far suggests that the Ukrainian government has mounted a stunningly sophisticated informational campaign in an effort to shape global opinions, to rouse domestic morale, and to persuade Russian soldiers to lay down their arms. Aided by the U.S. intelligence community’s exposure of Kremlin machinations and the introduction of [unprecedented intelligence sharing practices](https://warontherocks.com/2022/03/intelligence-disclosures-in-the-ukraine-crisis-and-beyond/), officials in Kyiv have mounted a coordinated yet agile, high-volume, multi-platform information effort. In the first moments of the conflict, Zelensky deftly [set the narrative](https://twitter.com/zelenskyyua/status/1496787304811315202?lang=en) in the informational battlespace, hijacking and inverting Moscow’s attempts to paint the authorities in Kyiv as fascists—instead casting the Kremlin as Nazis by tapping into deeply rooted historical memories of the Second World War.

From compelling captured-soldier videos, to social media posts targeting Russian troops, to the daily video updates from officials in Kyiv demonstrating continuity of government, to Zelensky’s tailored remarks to legislators, the Ukrainian leadership has used the information environment to its advantage. U.S. analysts, scholars, and practitioners of influence and information campaigns would benefit from monitoring, dissecting, and learning from Ukrainian information efforts.

The Ukrainian government’s information campaign over the past five weeks offers another important dimension to this lesson: that sophisticated information capabilities are not built in a day but honed over time. In 2014, Kyiv’s messaging in the wake of Russia’s annexation of Crimea and incursions into in the Donbas was [incongruous and slow](https://www.rand.org/pubs/research_reports/RR4373z1.html). [Officials reported divergent casualty figures](https://www.rand.org/pubs/research_reports/RR4373z1.html), which Russian actors exploited in their messaging as evidence of the incompetence of authorities in Kyiv. Since then, Ukraine has invested in and [retooled](https://foreignpolicy.com/2021/02/12/ukraine-volodymyr-zelensky-russia-propaganda-media-medvedchuk-euromaidan-kremlin-hybrid-war/) its approach to the informational aspects of crisis and conflict ([in some cases](https://www.wilsoncenter.org/blog-post/tug-war-ukraines-information-space-media-bans-versus-freedom-speech) drawing criticism), resulting in the robust capability we’re witnessing today.

The U.S. has allowed its information warfare and influence capabilities to atrophy before, particularly in periods of relative peace following [World War II](https://ahec.armywarcollege.edu/documents/A_Return_to_Information_Warfare.pdf) and fall of the Iron Curtain. There are several reasons for this neglect. First, those in the U.S. government responsible for information and influence activities have long been entrenched in [lexical and sectarian disputes](https://www.rand.org/blog/2019/03/is-it-time-to-abandon-the-term-information-operations.html). Put simply, there is little agreement on what to call information activities and who is responsible for them. Relatedly, the U.S. government community responsible for information efforts has also suffered from an optics problem.

In the wake of WWII, previously accepted terms of art including “propaganda,” “information warfare,” and “psychological warfare,” and their associated activities [gained a reputation as unsavory](https://warontherocks.com/2019/06/the-united-states-needs-an-information-warfare-command-a-historical-examination/). What is more, informational activities do not fit neatly within any one DOD portfolio where a largely [kinetic-focused culture](https://www.defenseone.com/technology/2021/11/joint-chiefs-information-officer-us-behind-information-warfare-ai-can-help/186670/) has meant these capabilities are often treated as “an afterthought…laminated on to” existing plans, in the words of former Chairman of the Joint Chiefs of Staff Gen. Joseph Dunford, Jr. Lastly, the U.S. lacks a national-level information strategy and/or body to set guidance and serve as arbiter between the various entities with hands in this space.

Recently, leaders in the Defense Department and broader U.S. government [acknowledged](https://www.c4isrnet.com/information-warfare/2019/07/11/joint-chiefs-nominee-wants-to-boost-information-warfare/) the criticality of information in conflict and competition. In this vein, federal agencies and the armed services have taken steps to institutionalize this refocusing through the establishment of informationally-focused [organizations](https://sgp.fas.org/crs/row/IN10744.pdf), [units](https://www.c4isrnet.com/dod/air-force/2019/10/14/what-the-new-16th-air-force-means-for-information-warfare/), and [positions in leadership](https://www.c4isrnet.com/c2-comms/2018/05/18/marines-get-new-information-war-leader/https:/www.c4isrnet.com/c2-comms/2018/05/18/marines-get-new-information-war-leader/). Even so, recent research in this arena has indicated that these nascent efforts still have a [long way to go](https://www.rand.org/pubs/research_reports/RR4373z1.html). It would seem to be a mistake to take Russia’s recent blunders in the information space in Ukraine as reasons to deprioritize or reduce American investments in its informational capabilities.

#### Information is uniquely crucial to military morale, makes an information war the biggest threat.

**Childs 16**, Sean Childs Major Sean V. W. Childs is a serving member of the regular Australian Army. He holds a Bachelor of Science from Macquarie University and a Master of Arts (Strategy and Security) from the Australian Defence Force Academy. Prior to joining the Australian Defence Force in 2010, Sean was a video journalist and senior producer based in London covering global security conflicts for US-based The Associated Press Television News, a policy adviser for Free TV Australia and an account director with the media intelligence corporate, the iSentia Group.“Soldier Morale: Defending a Core Military Capability” Institute for Regional Security <https://www.jstor.org/stable/pdf/26465606.pdf?refreqid=excelsior%3A7f42224105cd423760bc254a143296ab&ab_segments=&origin=&acceptTC=>, Accessed 7-14-22, BVW-RB

Social media has and will continue to change the character of morale or the will to fight in the spectrum of modern conflict. More significantly, the West’s ‘rules-based’ democracies and their body politics’ will to uphold and defend international norms is being challenged by the proliferation of social media and its detribalising effect. What this means is that the role of the individual within the military institution and its use of social media is vital in order to defend the military capability of morale. Crucially, information as image and perception must be privileged above the twentieth-century’s mentality of information as data and commodity. Information is the resource for shaping perception and imagination, and is the most potent way of defending and strengthening morale.

#### Authoritarian states will take advantage of social media as a means to deck Soldier morale – Daesh proves.

**Childs 16**, Sean Childs Major Sean V. W. Childs is a serving member of the regular Australian Army. He holds a Bachelor of Science from Macquarie University and a Master of Arts (Strategy and Security) from the Australian Defence Force Academy. Prior to joining the Australian Defence Force in 2010, Sean was a video journalist and senior producer based in London covering global security conflicts for US-based The Associated Press Television News, a policy adviser for Free TV Australia and an account director with the media intelligence corporate, the iSentia Group.“Soldier Morale: Defending a Core Military Capability” Institute for Regional Security <https://www.jstor.org/stable/pdf/26465606.pdf?refreqid=excelsior%3A7f42224105cd423760bc254a143296ab&ab_segments=&origin=&acceptTC=>, Accessed 7-14-22, BVW-RB

Australia and the West’s soldiers of today are part of a globalised information age which is resulting in the West’s continued detribalisation.34 In other words, by today’s soldiers accessing and processing knowledge from across the world they are facilitating for themselves more diverse views and opinions that challenge dominant Western paradigms and which serve to erode a consensus. Put another way, their actions potentially serve to erode the will to fight, a will which relies on a “sense of identity, belonging and cause”.35 Quite simply, the already dynamic process of human relations and discourse is becoming even more dynamic. Daesh, seizing on the phenomenon, is making expert use of social media in its propaganda efforts by using it as an **information weapon**, and in the realm of stated war aims, social media is extenuating the strategic debate. The main allegation commentators level against the international coalition’s fight against Daesh in Iraq and Syria is its lack of strategy or, to put it another way, the purpose of its stated war aims. This is in the context of perceived previous politicomilitary failures in the Middle East, which many argue have resulted in the rise of Daesh. In a theoretical sense, what this means is that an already detribalising West along with its soldiers are afforded access via social media to an ever expanding, dissenting discourse which serves to lower morale. The important effect social media has here stems from the realm of memory studies and the way in which meaning is created. Put simply, meaning is created in the space between history and imagination, which in the present spectrum of modern conflict is a recipe for a decrease in the West’s will to fight for their ideals and values. In other words, the history of past failures coupled with proliferated online content makes for the questioning of the ends and a greater potential for dissent, with all of its attendant consequences. For example, the potential drop in voluntary military recruitment numbers and increase in military separations (people quitting or worse, disserting). Social media’s detribalising effect in the spectrum of modern conflict certainly requires further research. Turning to morale’s exogenous situational factor one can argue that in the spectrum of modern conflict social media has the greatest practical impact. Well before the notion of social media was fathomable, David Galula, a leading military and academic figure of counterinsurgency warfare, provided a prescient warning in 1968 which typifies the threat to morale posed by Daesh’s use of social media today when he said, “the insurgent [is] judged by what he promises, not by what he does ... the counterinsurgent [is] judged on what he does, not on what he says”.36 Certainly the increase in the amount of information available is synonymous with the information age and social media. Certainly also the quality and authenticity of much of that information is questionable—all of which feeds the potentiality of rumour and friction in the context of success and failure. From the Australian Defence Force’s force protection perspective, two practical examples of social media’s likely impact on the morale of the men and women of its Air Task Group (ATG) conducting combat operations against Daesh in Iraq and Syria are available. I say likely as this is an area also requiring further research. Force protection relates to the identification of threats to the force, and the mitigation and control of those threats, which is a process of risk management. In this sense then, it is not difficult to appreciate that defending morale falls within the remit of force protection. First, take the horrifically barbaric February 2015 burning-alive of the caged and conscious Jordanian pilot by Daesh in Syria, subsequently disseminated by social media and widely reported on by the Western media. That, more than likely, had a material impact on the ATG’s exogenous situational factor of morale. In an already heightened force protection state it is not hard to imagine that social media’s transmission of the act would have caused a high degree of increased ‘home-front’ friction for the families of the ATG’s aircrews. In other words, an increase in the ATG’s families’ associated levels of concern and worry. The impact too in turn potentially feeds back into morale’s political factor of the stated war aim, spurring the debate surrounding the question of ‘is this really worth risking lives for an apparently uncertain end?’ Daesh’s use of social media in this case, as with their media content from their victories in Mosul and Ramadi, is an example of degrading the West’s situational factor of morale by highlighting their perceived victory and the coalition’s failure. Separately, although related in the realm of morale, was Daesh’s so called ‘Hacking Division’s’ August 2015 publication via social media of a “hit list” containing, supposedly, around 1,400 peoples’ details, including mobile phone numbers, credit card details, online passwords and private emails. Of those 1,400 the Australian Government confirmed the leak included the personal information of Australian Defence Force (ADF) employees.37 If the ATG and their families were not already overly apprehensive, one imagines their perception of Daesh’s domestic threat and potential reach increased somewhat if not dramatically. How does the ADF Presently Defend and How Might It Better Defend against Social Media’s Threat to Morale? From a force protection perspective, the ADF has measures in place to defend against social media’s threat to morale. Personnel are educated on the use of social media and on what personal security measures should be followed and what operational security (OPSEC) measures must be followed. These are important and necessary requirements for defending the military capability of morale. From a technical perspective, however, there is not a lot else one may implement short of banning social media’s use,38 which like our existing approach would fall within the realm of information as data and commodity.39 Put another way, this relates to the military’s traditional approach to OPSEC and “the information security triad of confidentiality, integrity and availability”.40 The important point here is that that approach, although important, fails to acknowledge the greater power of information as image and perception in the world of social media.41 Information as image and perception means information must be seen as a resource for shaping perception and imagination, which in turn is a more potent way of defending and, more importantly, strengthening morale.42 In the realm of modern conflict, social media and morale; attack is the best form of defence. Rather than being overly shielding we must facilitate and encourage soldiers to take up social media and get deep into the discourse it richly enables. Soldiers must go ‘waist-deep’, get personal, communicate the reality, create bonds, expand networks and proactively contribute to the collective shaping of perception and image. Our soldiers need to be outfront. With clarity, simplicity, common intelligibility and realistic interpretation,43 their authentic first-hand social media content should evoke identities and perceptions that create meanings, which in turn serve to boost morale. Such an approach’s strength lies in the content’s authenticity. In this way, akin to a constructivist approach within security studies, the will can be positively influenced through “behaviour [which] is always socially constructed, historically determined, and culturally contingent”.44 Conversely, a weakness of such an approach will stem from the tension between the opportunity for the soldier to engage independently and the strategic imperative dictated by policy, which is inherently political.Conclusion Social media has and will continue to change the character of morale or the will to fight in the spectrum of modern conflict. More significantly, the West’s ‘rules-based’ democracies and their body politics’ will to uphold and defend international norms is being challenged by the proliferation of social media and its detribalising effect. What this means is that the role of the individual within the military institution and its use of social media is vital in order to defend the military capability of morale. Crucially, information as image and perception must be privileged above the twentieth-century’s mentality of information as data and commodity. Information is the resource for shaping perception and imagination, and is the most potent way of defending and strengthening morale.

#### Social media scams extort the U.S. military, leads to soldiers sharing valuable information with adversaries.

**Lange** July 31, **2019** Katie Lange, Social Media/Public Affairs specialist, senior digital producer, writer and editor, temple university bachelors degree of arts. These social media scams affect the military, U.S. Department of Defense, <https://www.defense.gov/News/News-Stories/Article/Article/1921988/these-social-media-scams-affect-the-military/>, Accessed 7-11-22, BVW-RB

Nowadays, you have to be cautious of everything you do online. Scammers are always trying to get money, goods or services out of unsuspecting people — and military members are often targets. Here are some scams that have recently been affecting service members, Defense Department employees and their families. Romance Scams In April, Army Criminal Investigation Command put out a warning about romance scams in which online predators go on dating sites claiming to be deployed active-duty soldiers. It's a problem that's affecting all branches of service — not just the Army. CID said there have been hundreds of claims each month from people who said they've been scammed on legitimate dating apps and social media sites. According to the alleged victims, the scammers have asked for money for fake service-related needs such as transportation, communications fees, processing and medical fees — even marriage. CID said many of the victims have lost tens of thousands of dollars and likely won't get that money back. Remember: Service members and government employees DO NOT PAY to go on leave, have their personal effects sent home or fly back to the U.S. from an overseas assignment. Scammers will sometimes provide [false paperwork](https://www.cid.army.mil/romance-scam-examples.html) to make their case, but real service members make their own requests for time off. Also, any official military or government emails will end in .mil or .gov — not .com — so be suspicious if you get a message claiming to be from the military or government that doesn’t have one of those addresses. If you're worried about being scammed, know what [red flags to look for](https://www.cid.army.mil/romancescam.html). If you think you've been a victim, contact the [FBI Internet Crime Complaint Center](https://www.ic3.gov/default.aspx) and the [Federal Trade Commission](https://www.ftc.gov/). DOD officials said task forces are working to deal with the growing problem, but the scammers are often from African nations and are using cyber cafes with untraceable email addresses, then routing their accounts across the world to make them incredibly difficult to trace. So be vigilant! 'Sextortion' Sexual extortion — known as "sextortion" — is when a service member is seduced into sexual activities online that are unknowingly recorded and used against them for money or goods. Often, if a victim caves on a demand, the scammer will just likely demand more.Service members [Who] are attractive targets for these scammers for a few reasons: They're often young men who are away from home and have an online presence. They have a steady income and are often more financially stable than civilians. Because of their careers, they're held to a higher standard of conduct. Military members have security clearances and **know things** that might be **of interest to adversaries**. To avoid falling victim to sextortion, don't post or exchange compromising photos or videos with ANYONE online, and make sure your social media privacy settings limit the information outsiders can see — this includes advertising your affiliation with the military or government. Be careful when you're communicating with anyone you don't personally know online, and trust your instincts. If people seem suspicious, stop communicating with them. DOD officials said sextortion often goes unreported because many victims are embarrassed they fell for it. But it happens worldwide and across all ranks and services. Here's what you should do about it if it happens to you: Stop communicating with the scammer. Contact your command and your local CID office. Do NOT pay the perpetrator. Save all communications you had with that person. Service Member Impersonation Scams Scammers love to impersonate people of authority, and that includes service members. These people often steal the identity or profile images of a service member and use them to ask for money or make claims that involve the sale of vehicles, house rentals or other big-ticket items. These scammers often send the victim bogus information about the advertised product and ask for a wire transfer through a third party to finish the purchase, but there’s no product at the end of the transaction. Lately, fake profiles of high-ranking American military officials have been popping up on social media websites using photos and biographical information obtained from the internet. Scammers often replicate recent social media posts from official DOD accounts and interact with official accounts to increase the appearance of legitimacy. As an example, there are impersonator accounts on Facebook, Instagram and Twitter for Marine Corps Gen. Joe Dunford, the chairman of the Joint Chiefs of Staff. These accounts are also interacting with Joint Staff account followers in an effort to gain trust and elicit information. The only Joint Staff leader with an official social media presence is Senior Enlisted Advisor to the Chairman Army Command Sgt. Maj. John Wayne Troxell, who is listed as [@SEAC.JCS](https://www.facebook.com/SEAC.JCS) on Facebook and [@SEAC\_Troxell](https://twitter.com/SEAC_troxell) on Twitter.  Scammers are making these profiles to defraud potential victims. They claim to be high-ranking or well-placed government/military officials or the surviving spouse of former government leaders, then they promise big profits in exchange for help in moving large sums of money, oil or some other commodity. They offer to transfer significant amounts of money into the victim's bank account in exchange for a small fee. Scammers that receive payment are never heard from again.

## \*\*Baltics\*\*

### 2AC Baltic Add-On

#### Disinformation wrecks NATO decision-making and cohesion and makes a Baltic conflict inevitable – only a shared consensus on cyber response solves

Richard Sokolsky 17 - Richard Sokolsky focuses on U.S. policy for Russia (“The New NATO-Russia Military Balance: Implications for European Security,” Carnegie Endowment for International Peace, 03-13-17, [https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222, Accessed](https://carnegieendowment.org/2017/03/13/new-nato-russia-military-balance-implications-for-european-security-pub-68222,%20Accessed) 7-10-22, LASA-KK)

During the July 2016 NATO summit, the alliance and the EU issued an important joint declaration on a new strategic partnership that pledges to substantially improve cooperation between the two organizations to bolster alliance defenses against hybrid threats. The Baltic states are the first line of defense against Russian hybrid measures, yet their vulnerability to Russian unconventional warfare is the alliance’s Achilles’ heel. It remains unclear whether the Baltic states can make a sustained resource commitment to closing the many gaps in their defenses against Russia’s nonkinetic tools—such as those in their banking and financial sectors, mass communications, and domestic and foreign intelligence and law enforcement. Further, the states may not have the resources to increase investment in underdeveloped areas with large concentrations of ethnic Russians. The United States and the EU should boost funding for the Baltic countries to build their capacity to address their most critical vulnerabilities to Russian hybrid warfare. And NATO and the EU should avoid getting bogged down in theological and bureaucratic disputes over which organization should assume primary responsibility for this mission.

ENHANCE NATO PLANNING FOR HYBRID WARFARE

Russia’s hybrid warfare could pose a serious challenge to NATO’s existing planning and decisionmaking mechanisms. Should Moscow decide to take actions to undermine Baltic security, it is likely to engage in disinformation and deception to disguise both military and nonmilitary moves. NATO could therefore be confronted with ambiguous or uncertain indications of a possible Russian hybrid attack, creating the potential for disagreement within NATO councils on when and how the alliance should respond. A hasty decision on a forceful response based on incomplete and ambiguous information may make a crisis more difficult to manage; by the same token, a slow decision held hostage to NATO’s consensus-based, decisionmaking procedures could put Baltic security at risk. NATO decisionmaking could also be further complicated if one of the Baltic states, in the event of a provocation by little green men or some other activities in the gray zone, decides to trigger Article 5 by using lethal force to deal with the situation.

To deal with these potential dilemmas, the alliance needs to reach an internal consensus on a doctrine that reflects agreement on the following questions: What would be the trigger for a NATO nonkinetic response to Russia’s use of hybrid warfare against the Baltic states? Would the alliance need to respond collectively and militarily to more aggressive Russian information operations? What would be the costs and consequences if NATO failed to act under these circumstances? What if the source of the attack is unclear but is generally believed to be Russia?

New planning mechanisms need to be established within the alliance to determine military, operational, and capability requirements to deal with a range of Russian hybrid warfare contingencies. However, many of these needs fall outside NATO’s core competencies and will therefore require much closer NATO-EU cooperation, as well as stepped up efforts by the Baltic states. The alliance might also have to reevaluate its crisis management and decisionmaking procedures to ensure that they are structured for quick and effective responses to Russian activities that are truly hybrid in nature—in other words, those that combine low-intensity and high-intensity military moves.

#### Baltics invasion escalates quickly

Brent Eastwood 22, Now serving as 1945s New Defense and National Security Editor, Brent M. Eastwood, PhD, is the author of Humans, Machines, and Data: Future Trends in Warfare. He is an Emerging Threats expert and former U.S. Army Infantry officer, January 2022, "Forget Ukraine: Could Russia Invade And Conquer The Baltic States?" https://www.19fortyfive.com/2022/01/forget-ukraine-could-russia-invade-and-conquer-the-baltic-states/ //AShah

We’re Focused on Ukraine But Look Out For the Russian Threat to the Baltics: It was a shot heard around the world in the Russian military analysis community. A RAND Corporation simulated wargame in 2016 concluded that the Russian military could reach the suburbs of the Estonian and Latvian capitals of Tallinn and Riga in less than 60 hours. In the iterations of the exercise, the Estonians and Latvians would need at least seven brigades of troops that include at least three armored brigades to potentially fight the Russians to a standstill.

But it gets worse from here. In another RAND wargame in 2019, the players examined if NATO and Russia would use tactical nuclear weapons during a simulated war in the Baltic states (Estonia, Latvia, and Lithuania). The scenario also had Russian conventional forces over-running capitals in the Balkans and NATO having the last fail-safe option to use non-strategic nuclear weapons.

What Type of Warfare Could the Russians Use Against the Baltics?

A widespread fear is that the Kremlin could use hybrid warfare (conventional and unconventional aspects of power projection) again to annex parts of the Baltics, which would trigger Article V with NATO allies and would require a military response against the Russians from NATO members. A glance at a map will tell you that St. Petersburg is dangerously close to Tallinn, Estonia and Riga, Latvia. But according to General Valery Gerasimov, the Chief of the General Staff of the Armed Forces of Russia, the distinctions between offensive aspects of war and defensive aspects of war are blurring.

Under this Gerasimov Doctrine, the Kremlin then could engineer a Russian hybrid incursion of cyber and information warfare attacks against the Baltics, and these tactics could be made to be seen as a defensive operation. Since the Baltics have ethnic Russians as part of the population, Moscow could employ special operations forces as peacekeepers to protect compatriots. This could happen with an information warfare campaign that would increase the chances for protest and other domestic unrest with ethnic Russians as victims in the Baltics. Then a hybrid operation would ensue to protect ethnic Russians.

According to the two RAND sets of wargames, the Russians would then bring in the heavy armored and mechanized infantry units to “teach the Baltics a lesson.”

#### Baltic invasion goes nuclear.

Hal Brands 19, Hal Brands is a senior fellow at the American Enterprise Institute, where he studies US foreign policy and defense strategy. Concurrently, Dr. Brands is the Henry A. Kissinger Distinguished Professor of Global Affairs at the Johns Hopkins School of Advanced International Studies (SAIS). He is also a columnist for Bloomberg Opinion, November 2019, "How Russia Could Force a Nuclear War in the Baltics," https://www.aei.org/op-eds/how-russia-could-force-a-nuclear-war-in-the-baltics/ //AShah

Would the US fight a nuclear war to save Estonia? The question would probably strike most Americans as absurd. Certainly, almost no one was thinking about such a prospect when NATO expanded to include the Baltic states back in 2004.

Yet a series of reports by the nonpartisan RAND Corporation shows that the possibility of nuclear escalation in a conflict between the North Atlantic Treaty Organization and Russia over the Baltic region is higher than one might imagine. The best way of averting it? Invest more in the alliance’s conventional defense.

There was a time when it seemed quite normal to risk nuclear war over the sanctity of European frontiers. During the Cold War, NATO was outnumbered by Warsaw Pact forces, and it would have had great difficulty stopping a Soviet attack with conventional weapons. From the moment it was formed, NATO relied on the threat of nuclear escalation — whether rapid and spasmodic, or gradual and controlled — to maintain deterrence. American thinkers developed elaborate models and theories of deterrence. US and NATO forces regularly carried out exercises simulating the resort to nuclear weapons to make this strategy credible.

After the Cold War ended, the US and its allies had the luxury of thinking less about nuclear deterrence and war-fighting. Tensions with Russia receded and nuclear strategy came to seem like a relic of a bygone era. Yet today, with Russia rising again as a military threat, the grim logic of nuclear statecraft is returning.

The spike in tensions between Russia and the West over the past half-decade has revealed a basic problem: NATO doesn’t have the capability to prevent Russian forces from quickly overrunning Estonia, Latvia and Lithuania. Russian invaders would be at the gates of the Baltic capitals in two to three days; existing NATO forces in the region would be destroyed or swept aside. NATO could respond by mobilizing for a longer war to liberate the Baltic countries, but this would require a bloody, dangerous military campaign. Critically, that campaign would require striking targets — such as air defense systems — located within Russia itself, as well as suppressing Russian artillery, short-range missiles and other capabilities within the Kaliningrad enclave, which is situated behind NATO’s front lines.

Moreover, this sort of NATO counteroffensive is precisely the situation Russian nuclear doctrine seems meant to avert. Russian officials understand that their country would lose a long war against NATO. They are particularly alarmed at the possibility of NATO using its unmatched military capabilities to conduct conventional strikes within Russian borders. So the Kremlin has signaled that it might carry out limited nuclear strikes — perhaps a “demonstration strike” somewhere in the Atlantic, or against NATO forces in the theater — to force the alliance to make peace on Moscow’s terms. This concept is known as “escalate to de-escalate,” and there is a growing body of evidence that the Russians are serious about it.

A NATO-Russia war could thus go nuclear if Russia “escalates” to preserve the gains it has won early in the conflict. It could also go nuclear in a second, if somewhat less likely, way: If the U.S. and NATO initiate their own limited nuclear strikes against Russian forces to prevent Moscow from overrunning the Baltic allies in the first place. And even the limited use of nuclear weapons raises the question of further escalation: Would crossing the nuclear threshold lead, through deliberate choice or miscalculation, to a general nuclear war involving intercontinental ballistic missiles, strategic bombers and apocalyptic destruction?

#### (time depending) BUT building on existing NATO counter-disinformation ensures a stable presence in the Baltics that deters invasion.

Marta Kepe 17, Senior Defense Analyst at the RAND Corporation, M.A. in Security Studies from Georgetown University School of Foreign Service June 2017, "NATO: Prepared for Countering Disinformation Operations in the Baltic States?," <https://www.rand.org/blog/2017/06/nato-prepared-for-countering-disinformation-operations.htmls>, RMax

NATO plans to have around 3,000 troops in the Baltic states by the end of May as part of the Enhanced Forward Presence (EFP) — the largest reinforcement of NATO troops in the region for a generation. This represents a geopolitical shift of focus for NATO, from its earlier Central European theatre vis-à-vis the Soviet Union, further eastwards to the Baltic region vis-à-vis Russia. The aim is to demonstrate the “strength of the transatlantic bond,” reiterating to Russia the message that an attack on one ally would be considered an attack on the whole NATO alliance, an alliance which now includes the three ex-Soviet members of Lithuania, Latvia and Estonia. These NATO troops will be joining the US troops deployed there as part of Operation Atlantic Resolve that the Pentagon claimed demonstrates continued “US commitment to collective security” in Europe.

Strategic communications planning is part of preparing any military deployment; however, this deployment could face the Kremlin's sophisticated disinformation operations and propaganda in NATO territory. This represents the “geopolitics of disinformation,” currently being tracked by the Centre for European Policy Analysis (CEPA), who argue that such Russian “disinformation has specific geopolitical objectives;” namely to try to decrease public support for the NATO deployments in both the troop-sending states and the host nation countries.

The disinformation campaigns waged by Russia in the Baltic region may take different forms. NATO defence planners and decisionmakers need to prepare for “fake news” stories, which report fictional incidents and opinions. For example, a recent “fake news” story alleged that German soldiers deployed in Lithuania had raped a teenage girl. A Lithuanian police investigation determined that the report was false and that the email from which the story originated was “sent from a country outside the European Union.” Other deceptive reports include: (1) claims that bad behaviour by allied soldiers deployed in the region has become the “norm;” (2) reports that allied troops in Latvia would be permitted to roam the country with loaded weapons; and, (3) allegations that American soldiers in Latvia have been poisoned with mustard gas that have been sunk in the Baltic sea, the latter having been published on a Lithuanian news site after it was hacked. Specific disinformation was deployed “to rally the country's [Latvia's] Russian-speaking minority against NATO.” Other methods include using provocations to create incidents, such as the alleged attempts by a Russian TV crew to pay local youths to riot in Sweden. Actual incidents may also be used to give them political colour and portray the allied soldiers as disrespectful of the host Baltic states, their culture and people, as well as using compromising information published by the allied soldiers in social media. The risk of allied troops being provoked in order to discredit the alliance has also been raised by the head of the Estonian intelligence agency Estonian Information Board (EIB).

In this regard, the Baltic states have been heavily targeted by Russia for their eagerness to have allied forces on the ground and accused of “plotting an attack on Russia.” The Baltic states are, however, hardened and sensitised to information attacks, having learnt many lessons from their history of dealing with Soviet era Kremlin propaganda. Despite Russian disinformation, the populations of the Baltic states are very supportive of the allied presence. For example, a Lithuanian poll, carried out in December 2016, suggested that 81 per cent of respondents supported the permanent presence of NATO troops in Lithuania. Typical of Russian disinformation strategy was the rejection of the poll by the website newsbalt.ru (based in the Russian enclave of Kalingrad), which argued that the poll was skewed “to please” the Lithuanian Ministry of National Defence.

However, many of the troop-sending countries are less aware of the character of the Kremlin's information warfare. Information warfare is part of the Russian approach to non-linear warfare that encompasses old and new methods and tools. One such example is the Soviet “reflexive control” that aims to interfere with the decisionmaking processes of the adversary through disinformation and deception and the use of today's information technologies and media, not only in Russian but many other languages. It also encompasses “strategic masking,” which is spreading disinformation via media and manipulation of the adversary into believing reports of military movements. With the proliferation of information technologies and the amounts of private information that people make available online, national governments, international organisations and societies have become more vulnerable to information warfare.

It is clear that NATO needs to prepare for such disinformation campaigns. Some of the EFP framework nations have already announced that they are aware of the need to deal with these challenges. Most recently Gen. Jonathan Vance, the Canadian Chief of Defence Staff, announced that Canada will “take all the precautions” it can and noted that they “[…] have to take on a sophisticated, strategic communications role so that truth prevails.” Gen. Curtis Scaparotti, NATO's Supreme Allied Commander and the Commander of the U.S. European Command, has also suggested doing more to deal with Russian disinformation, telling the US Senate Armed Forces Committee that “I think we're focused on it, I don't think we've had enough of a response at this point.”

While the varied nature of disinformation warfare complicates preparation, NATO could pursue well-designed and holistic strategic communications approaches in the Baltic states, while also recognising the threat of disinformation beyond the region. Countering Russian disinformation requires rapid investigation of the information and its sources, establishing the facts and ensuring that the facts reach the same audiences that were targeted with the disinformation. However, reactive responses alone will likely be inadequate to deal with the threat. NATO could be more proactive and shape the information agenda with support and possibly led by the host nations. Soldiers and their commanders also could be educated on the nuances of preparing for and reacting to information warfare. The Allies might learn from Lithuania's “information influence identification and analysis ecosystem (PDF)” project that monitors and analyses physical and electronic information environments. Consulting with the NATO Strategic Communications (STRATCOM) Centre of Excellence, based in Latvia could also help, given its work on Russian information war and propaganda efforts elsewhere in the region.

In managing disinformation, allies will need therefore to strike the right balance between combating the disinformation threat and maintaining secrecy about military details. This balancing act could be a challenge for NATO and its allies. However, a proactive and open communications strategy could help to ensure that disinformation does not impact on military operations in the Baltic states. Finally, the efforts would likely need to move beyond a centralised strategic communications messaging plan and involve each and every soldier, and member of society. This could demand a higher level of information resilience, especially during the first months of the deployment.

To conclude, NATO alliance countries deploying in the Baltic states should be prepared to deal with increasing levels of disinformation, both proactively and reactively. A high level of preparation, including an open and robust communication strategy, could be crucial in tackling a sophisticated Russian disinformation campaign aimed to disrupt support for these deployments in the sending and host nations.

### Russian/NATO Cohesion Extensions

#### Russia will use information warfare to undermine NATO cohesion

Marcus Kolga 21 - Marcus Kolga is an analyst of foreign influence operations and disinformation (“Confusion, Destabilization and Chaos: Russia’s Hybrid Warfare Against Canada and its Allies,” Canadian Global Affairs Institute, October 2021, [https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4841/attachments/original/1635282447/Confusion\_Destabilization\_and\_Chaos\_Russias\_Hybrid\_Warfare\_against\_Canada\_and\_its\_Allies.pdf?1635282447, Accessed](https://d3n8a8pro7vhmx.cloudfront.net/cdfai/pages/4841/attachments/original/1635282447/Confusion_Destabilization_and_Chaos_Russias_Hybrid_Warfare_against_Canada_and_its_Allies.pdf?1635282447,%20Accessed) 07-10-2022, LASA-KK)

Operating in the shadows of the grey zone that lies between war and peace, Russia’s hybrid warfare aims to undermine targeted societies and democracies through a toxic mix of disinformation, cyber-attacks, transnational repression, economic pressure and the use of both regular and irregular military force. These operations are intended to support the Putin regime’s ultimate objectives: to erode Western alliances, re-consolidate Russia’s Soviet-era regional and global influence and remain in power as long as possible. The Russian government’s use of non-kinetic strategies and tactics to advance its interests and gain an advantage over its enemies is not new and can be traced back to the Soviet era. However, evolving technologies, shifting media landscapes and the growing emphasis placed on hybrid warfare in Russia’s modern military doctrine represent a persistent and expanding threat to liberal Western democracies and societies, including Canada. Vladimir Putin’s domestic political authority and legitimacy rely on his regime’s ability to demonstrateand project strength and control –both domestically and geopolitically. Putin’s guiding ambition has been to reverse what he believes is the “greatest geopolitical catastrophe” of the 20th century: the collapse of the Soviet Union. The Kremlin’s effort to restore Russia’s bygone czarist and Soviet imperial glory is as much a tactical domestic propaganda operation intended to support Putin’s effort to extend his reign to 2036, as it is meant to further enrich Russia’s corrupt oligarchs and kleptocrats. What has so far prevented Putin from fully realizing his goal is a strong and united transatlantic alliance –one that is committed to deterring Putin’s foreign aggression against allied Western democracies. Breaking down our alliances and the cohesion within them is a critical component of the Putin regime’s strategy to survive, compete, and when possible, dominate. Undermining and subverting the democratic processes and societies in NATO member states are part of this strategy. During his first 21 years in office, Putin has frequently challenged unity within the transatlantic community and the commitment to collective defence. Cyber-attacks, influence operations and information warfare are deployed to destabilize and undermine democratic processes and erode Western trust in media, government and societies in allied nations, and those like Ukraine and Georgia, which seek to join them.Russia’s invasion of Ukraine in 2014 and the ongoing conflict in Eastern Ukraine are extreme examples of Russian hybrid warfare. The mixture of irregularkinetic warfare with information and psychological warfare has resulted in a grinding, low-intensity conflict that is intended to perpetually sabotage Ukraine’s goal of becoming a full member of the transatlantic community.

#### Russian disinformation leads to indecision and divides NATO

David Grimes 22 - Grimes studies society’s understanding of science ("Russian Misinformation Seeks to Confound, Not Convince," Scientific American, 03-28-22, <https://www.scientificamerican.com/article/russian-misinformation-seeks-to-confound-not-convince>/, Accessed 07-13-22, LASA-KK)

As the Russia-Ukraine war intensifies, so too will the flow of disinformation. This is an age-old strategy Russia has long history of employing, and a playbook that others, most notably anti-vaccine activists, have borrowed from liberally. Yet, rather than focusing effort on convincing people of a falsehood, the Russian strategy takes a tack reminiscent of a strategy long employed by the tobacco industry: to sow so much doubt about what is true that it sends people into decision paralysis. Faced with a cacophony of wild and conflicting claims, people do nothing, unsure of what is right. Despite constituting only a small part of our media diet, disinformation campaigns, in our digital world, can be devastatingly effective. We are intrinsically biased towards information that is emotionally visceral. We afford more weight to content that frightens or outrages us, with the ability to induce anger serving as the single greatest predictor of whether content goes viral. This propels the most visceral, divisive narratives to the forefront of discourse, creating a sound and fury of passionately debated claims and counter claims. In that atmosphere, it becomes increasingly difficult to ascertain what to believe, and easy to abandon the task of discerning the truth. If we are not to fall victim to such rank dishonesty, it is crucial now that we question our sources more carefully than ever before. Indecision and distraction have long been central to Russia’s dezinformatsiya (disinformation) policy, a term Stalin himself is credited with coining. While an ancient concept, Russia had by the imperial age mastered dark obfuscation techniques refined for the era of mass communication. By the dawn of the Soviet empire, they realized this potential on an industrial scale, establishing the world's first office dedicated to disinformation in 1923. In the 1960s, the KGB covertly sponsored American fringe groups, amplifying conspiratorial narratives about everything from the assassination of president John F. Kennedy to water fluoridation. The goal, as KGB Major General Oleg Kalugin elucidated in 1998, was “not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America....”. Operation INFEKTION, a mid-1980s clandestine effort to spread the myth that AIDS was a CIA-designed bioweapon, was but one infamous exemplar. While utterly fictious, it resonated with communities ravaged by HIV and neglected by the callous indifference of the Reagan administration. Despite Russian intelligence taking responsibility for this lie in 1992, the legacy of AIDS denialism persists to this day worldwide.

## \*\*European Populism\*\*

### 2AC Populism Add-On

#### Russia is killing democracy and eroding trust in politicians in Europe through disinformation campaigns that undermine democratic institutions

Matt Apuzzo and Adam Satariano 19 – Matt Apuzzo teaches journalism at Georgetown University and wrote strories for the New York Times regarding the Justice Department’s Civil Rights efforts. Adam Satariano graduated from the University of California, Santa Cruz. He’s written stories for Bloomberg News and The New York Times on digital policy and the spread of disinformation and censorship by the government. ("Russia Is Targeting Europe’s Elections. So Are Far-Right Copycats. (Published 2019)," New York Times, 5-12-2019, https://www.nytimes.com/2019/05/12/world/europe/russian-propaganda-influence-campaign-european-elections-far-right.html, Accessed 7-10-2022, LASA-KS)

Less than two weeks before pivotal elections for the European Parliament, a constellation of websites and social media accounts linked to Russia or far-right groups is spreading disinformation, encouraging discord and amplifying distrust in the centrist parties that have governed for decades. European Union investigators, academics and advocacy groups say the new disinformation efforts share many of the same digital fingerprints or tactics used in previous Russian attacks, including the Kremlin’s interference in the 2016 U.S. presidential campaign. Fringe political commentary sites in Italy, for instance, bear the same electronic signatures as pro-Kremlin websites, while a pair of German political groups share servers used by the Russian hackers who attacked the Democratic National Committee. The activity offers fresh evidence that despite indictments, expulsions and recriminations, Russia remains undeterred in its campaign to widen political divisions and weaken Western institutions. Despite online policing efforts by American technology companies, it remains far easier to spread false information than to stop it. Russia remains a driving force, but researchers also discovered numerous copycats, particularly on the far right. Those groups often echo Kremlin talking points, making it difficult to discern the lines between Russian propaganda, far-right disinformation and genuine political debate. Investigators are confident, however, that networks of Facebook profiles, Twitter accounts, WhatsApp groups and websites are spreading false and divisive stories about the European Union, NATO, immigrants and more. Conspiracy theories are peddled freely, including that last month’s Notre-Dame fire was the work of Islamic terrorists, a spy agency, or an elite cabal that secretly runs the world. Often, these messages come directly from Russian news media and are repeated and amplified elsewhere. Others are more carefully cloaked: Facebook shuttered a pair of pages in Italy last week that were concealing far-right political messaging in what appeared to be lifestyle or sports sites unrelated to politics. “The goal here is bigger than any one election,” said Daniel Jones, a former F.B.I. analyst and Senate investigator whose nonprofit group, Advance Democracy, recently flagged a number of suspicious websites and social media accounts to law enforcement authorities. “It is to constantly divide, increase distrust and undermine our faith in institutions and democracy itself. They’re working to destroy everything that was built post-World War II.” The European Parliament elections, which will be held between May 23 and May 26, are regarded as a test of rising populism in the European Union. Populist leaders, many of them sympathetic to Russia, have loosely joined together in hopes of expanding their influence in the Parliament and, in turn, redirecting or subverting policymaking in Brussels. Intelligence officials have not publicly accused the Kremlin of backing specific candidates in Europe in the way that American authorities say that President Vladimir V. Putin sought to promote Donald J. Trump in 2016. But Mr. Putin has long sought to divide the European Union, and has supported populist movements that seek to undermine the bloc from within. It is nearly impossible to quantify the scale and resonance of the misinformation. Researchers say millions of people see the material. Investigators have found hundreds of Facebook and Twitter accounts, more than a thousand examples of WhatsApp messages sharing suspicious materials, and a hodgepodge of dodgy websites that launder varying degrees of misinformation — whether conspiracy theories or polarized slants on the news. A longstanding debate has been whether this material changes behavior or votes, especially as tech companies have worked to stamp it out. But security researchers suggest that swinging elections is a stretch goal for this kind of campaign, if that. The primary point is to muddle the conversation, make people question what is true, and erode trust. Russia dismisses accusations of meddling. “The election has yet to come, and we are already suspected of doing something wrong?” the Russian prime minister, Dmitri A. Medvedev, said in March. “Suspecting someone of an event that has not yet happened is a bunch of paranoid nonsense.” Distinguishing Russian interference from clickbait or sincere political outrage is difficult, even for intelligence services. The digital trail often winds up in one of the internet’s anonymized dead ends. But pro-Russian fingerprints exist.

#### Democratic backsliding from Russia’s influence campaign is weaking NATO --- allows Russia to exploit the weaknesses and further undermine the coherence of the alliance

David Deulofeu AntúNez 18 – AntúNez was a former staff writer for the International Affairs Review. He studies and writes about security policy. ("NATO’s Trojan Horse: How Democratic Deconsolidation and Populism are Weakening the Alliance — THE INTERNATIONAL AFFAIRS REVIEW," INTERNATIONAL AFFAIRS REVIEW, 11-29-2018, https://www.iar-gwu.org/blog/2018/11/29/natos-trojan-horse-how-democratic-deconsolidation-and-populism-are-weakening-the-alliance, Accessed 7-13-2022, LASA-KS)

The North Atlantic Treaty Organization (NATO) is facing an internal problem that coauld permanently weaken the Alliance. In recent years, we have seen the rise of a nationalist-populist wave in Europe and the United States: Viktor Orbán of Hungary, the Kaczynski in Poland, and President Donald Trump in America. This rise in illiberal world leaders has led to significant democratic backsliding in NATO countries, which pose a grave threat to NATO’s strength in the face of an aggressive and revisionist Russia. Democratic governance and strong institutions are as much a cornerstone of the Alliance as is collective defense. Article II of the North Atlantic Treaty (also known as the Washington Treaty) stresses the importance of “states’ promises to strengthen free institutions within their borders,” underscoring the vital democratic aspects of the alliance. Within NATO today, however, some states are shifting away from the core tenets of Article II and are actively conspiring to undermine the same institutional channels that brought them to power. These regressions of democracy create vulnerabilities that can be exploited by NATO adversaries, namely the Kremlin. In Hungary, Orbán’s increasingly authoritarian Fidesz government has taken an increasingly pro-Russia stance, doling out energy contracts to the country’s oligarchs and calling for Hungary to model itself a similarly to Russia’s illiberal state. In Turkey, the rise of Recep Tayyip Erdogan has resulted in members of the military being sacked and indiscriminate jailing of journalists and academics, while leaving no real opposition to his rule. This in turn has led to closer ties between Ankara and Moscow, especially in matters of defense and the ongoing Syrian civil war. Poland continues to see Russia as both an adversary and a threat; however, Poland’s judiciary reform has effectively turned the high court into a PiS puppet while media repression has simultaneously turned Poland into both a victim and purveyor of disinformation campaigns, further isolating it from its allies and European partners. Democratic backsliding and increased illiberal leaders in NATO countries have opened the door for Russia to engage in an influence campaign, and to pull those countries away from the Liberal Western Order the Alliance is founded on. Democratic backsliding weakens NATO internally by making cohesion, trust, and operations more difficult. Democracies tend to foster cooperation and trust; autocracies are always looking to blame “the other.” Within NATO, we are seeing bigger wedges being driven into member states, as illiberal regimes criticize their democratic allies, and democracies sanction authoritarian actions. Germany and the EU have become targets of the right-wing populist Prawo i Sprawiedliwość (PiS/Law and Justice) government in Poland. The current government has sought to expunge any guilt the “Polish Nation” incurred during the Second World War by engaging in an aggressive revisionist campaign aimed at denying Poland’s participation in Nazi death camps. Furthermore, Poland’s attempt to sack its Constitutional Court and replace 27 justices with PiS loyalists has alienated it from France, Germany, and the European Commission, which opened an Article 7 investigation last year into Poland’s actions and is currently threatening to take legal action against it. Likewise, Hungary has taken an antagonistic stance with EU members and their efforts to promote rule of law. Budapest has been in an entrenched battle against the EU, in what Orbán has called “liberal forces acting against Central and Eastern European countries,” while actively opposing and restraining EU laws on immigration, entertaining anti-Semitic conspiracy theories, and curtailing individual freedoms within Hungary’s borders. The right-wing populism of both Poland and Hungary, with their villainization of minorities, suppression of dissent, crackdown on civil society, and erosion of democratic norms and institutions, puts them at odds with their NATO allies and EU partners, fostering uncertainty and deep mistrust among them. Poland and Hungary are not the only NATO members breaking down trust. Traditional allies have taken an unprecedented stance on NATO, one which brings its members uncertainty and lack of trust. President Donald Trump has been a vociferous critic of the Alliance, admonishing members for failing to spend 2 percent of their GDP on defense while frequently highlighting the “lion’s share” the United States contributes. Trump has gone to the extent of questioning the alliance itself, asking, “What good is NATO…?” in a tweet. Apart from voicing criticism against NATO, Trump has repeatedly insulted NATO members and their leaders, while directing attention to closer relations with Russia, even though there have not been any significant changes in the Kremlin’s commitment to democracy, rule of law, or its meddling in internal processes of other nations. Russia continues to be a U.S. and NATO adversary. These stances from the current U.S. administration encourage anti-EU and anti-NATO rhetoric from other leaders, while at the same time erodes trust among its members and ultimately plays into the Kremlin’s intentions to destabilize the West and undermine the Alliance.

#### Democratic backsliding causes the replacement of democratic instutions and leaders with populist ones which increases the chances of nuclear dangers and hurts international order

Oliver Meier 21 – Oliver Meier is the ACA International Represenative and senior researcher with the Institute of Peace Research and Security Policy at the University of Hamburg. ("Upsetting the nuclear order: how the rise of nationalist populism increases nuclear dangers," Taylor & Francis, 12-16-2021, https://www.tandfonline.com/doi/full/10.1080/10736700.2020.1864932, Accessed 7-14-2022, LASA-KS)

Nationalist populists as leaders of states that possess nuclear weapons undermine the nuclear order and increase nuclear dangers in novel, significant, and persistent ways. Such leaders talk differently about nuclear weapons; they can put nuclear policy making and crisis management in disarray; and they can weaken international alliances and multilateral nuclear institutions. The rise of nationalist populists in nuclear-armed states, including some of the five nuclear-weapon states recognized under the 1968 Treaty on the Nonproliferation of Nuclear Weapons, shatters the presumed distinction between responsible and irresponsible nuclear powers and complicates attempts to heal rifts in the international order. Policies to wait out populists or to balance their influence in multilateral institutions seem to have had limited success. A sustainable strategy to deal with the challenge posed by populists would need to start by recognizing that we can no longer assume that nuclear weapons are safe in the hands of some states but not in others’. Introduction The rise of nationalist populists1 to power in nuclear-armed states and their allies is undermining the nuclear order and raising the risks of nuclear war. That populists such as Boris Johnson, Narendra Modi, Vladimir Putin, and Donald Trump were able to take charge of nuclear arsenals, including in some of the nuclear powers recognized under the 1968 Treaty on the Non-Proliferation of Nuclear Weapons (NPT), challenges the assumption that established nuclear-weapon states behave responsibly. Nationalist populism,2 understood as a nationalist, anti-elitist, illiberal, and anti-pluralist set of ideas and politics conducted in the supposed interests of “the people”—that is, the domestic constituencies of the nationalist-populist leaders—has been on the rise globally since the mid-2000s. It has come to include the leadership of a growing number of countries3 and has begun to influence the effectiveness of time-honored institutions of the nuclear order. We argue that this rise of nationalist populists and their foreign and defense policies weakens the nuclear order in novel, significant, and persistent ways. Three characteristics are typical of nationalist populists’ nuclear policies: they talk differently about nuclear weapons; they have a specific way of getting involved in national decision making on nuclear-weapon issues; and their approach to international alliances and institutions is unique. The fact that nationalist-populist leaders have assumed control over nuclear weapons in countries at the core of the nuclear order shatters the presumed distinction between “responsible” and “irresponsible” nuclear powers. These leaders threaten the nuclear order built on the principled acceptance of a logic of restraint by the nuclear-weapon states. Although it highlights the risks associated with populists’ control over nuclear weapons, this article does not aspire to a radical critique of the nuclear order.4 Our aim is to show that the rise of populists to the centers of power in nuclear-armed states challenges prevailing presumptions about nuclear risks and how they are to be managed. The view that a few responsible nuclear-armed states guard against irresponsible behavior by states mostly peripheral to the nuclear order is no longer defensible, if it ever was. Nationalist populists thus starkly expose the dangers intrinsically linked to nuclear weapons, regardless of regime type and the position of nuclear-weapon possessors in the international system. We understand nationalist populists to be leaders who claim to implement policies to defend the interests of their constituencies, which they brand as “the people,” against supposed foreign and internal elites in order to bolster national sovereignty. Nationalist-populist leaders who had or have nuclear weapons under their control include former US President Donald Trump, British Prime Minister Boris Johnson, Indian Prime Minister Narendra Modi, and Russian President Vladimir Putin.5 We concentrate our analysis on these four nationalist-populist leaders, who have shaped foreign and defense policies—and particularly nuclear-weapon policies—in key nuclear-possessor states.6 The 2016 election of Donald Trump, a populist by any measure, is of particular significance, since the United States has consistently been the state with the largest ability to uphold and strengthen the institutions and practices that underpin the nuclear order. Former Prime Minister Benjamin Netanyahu of Israel and Prime Minister Imran Khan of Pakistan are also nationalist populists. Israel, however, has a policy of nuclear opacity, under which it does not acknowledge possession of nuclear weapons.7 This made it impossible for Netanyahu to openly use nuclear weapons as a policy instrument in the same manner as other populists do. In Pakistan, the civilian leadership has only limited influence over nuclear-weapon policies because nuclear command and control rests with the armed forces.8 Chinese President Xi Jinping and North Korean leader Kim Jong Un are also often described as populists.9 Both leaders frequently use nationalist rhetoric, which resembles the populists’ style. However, we do not classify either as a nationalist populist because they do not rely on an internal in-group versus out-group dichotomy to justify their leadership. In autocratic regimes, such as those in China and North Korea, the leader holds absolute power and does not need to appeal to popular sovereignty or to employ other populist strategies. In France, the Front National, now Rassemblement National, is an influential nationalist-populist movement. Opposition leader Marine Le Pen has promised to “restore the full meaning of the ‘force de frappe’” and reinvigorate national sovereignty through nuclear deterrence.10 A populist turn in French nuclear policies therefore remains a distinct possibility. In two of the five nations that host US nuclear weapons under NATO nuclear-sharing arrangements, populists are in power (Turkey) or part of a government (Italy). In a third host nation, Belgium, a right-wing populist party has very recently been part of the government. In Germany, until the September 2021 parliamentary elections, a right-wing populist party was the strongest parliamentary opposition party.11 While populism, and particularly nationalist populism, has been on the rise in nuclear-armed states, three major developments in the background have reshaped the nuclear order. We understand this order to be characterized by the continuous search for accommodation between the goals of nuclear disarmament, on the one hand, and stability based on nuclear-deterrence relationships, on the other hand, through a policy of restraint and responsible behavior, particularly by the five nuclear-weapon states recognized under the NPT.12 First, a more multipolar logic has begun to replace the primarily bipolar Cold War nuclear structure. In particular, the rise of new challengers to US hegemony has produced new power constellations.13 Second, new actors, including transnational non-state groups, are challenging the predominance of governments and pose new threats, particularly if those actors strive to acquire weapons of mass destruction. Third, the emergence of new military technologies has weakened strategic stability. For example, the entanglement of novel conventional and nuclear warfighting capabilities threatens to destabilize long-standing mutual-deterrence relationships, particularly between Russia and the United States, on the one hand, and between China and the United States, on the other hand.14 All three developments, and the interrelations among them, already are increasing nuclear dangers and unsettling the existing nuclear-deterrence relationships. The rise of nationalist populism and populists to power is a recent fourth development that adds to and amplifies these risks. Our examination of the impact of the rise of nationalist populism on the nuclear order meshes with the attention given in academic literature to the role of individuals in nuclear policies. The recent shift toward the first image (that is, the analysis of international relations focusing on the impact of individual leaders as opposed to an analysis at the level of states or the international system)15 is associated with an investigation of how the perceptions and preferences of specific personality types have altered national nuclear policies and the nuclear order. We add to this literature by considering a specific type of leader, the nationalist populist, and his (rarely her) influence on nuclear issues. The role of populism in foreign and defense policy, and particularly on nuclear policies, is seldom treated as a distinct phenomenon. This research gap has not been filled by issue-, country-, or region-specific investigations of the causes and effects of populism, which are more interested in how individual leaders have addressed particular issues than in the broad implications of the rise of nationalist populism.16 Our conception of nationalist populism overlaps with Jacques Hymans’s description of the “oppositional nationalist.”17 Hymans makes a convincing case that this type of leader has a particular affinity for nuclear weapons. However, where Hymans is interested in how leadership traits influence the decision to acquire nuclear weapons, we focus on policies affecting established nuclear arsenals. There is also a difference in framing between our idea of nationalist populism and Hymans’s notion of national-identity conceptions. The concept of “nation” is central to both frames. Yet populists equate the nation with their core domestic constituencies (and perhaps their own selves), while oppositional nationalists mostly view the nation-state as an entity in relation to other nations. Both view politics as the manifestation of an us-versus-them struggle. But nationalist populists and oppositional nationalists have different notions of the “us” (the people/nation) and different concepts of “them” (elites, other people/other nations).18 In our analysis, the Trump administration receives more attention than other nationalist-populist leaderships. This imbalance reflects the extraordinary amount of writing on an atypical US president. A focus on Trump is justified, since the United States remains the most important actor in the nuclear order. Also, Trump is often described as a prototypical populist19 who has inspired others to follow his lead and has generally increased the impact of populists in other countries. With Trump now out of office, this is a good time to take stock of his administration’s impact on the nuclear order: “Trump’s presidency offers, for good or ill, an excellent laboratory to examine whether and to what extent the assumption of government power by populists translates into foreign policy change.”20 We also consider the roles of other nationalist-populist leaders within the nuclear order and offer some observations on the implications of the rise of this phenomenon for nuclear disarmament, arms control, and nonproliferation. We hope to provide a number of tentative arguments and conclusions about the distinct, dangerous, and often strange ways that populists are shaping the nuclear order. Populist foreign and defense policy To examine the influence of populism on foreign and defense policy, the idea of populism itself requires definition, or at least approximation. Populism is a fuzzy concept. At the most basic level, populists present themselves as atypical leaders from outside the establishment. Populists like to tell a story of how they are virtually predestined to represent and empower a silent and politically neglected majority (which they label as “the people”). But populism is neither a full-fledged political ideology nor simply a political or rhetorical style. It is rather a “thin-centered ideology.”21 Populism is inherently difficult to pin down, since populists want to maintain maximum flexibility to apply their ideas to, or combine them with, other ideologies—right, left, or drawing upon both—regardless of the underlying political system. The notion of a populist foreign and defense policy is equally hard to delineate. Leaders’ foreign policies reflect their personal characteristics and political behavior, how they interpret the world and their role in it, how they make decisions, and how they interact with others.22 As Daniel Byman and Kenneth Pollack state, “It is individuals who build the alliances, and create the threats that maintain or destroy balances of power.”23 Populist leadership is especially personalistic; a populist leader’s beliefs and decisions can be assumed to be more influential in shaping foreign and defense policies than those of other leaders. Nationalism, as one of the possible host ideologies of populism, adds another layer. Nationalist and populist discourses overlap; what the nation is to the nationalist, “the people” is to the populist. The concepts of sovereignty and self-determination drive both discourses, but they affect foreign and defense policies through different mechanisms. In principle, there is a clear delineation between a given nation and all other nations. The populists’ idea of “the people” is vaguer. Populists use this ambiguous construct to evoke a group (their “base”) within a polity, juxtaposing it with “elites” at the top. According to populists, these elites are outside the group of the “real” or “true” people. Populist politicians boast about not being part of the elite class (a claim that is rarely true, in economic or educational terms) and thus claim to speak and act in the name of the people from within their ranks, implying that only they can genuinely represent them.24 Nationalist populists not only claim to speak for “the people” but also presume to define the nation. They fuse inward-looking populist discourse with a more outward-oriented nationalist ideology. This shift in the frame of reference portrays the elites as depriving the people of their sovereignty both at home and abroad.25 As Jordan Kyle and Brett Meyer put it, “foreign policy is often collateral damage of populists’ divisive approach to domestic politics.”26 We identify the following characteristics of external policies pursued by nationalist populist leaderships: Polarization. “Us versus them” is the predominant discourse. Restraint, empathy, and compromise are anathema.27 Romanticizing of the historical past. Populists want to revive the “national missions” of their own countries.28 Personalistic leadership. Political authority rests primarily with a single person, often the head of a movement,29 rather than within structures and institutions. Foreign and defense policies are extensions of domestic policy debates. The leader’s political messaging is direct, with “the people,” often via social or new media, while ignoring established channels of interaction with the broader public.30 National sovereignty. Populists view alliances and international institutions as constraining the freedom of nation-states.31 The short-term, narrow interest of the nation is the sole yardstick of success.32 Iconoclasm. Populists want to dismantle international organizations, which they view as the instruments of circles of elites who support international cooperation and integration. They reject cultural and economic globalization and free trade.33 These criteria do not represent a comprehensive account of the nationalist-populist phenomenon, and the checklist is not exhaustive. Some of these traits could also apply to non-populist foreign and defense policies. Nevertheless, taken together, these features of the nationalist-populist approach to international policy issues capture a unique, identifiable phenomenon: if a leader walks like a populist, talks like a populist, and acts like a populist, then he or she most likely is a populist (see Figure 1). Here to stay: the proliferation of populism The rise of nationalist populists to power in nuclear-weapon states is a phenomenon worthy of in-depth analysis for three reasons. First, the development is of an unprecedented scale globally. A recent overview found that there are “more populist leaders and parties in power than at almost any time in history.”34 Individuals and their beliefs and preferences, along with external systemic factors, shape foreign-policy decisions and interactions among states. However, how and to what degree populists influence nuclear policies varies between countries. Populists have risen to power in democracies, electoral autocracies,35 and other hybrid regimes. Depending on the political system, their influence may be constrained by other branches of government and by actors, such as private companies, whose interests may be inconsistent with a populist agenda. Generally speaking, the individual leader has the greatest influence on a state’s decisions and behavior in personalistic systems. By contrast, the checks and balances of pluralistic systems often constrain democratically elected leaders. Even there, however, nationalist populists increase their influence by constantly chipping away at the core values, principles, and procedures of liberal democracy, such as separation of powers, rule of law, political representation, and individual rights and freedoms.36 Second, nationalist populists have risen to power in three of the five nuclear-weapon states. The significance of that development for the nuclear order is particularly great, since these five states bear a special responsibility for maintaining and improving that order and international peace generally.37 In their parallel role as the five permanent members of the UN Security Council, their consent is necessary for enforcement of compliance with the NPT and other multilateral regimes. Their willingness to forgo nuclear, biological, and chemical weapons, or their lack of willingness, sets examples for other, less influential states. In the past, Western leaders often dismissed populism as a problem of less developed countries.38 At the same time, nuclear establishments saw the peace movement and other grassroots movements as populist—that is, non-elite groups that were challenging elitist policies supposedly based on rationality and stability.39 To be sure, the time for finger pointing is over. “Populism has not just risen in emerging democracies with weaker political parties and institutions but in systemically important democracies with long institutional histories like the United States and India,” as Kyle and Meyer observe.40 Few if any states now appear to be immune to populist challenges. Consequently, the assumption that the established nuclear-weapon states can protect the nuclear order from less responsible challengers must be revised. Third, populism is here to stay. To be sure, populism is not a new phenomenon, and populists have challenged the nuclear order before in various ways.41 Today’s populism, additionally, is fueled by the perceived inability of states and institutions to attend to the political, economic, and cultural consequences of the global economic crisis of 2008, as well as the increase in xenophobia following the increase in conflict-induced flight and migration into Europe since 2015.42 In the context of “crises of political representation engendered by dislocations caused by globalization and other shifts in international politics” and as a “reaction to concurrent political and economic crises in a rapidly denationalized and deterritorialized world,”43 the rise of populism has been a reaction to perceived insecurity, inequality, depoliticization, and economic stagnation. As a result, a rise of illiberalism and a wave of autocratization can be observed.44 Nationalist populists have come to power in the shadow of the crisis of the liberal international order, benefiting from the crisis and perpetuating it. The impact of nationalist populism is going to stay with us, likely beyond the lifetime of individual nationalist-populist governments. That is partly because the leaders have begun to paralyze, reshape, and dismantle existing bureaucracies. Nationalist populists define themselves as being anti-elitist (even if they themselves are members of the elite). Once they occupy the seats of power, national populists co-opt, exchange, or sideline old elites. The resulting reshuffle in the foreign and defense apparatuses sometimes resembles a purge and can lead to dramatic discontinuities in expertise. It will take time to repair the damage done to governance structures and to heal the wounds caused by political polarization. In the nuclear world, this destabilization of institutions is particularly significant. The nationalist-populist assault weakens the influence of those who are supposed to act as “guardians of the arsenals.” The influence of nationalist-populist leaders on nuclear-weapon policies also has grown.45 When it comes to nuclear-weapon use, the dangers posed by nationalist populists are stark because in most nuclear-weapon states the head of state or government has the legal authority to order the use of nuclear weapons. But there are different shades of gray. In nuclear-armed states with presidential systems (France, Russia, and the United States), launch authority “clearly rests in the hands of one single person,” while in those with parliamentary systems (India, Israel, Pakistan, and the United Kingdom), “the decision to launch a nuclear strike would necessarily not be the sole authority of one individual, even if it is ‘legally’ (i.e. on paper).”46 Three ways populists change the nuclear order Against this background of the characteristics of populists’ foreign and defense policies and the diffusion of populism into nuclear powers’ decision-making centers, we describe three relevant causal mechanisms through which nationalist populists influence the nuclear order. First, nationalist populists have a different way of speaking. “[T]he specific style of rhetoric used by the populists involves adversarial, emotional, patriotic, and abrasive speech through which they connect with the discontented often via grassroots, community-oriented, communicative practices and spaces.”47 For nationalist populists, the domestic audience is the most important recipient of any messaging; everything is said with a communicative purpose to please “the people,” to secure their approval and votes and therefore to retain power. Second, nationalist populists have a particular way of making decisions, sometimes reflective of the fact that delineating “the people” from an “elite” is a constitutive element of populism. Whereas usually a small and closed group of experts and officials prepares and executes decisions in foreign and defense policy, the policy style of nationalist populists is a peculiar mix of laissez-faire on routine issues and very visible leadership when the stakes are high. As Kyle and Gultchin argue, populists seek to convince their supporters that they “see and acknowledge the crisis and that their strong leadership alone can fix it.”48 Third, nationalist populists have a distinct perspective on the international order. They view the world through a “great-power” lens that is consistent with the “realist” logic of foreign and defense policy. At the same time, nationalist populists reject the notion of an international order based on and shaped by bilateral and multilateral agreements and treaties. This is partly because the rise of nationalist populism “has brought a new persona to the global stage—the iconoclast. This deliberate rule breaker disrupts the practice of international relations, a system that depends upon consensus around norms.”49 Talking about nuclear weapons As Alexey Arbatov has observed, “when it comes to nuclear weapons, words are deeds.”50 This is because nuclear weapons have been exploded in war only twice. All other “uses” of nuclear weapons have been limited to verbal actions, policy documents, deployment, testing, and other actions short of direct hostile use.51 Usually, nuclear messaging is the outcome of a careful and deliberate process. For example, heads of state or government typically speak about nuclear arsenals and nuclear strategy on the basis of carefully scripted and meticulously reviewed statements. Exegesis of nuclear-policy documents and speeches is the preoccupation of many nuclear analysts, based on the assumption that, especially in the nuclear world, leaders and officials have thoroughly weighed and consciously selected their words. Nationalist populists, by contrast, often speak loosely about nuclear weapons, which complicates a “reading” of their statements.52 This concerns both style and substance, which coincide with their personalistic style of leadership53 and their desire to flout the rules of what they deride as “political correctness.”54 Donald Trump has again led the way—for example, through his excessive tweeting on nuclear-weapon issues.55 Other nationalist populists have also deviated from previous rhetorical styles by bragging about their nuclear weapons. In April 2019, shortly after an escalation of the Pulwama crisis between India and Pakistan had been averted, Indian Prime Minister Narendra Modi suggested that his country was ready to use nuclear weapons against Pakistan: “Every other day they used to say ‘we have nuclear button, we have nuclear button’. What do we have then? Have we kept it for Diwali?”56 President Recep Tayyip Erdogan’s October 2019 statement that it is unacceptable for Turkey not to have nuclear weapons because “[t]here is no developed nation in the world that doesn’t have them”57 is another typically populist statement, conflating strong views with half-truths or lies. Such loose talk may have several purposes. By emphasizing nuclear weapons, nationalist populists can set themselves apart from the established elite discourse. Donald Trump boasted of having gained knowledge of nuclear weapons not through a formal education but through his uncle, a professor of engineering at the Massachusetts Institute of Technology.58 Thus, the US president believed that he did not need to rely on the expertise and experience of the nuclear elite. This ignorance of nuclear lessons by virtue of not “being socialized to the dangers of nuclear weapons”59 derived from the past is a trademark of nationalist populists, but is also part and parcel of a general loss of expertise in executives and parliaments in nuclear-weapon states and nuclear-allied countries.60 Nationalist populists also like to make strong statements on nuclear issues because they may believe that this impresses their main target audience—that is, their domestic power base. Thus, Putin has several times used his regular direct encounters with the Russian public to highlight the importance of nuclear weapons for Moscow’s standing in the world. In March 2018, Putin, in his speech to the Federal Assembly of Parliamentarians, policy makers, religious leaders, public figures, and members of the media, boasted about Russia’s nuclear capabilities and in true populist fashion even invited “[t]hose interested in military equipment … to suggest a name for this new weaponry, this cutting-edge” nuclear-weapon system.61 And Modi made repeated reference to India’s nuclear weapons during the 2019 parliamentary election campaign. As one analyst observed, “The context of Modi’s remarks on nuclear weapons—election rallies—matter[s], of course. With a poor economic track record since 2014, the [Bharatiya Janata Party] has rightly decided to focus on what much of the Indian public perceives as a strength: its management of national security and defense.”62 In a similar vein, nationalist populists may bring religious motives into the nuclear discourse. Thus, Putin seems to believe that “Orthodoxy and the nuclear deterrent are equally important bulwarks of Russian statehood, guaranteeing the nation’s security internally, in the case of the church, and externally, in the case of the nuclear arsenal.”63 Talking about nuclear weapons primarily in order to impress the domestic power base—rather than external actors—can increase nuclear risks in various ways. Nationalist populists tend to trivialize nuclear risks while exaggerating the benefits of having nuclear weapons. This idealization of nuclear weapons can break down (verbal) barriers and incentivize other states to pursue nuclear weapons. The mixing of domestic and external audiences also may make it more difficult for third parties to judge the intentions behind strong statements. When Trump says that he wants to unleash “fire and fury” on North Korea, to whom is he talking?64 External observers may believe that signals are intended for domestic consumption—but they cannot be sure. Populist decision making on nuclear weapons In most nuclear-weapon states and under normal conditions, a small group of experts prepares decisions on the direction of nuclear-weapon policies.65 Routine nuclear policy making often remains remarkably unaffected by changes in political leadership. Secrecy and path dependencies complicate any precise analysis of the impact of the rise of nationalist populism on routine policy making. But a few tentative observations can be offered. Routine decision making on nuclear-weapon-related issues appears to remain mostly below the radar of most nationalist populists in power. The long, deliberative processes behind nuclear-weapon policies do not lead to the quick payoffs in public attention that nationalist populist leaders typically seek. From the perspective of the guardians of the arsenal—the group of “initiated” experts with relevant security clearances—there is little reason to change that. If and when nationalist populists get involved in policy making, their instincts usually favor greater reliance on nuclear weapons. But their unruly approach to politics is not very compatible with the inertia-driven approach of the nuclear establishment. Thus, at a briefing for him at the Defense Department on July 20, 2017, Trump reportedly asked why he didn’t have as many weapons as past presidents did, pointing out that the United States at the height of Cold War had had more than 30,000 nuclear weapons, as opposed to “only” a few thousand by 2017.66 Nationalist populists’ disinterest in and absence from routine policy making may empower officials with radical views. Nuclear doctrines are a case in point. Thus, the February 2018 US Nuclear Posture Review (NPR) changed the trajectory of US nuclear-weapon policies by introducing new types of nuclear weapons. The NPR widened the scenarios under which nuclear weapons might be used, blurred boundaries between conventional and nuclear scenarios of warfighting, lowered the threshold for nuclear-weapon use, and shifted nuclear-weapon-deployment scenarios in the direction of warfare—that is, away from the idea that the only legitimate use of nuclear weapons is to deter existential threats.67 But “Trump had nothing to do with the [NPR]; it was written almost entirely inside the Pentagon, as previous reviews had been, with still less direction or input than usual from the White House,” as Fred Kaplan observed.68 So the changes can be explained partly by the “resurgence of the nuclear establishment” and its “convergence” with the rise of Trump.69 A similar hands-off attitude may explain the rash nuclear threats that Russian diplomats have issued against third countries. Such bullying appears to be possible only because the Kremlin provides the political space for it by justifying aggressive postures (and annexations) in nationalist terms.70 Thus, the hands-off approach of nationalist-populist leaders to routine issues can also have a disruptive effect on nuclear policies. While the outcome may resemble the policies of hawkish conservatives, the policy process leading to the outcome is markedly different. This difference is relevant to the effect of such policies: nationalist populists’ neglect of detail and their ignorance of strategy can make it harder for others to assess the significance of policy changes and associated messages. Thus, bringing the nationalist populists into decision making on nuclear policy also runs the risk of their instincts ruining and counteracting the results of previous policy making, again adding a degree of unpredictability. A prime example is the January 2019 US Missile Defense Review. The document itself is the product of a multi-year interagency process. One of the key questions was whether the review should revise US and NATO policies so that they would direct missile defenses against the threat of Russian long-range missiles. The potential use of Western missile defenses in that way is a central factor influencing Russian nuclear policies. The review itself did not result in such a change of policy.71 President Trump, however, presenting the review results at a January 17, 2019, press conference, contradicted US policy by stating, “Our strategy is grounded in one overriding objective: to detect and destroy every type of missile attack against any American target, whether before or after launch. When it comes to defending America, we will not take any chances. We will only take action. There is no substitute for American military might.”72 Predictably, Russia seized on the contradictions between policies coming out of the bureaucracy and statements by the president to argue that the Trump administration was seeking to attain military dominance and justify its own expansion of nuclear capabilities.73 Nationalist-populist grandstanding thus can have the indirect effect of paving the way for competitors to react by increasing their own nuclear capabilities. The impact of nationalist-populist decision making and “instincts” during nuclear crises is a particular cause for concern. Nationalist populists by nature tend to be risk takers, and their mistrust of their own nuclear establishments—which tend to be risk averse—may facilitate dangerous moves. Putin’s statements after the annexation of Crimea that Russia “was ready” to put nuclear forces on alert is an indication of his willingness to raise the stakes.74 Erdogan’s decision to cut off power to Incirlik Air Base, where about 50 US nuclear weapons are deployed, during the 2016 coup attempt against him is another example of ignorance of nuclear dangers during a crisis. For nationalist populists such as the Turkish president, the importance of securing the domestic power base overrides all other concerns about nuclear security.75

## \*\*ISIS\*\*

### 2AC ISIS Add-On

#### ISIS uses misinformation to drive recruitment of home-based fighters that increase the prevalence and frequency of attacks

Bruno Lete, senior fellow at The German Marshall Fund of the United States in Brussels, 2022, “Stopping ISIS from Luring People into Terrorism”, GMFUS, [https://www.gmfus.org/download/article/15697 //](https://www.gmfus.org/download/article/15697%20//) [AWV]

The self-proclaimed Islamic State group has revolutionized the way terrorist organizations recruit people. Where in the past jihadist groups would spend months approaching, evaluating, and radicalizing potential recruits, ISIS succeeded to combine old-fashioned ways of communication, internet-based technologies, and an understanding of the global audience to accelerate a very effective pattern of support. Indeed, it should not only be the broad extent of their reach that should worry us, but also the speed at which they are able to recruit new fighters.

But why would a person feel excited by the things ISIS is doing? Why do they pro-actively seek to offer support, and are often ready to sacrifice their own life to advance the terrorist cause? A recent publication by the NATO Strategic Communications Centre of Excellence sheds new insights on how ISIS lures people into terrorism.

First of all, one of the easiest ways is to encourage mental support and personal belief for the self-proclaimed Caliphate — rather than to ask for direct action from the potential recruit. ISIS uses religion, convictions, and social narratives to stress how important the intentions are for jihad. In many of its official publications, ISIS avoids to ask to participate in suicide missions or to engage on the battlefield. As such, the organization adopts a more accessible profile and effectively lowers the private acceptance threshold for those that still doubt whether they should support the organization. Indeed, for the people that do not want to fight, ISIS provides alternative ways to participate in the battle. For instance, they ask for financial donations that serve to support the Mujahedeen and their families. As such, ISIS also creates an appealing narrative of social protection. This narrative provides the potential recruits a feeling of trust that the fighters, as well as their families, will not be forgotten and that somebody will take care of them.

Secondly, ISIS aggressively uses multiple media platforms to spread and amplify news, education, data, and other messages among potential recruits. The strategy is designed around a carefully chosen series of words and images that repetitively talk about a ‘corrupt Western world’ that is a threat to the ‘Caliphate,’ that ‘insults Allah,’ and that demonizes the ‘glorious martyrs.’ The internet has become an excellent medium for spreading the call of jihad and news on individually featured fighters who are given the allures of Hollywood movie stars. The Internet gives a huge advantage to ISIS in a sense that the group does not need to be on the ground and connect face-to-face with potential recruits. Instead the Caliphate can support itself virtually by establishing global discussions forums or e-mail lists that facilitate the sharing of news and literature. For ISIS, online jihad is as important as boots on the ground.

Finally, ISIS actively communicates how people can be engaged in the fight against its opponents. The group has built a narrative around the concept that ‘the Islamic State needs You,’ while stressing that the defeat of the Caliphate would not be due to the strength of the enemy, but rather to the weakness of the people who are still hesitating to give support. In this respect, ISIS actively appropriates the Islamic concepts of ‘Walaa’ and ‘Baraa’ — loyalty to Allah and hostility toward the enemies of the Caliphate — to galvanize personal commitment from Muslim believers around the world. Religious loyalty is used in hope that it will influence those that are still hesitating to actively engage in the battle. To that purpose, ISIS publications regularly feature inspiring stories of those who have already showed dedication and sacrifice by travelling to Syria or Iraq, and even engaged in suicide missions, but also suggesting a feeling of guilt to the Muslims who remain passive.

The phenomenon of home-based and foreign fighters has long been on the list of concerns, but arguably, it is only since recent that it features among our top priorities. The international community may have underestimated the threat of radicalization among our populations. And many countries in Europe, in North America, and elsewhere in the world have paid a heavy price for miscalculating the impact of ISIS’s recruitment strategy on our security. Indeed since it declared its Caliphate in June 2014, ISIS has relentlessly used its recruits to spread fear and carnage. According to a running count kept by CNN, the self-proclaimed Islamic State conducted or inspired more than 140 terrorist attacks in 29 countries (other than Iraq and Syria) killing at least 2,043 people. These attacks were conducted across the globe including Europe, North America, Russia, and Asia. In this light it is of vital interest that we continue to improve our understanding how ISIS is luring people into terrorism. The recruitment of individuals who eventually become willing to fight and carry out these attacks is, and will remain, an essential part of the ISIS terrorist strategy.

**Terrorist attacks cause nuclear retaliation**

**Ayson 10** [Robert, Professor of Strategic Studies, Director of Strategic Studies: New Zealand, Senior Research Associate with Oxford’s Centre for International Studies. “After a Terrorist Nuclear Attack: Envisaging Catalytic Effects. Studies in Conflict and Terrorism, Volume 33, Issue 7, July 2010, pages 571-593]

Washington's early response to a terrorist nuclear attack on its own soil might also raise the possibility of an unwanted (and nuclear aided) confrontation with Russia and/or China. For example, in the noise and confusion during the immediate aftermath of the terrorist nuclear attack, the U.S. president might be expected to place the country's armed forces, **including its nuclear arsenal**, on a **high**er stage of **alert**. In such a tense environment, when careful planning runs up against the friction of reality, it is just possible that **Moscow** and/or **China** might mistakenly read this as a sign of U.S. intentions to use force (and possibly nuclear force) against them. In that situation, the temptations to preempt such actions might grow, although it must be admitted that any preemption would probably still meet with a **devastating response**. As part of its initial response to the act of nuclear terrorism (as discussed earlier) Washington might decide to order a significant conventional (or **nuclear**) **retaliatory** or disarming **attack** against the leadership of the terrorist group and/or states seen to support that group. Depending on the identity and especially the location of these targets, Russia and/or China might interpret such action as being far too close for their comfort, and potentially as an infringement on their spheres of influence and even on their sovereignty. One far-fetched but perhaps not impossible scenario might stem from a judgment in Washington that some of the main aiders and abetters of the terrorist action resided somewhere such as Chechnya, perhaps in connection with what Allison claims is the “Chechen insurgents' … long-standing interest in all things nuclear.”42 American pressure on that part of the world would almost certainly raise alarms in Moscow that …might require a degree of advanced consultation from Washington that the latter found itself unable or unwilling to provide.

#### NATO can use meme warfare to counter ISIS recruitment narratives

Robbie Gramer 17 – Gramer reports on diplomacy and national security for Foreign Policy. (“Can NATO Weaponize Memes?,” Foreign Policy, 04-13-17, https://foreignpolicy.com/2017/04/13/nato-cyber-information-warfare-battle-of-ideas-memes-internet-culture/, Accessed 07-17-22, LASA-KK)

But if the most powerful political-military alliance has the real battlefield on lockdown, some worry it’s floundering in the battlefield of the internet, where ideas go to clash, Kremlin trolls go to spread half-truths, and ISIS goes to recruit foreign fighters.

The answer, some experts argue, lies in memes — those strange jokes and references that come out of the internet’s woodworks from seemingly nowhere, and seem to end up everywhere at once. A small contingent of academics and experts want NATO to get in on the action to confront pro-Russian, anti-NATO trolls, or to push back against internet jihadists in the cyber space.

“It’s time to embrace memetic warfare,” wrote Jeff Giesea, a widely-known social media and tech guru, in an article in 2015. “Trolling, it might be said, is the social media equivalent of guerrilla warfare, and memes are its currency of propaganda.” Giesea wasn’t writing in Wired or TechCrunch, but rather in Defence Strategic Communications, the journal of NATO Strategic Communications Center of Excellence (or Stratcom COE, because nothing’s complete without an onerous acronym).

“Daesh is conducting memetic warfare. The Kremlin is doing it. It’s inexpensive. The capabilities exist. Why aren’t we trying it?” Giesea asked.

It’s a question many military minds have been asking for years. A Marine Corps Major, Michael B. Prosser advocated for the U.S. military to develop a Meme Warfare Center (MWC) in his 2006 study, “Memetics–A Growth Industry in U.S. Military Operations” (abstract here).

Five years later, a specialized Pentagon unit, the Defense Advanced Research Projects Agency (DARPA) funded a study on “Military Memetics,” one of several related research programs into what it calls a “subset of neuro-cognitive warfare.” It argued the “war of ideas” was fundamental, especially when it comes to fighting terrorists, and the key characteristics of a military meme is that it be “information that propagates, has impact, and persists.” Like dancing cat videos, in other words, but with sharper claws.

The problem is that NATO, like governments everywhere, are pretty terrible at the internet. Meme’s aren’t really part of NATO’s arsenal yet, even if the alliance is desperately trying to tap into ideas from the private sector about how best to use social media.

Kremlin-backed trolls and internet-savvy ISIS supporters run circles around government social media programs, often run by stodgy diplomats with no authority to be creative. (The quest for funny memes is particularly tortured: In March, NATO’s Stratcom COE published “Stratcom Laughs: In Search of an Analytical Framework,” which included a chapter on “Humor as a Communication Tool: Designing Framework for Analysis.”)

### ISIL Extensions

#### Absent collective action against ISIL’s information operations, ISIL will exploit divisions within NATO

Eirik Hognestad 17 – Hognestad has a Master of Military Art and Science from the U.S. Army Command and General Staff College (“NATO Cohesion: The Threat Posed by ISIL,” US Army Command and General Staff College, 06-14-19, <https://apps.dtic.mil/sti/pdfs/AD1105114.pdf>, Accessed 07-10-22, LASA-KK)

ISIL does not have the military power to pose a military threat to NATO. However, as earlier discussed and reflected in the COG analysis, NATO’s weakness is within the organization itself. The question is therefore if ISIL has the capability and intention to exploit the internal critical vulnerabilities directly or indirectly. Different narratives of the threat from ISIL and threat priorities feed into the different member states national strategies, and therefore the political will to commit military and diplomatic power to fight ISIL. Therefore, if ISIL should exploit one of NATO’s critical vulnerabilities, the most dangerous Course of Action (COA) is to use ways and means that will drive a wedge between the different national strategies among the member states. One way of doing this will be to target the narrative of the threat perception of the terror organization. An approach leaning against the “near enemy” strategy may thus be a wise strategy from ISIL’s view because the further away the threat is, the less dangerous it is felt. Thus, it affects the dynamic relationship between the government, the military forces and the population of the different member states. As a result, political will may thus be affected in three ways: 1) the perseverance to continue to send troops and military hardware to ISIL’s core areas when ISIL is not a threat towards the member states, 2) legitimacy to priority funding for a threat that is felt less dangerous than others, and 3) legitimacy of the risk involved in taking casualties. Even though one may argue that reduced political will to fight ISIL is not a threat towards NATO itself, failed concurrence of threat priority is because it affects the cohesion that the alliance is built upon as a source of power. Hence, if one or more member states fails to recognize the threat towards other member states, and thus refuse to commit to the common defense, the alliance may start to disintegrate. Therefore, if ISIL targets one particular member state and focuses all its power against it, the narrative of ISIL as a threat may differ. It may lead to a decline in the mental interoperability that NATO’s cohesion depends on because other member states are more concerned by nearpeer threats such as Russia, China or Iran. This leads to different priorities for use of NATO’s power among the member states and thereby creates internal friction in the alliance. To illustrate; the Eurobarometer survey of 2018 showed a decrease in support for combating terrorism from 41% in April 2018 to 30% five months later, which is a significant reduction from the previous surveys where terrorism issues were at the top of Europeans’ concerns (European Parliament 2018, 68). Only the United Kingdom believed that the fight against terrorism should be one of Parliament’s #1 priority (38%). Among the other member states, “results show a general and significant decline of the number of respondents asking for this policy to be a top priority, led by Italy -19 (29%), Portugal -18 (28%) and Spain -18 (25%)” (European Parliament 2018, 68). As the example shows, NATO members differ widely in the perception of the priority to combat terrorism. Further, the feeling of an unequal share of the burden through participation and funding/investment creates tension within the alliance that may be exploited. The feeling of threat relates to the passion in the population and thus political will to prioritize resources to reduce the threat, to include both human resources (troops), military capabilities, and economical funding. These national resources need to be prioritized against other national strategies on the political agenda. Therefore, a feeling of inequality and unfair share of burden within NATO creates friction and discontent because all 81 member states need to balance their resources to reach their strategical ends to develop their nations according to their political programs and policies. The core of the NATO alliance is common defense, and thus if the feeling of “common” is not met, the passion to support the NATO alliance in the population is reduced which affects political will. By targeting the feeling of inequality of the Alliance, ISIL may disturb the internal cohesion of NATO. Means such as Information Operations directed at specific member states to affect the narrative of the threat from ISIL may lead to different threat perspectives within the Alliance. Further, selectively targeting certain military capabilities and soldiers to increase casualties for a specific member state may affect the population’s support and political will to maintain the use of resources for CT purposes. With the strategic shift to operate within the framework of the “Near Enemy” strategy, and by increasing IO campaigns to include poetry, community projects and religious preaching in contrast to the brutal propaganda acts the world witnessed between 2014-16, ISIL may change the narrative of the group with regards to both the global Muslim community and NATO members. The reduction of violent and bloody propaganda may be appealing to Muslims that, until now, have shied away from ISIL’s brutality, and it may affect the different member states’ perception of the group as a threat. Hence, exploitation of NATO’s critical vulnerabilities related to threat perception may result in different national narratives and priorities of political will and support of the populace. As a result, NATO’s attitude related to perseverance and legitimacy may differ within the different member states, leading to different national strategies prevailing above NATO’s political will. This may lead to a break of the trust upon which 82 the alliance rests, and ultimately the cohesion among the member states. Hence, the COG of NATO may be affected by ISIL.

#### That leads to ISIL recruitment that radicalizes and polarizes the west

Eirik Hognestad 17 – Hognestad has a Master of Military Art and Science from the U.S. Army Command and General Staff College (“NATO Cohesion: The Threat Posed by ISIL,” US Army Command and General Staff College, 06-14-19, [https://apps.dtic.mil/sti/pdfs/AD1105114.pdf, Accessed](https://apps.dtic.mil/sti/pdfs/AD1105114.pdf,%20Accessed) 07-10-22, LASA-KK)

ISIL seeks to polarize Western and Muslim Communities. The intention of this goal is related to ISIL’s goal of mobilizing potential supporters both in their core areas and globally. By taking “leadership” against Western or external involvement, ISIL is probably seeking to stand out as an attractive, dynamic, and strong organization for rebel movements and terrorist organizations globally. Hence, ISIL seeks to use this objective for recruiting new members and thereby new combat forces. The instruments for achieving the goal are international terrorism, polarizing communication, and delinquency in the form of sectarian violence. By using violent means such as brutal executions that are broadcasted, ISIL sends a message that their actions could potentially hit anyone. ISIL seeks to create fear in the people of Europe and the West for the purpose of indirectly influencing European and Western governments. To achieve this, any mobilized supporter who supports ISIL’s ideology can use a weapon he or she has at hand to attack random or selected targets in Europe. The fact that ISIL deliberately uses extreme violence made the world look when the American journalist James Foley was brutally beheaded, and the video was posted on youtube in 2014 entitled “A Message to America.” The title itself indicates that the message is directed to the entire United States, not just to the governments but to society as a whole. After the decapitation of Foley, 55 ISIL has repeatedly directed bestial and barbaric executions and published these through various media with the same kind of message. The actions in the videos evoke conflicting and different feelings in people. The sense of fear for the barbaric is undeniably awakened intentionally, but feelings such as disgust, empathy for the victims and aggression against ISIL as predators are also prominent. Based on Abrahm’s (2006) theory that terrorism’s actions are unable to communicate a strategic message, one can suggest that if the message ISIL wants to communicate is rooted in the far enemy strategy, the strategic message will drown in the effects of the violence. But at the same time, ISIL succeeds in provoking a polarizing message through this type of communication, which intends to mobilize supporters (Byman 2015, 178). There are several factors that point out that this is exactly what ISIL wants to achieve. The actions are perceived by the West as bestial, medieval, and represent a view of value and humanity that violates all legal, cultural and ethical perception and legitimacy seen in Western eyes. Thus, ISIL becomes an outgroup from the western in-group, and the polarization of “us” and “they” is a fact. We, therefore, see that ISIL not only wants to provoke polarizing conflict lines and a sectarian struggle in the Muslim population but also between itself and the Western world. The purpose is so much like the polarization of Muslim societies; eliminate the gray zone and mobilize supporters to increase their combat power. The final state of this strategic sub-goal is achieved when ISIL has polarized the world map into two groups; “The forces of faith and the forces of atheism,” which gives a clear enemy image and sets the framework for a sectarian struggle between the groups.

#### ISIL uses information warfare to spread its influence – makes it harder to govern

Chan Kung 21 - Kung is an expert in information analysis and public policy (“Features of ISIS’ Information Warfare,” Modern Diplomacy, 11-11-21,  [https://moderndiplomacy.eu/2021/11/11/features-of-isis-information-warfare, Accessed](https://moderndiplomacy.eu/2021/11/11/features-of-isis-information-warfare,%20Accessed) 7-14-21, LASA-KK)

In the field of information and anti-terrorism, a major concern is the impact of the Internet. The Internet has accelerated the flow of information, and the boundary of truth and falsehood are at times, indistinguishable. At the same time, social conditions can be exaggerated online. Combined with the psychological activities and circumstances of the masses, it is extremely easy to create a larger scale of dissatisfaction which will, to a certain extent, lead to the collapse of the original social ideological and belief systems. The United States and Western countries ignoring the social and stage of countries and regions in the Mediterranean region, Africa, and the Middle East and Central Asian countries, blindly export their ideology, and driven by the amplification effect of the Internet, this process of collapse has been accelerated. A terrorist organization such as ISIS has harnessed the great potentials offered by the Internet, and as such, it laid the foundation for the large-scale development of ISIS’s information warfare. First of all, the Islamic State has established a professional public relations organization, responsible for producing and disseminating content. ISIS has its homepage and accounts on major social networking sites, and even has multi-layered sub-accounts, thereby evading censorship. They launched DABIQ, an attractively designed online magazine with extremely provocative content, and developed a smartphone app called Dawn of Glad Tidings, focusing on the Western “high-end customer base” as their target group to inform them of the latest “news of jihad in real-time”. In addition, the Islamic State has also launched the online game, which creates scenarios for players to attack the U.S. military, police, and civilians, and rewards criminal acts and even terrorist attacks in the game. Today, ISIS can be seen almost on all social media platforms and is accessible in Western countries. It has thousands of accounts on Twitter alone, including both organized public accounts and terrorist personal accounts. ISIS is proficient in the so-called “viral marketing” model in information warfare. Through the user’s network, the information spreads like a virus and spreads to thousands of audiences using rapid replication. The organizer clearly achieves the word-of-mouth “relationship marketing” by providing a certain product or service, allowing others to become “marketing and communication levers” inadvertently. ISIS is often far more professional and sensitive than the government departments of various countries that hold the power of national governance. It has long been keenly aware of the evolution of political discourse from propaganda to information dissemination in contemporary society, and this trend is one of the keys that is enabling it to lead public opinion. Traditional propaganda methods such as sermons and speeches, obviously, lack interaction with the target audience. Therefore, ISIS encourages followers to use various websites as platforms to establish various forms of “self-media”. ISIS also cultivate Internet influencers to encourage netizens to create audio messages, videos and even websites. As ISIS cleverly hides its ambitions behind high-level productions and attractive propaganda, more and more people in the West, especially young people, have been successfully brainwashed, are actively participating in the dissemination of ISIS-related information, even going to the Middle East to become jihadists on the battlefield and gain the satisfaction of realizing their supposed self-worth. This kind of information warfare was so successful that in 2016, the official website of Tsinghua University in China was hacked by ISIS hackers where ISIS recruitment advertisements were posted. In the United States, the Federal Bureau of Investigation (FBI) has found cases where teenagers as young as 15 years old were recruited by ISIS, and in some cases in the United States, parents even encouraged their children to participate in terrorist organizations. In fact, the information warfare of ISIS is very active and successful not only in Western countries but also in Turkey and Syria. As a result, ISIS has obtained the human resources of thousands of sacrificial young people. The information society and the Internet have created a huge imbalance for the future world, making this world an unbalanced world and a world in transition. The formation of various transnational virtual organizations is now possible using simple network tools. This also means that terrorist organizations like ISIS cannot theoretically be eliminated at all. They can easily evolve into virtualized organizations that exist everywhere and can be found by search engines at any time due to the ubiquity of the information society and the Internet. They will continue to grow, gain popularity, and evolve into a new type of network-based anti-government organization. Terrorist organizations of various types have shifted their focus from the real world to the virtual world, and then back again. This is the enormous governance challenge that the information society will undoubtedly face in the future. Final analysis conclusion: Although ISIS faces restrictions as it is a terrorist organization, it has used the information society and the Internet to launch successful information warfare and has achieved remarkable results worldwide. In an age of information asymmetry, simple and easy network tools have made it possible to establish a variety of transnational virtual organizations. This will pose a huge governance challenge to the future information society.

#### ISIS declared it will use disinformation to divide and defeat enemies

Bridget Johnson 22 – Bridget Johnson is a terrorism analyst and editor at Homeland Security Today. (“ISIS Declares ‘Duty’ and ‘War Policy’ to Deploy Disinformation as a Weapon,” Homeland Security Today, 5-6-22, https://www.hstoday.us/featured/isis-declares-duty-and-war-policy-to-deploy-disinformation-as-a-weapon/, Accessed 7-17-22, LASA-KK)

Disseminating disinformation is a “duty” of jihadists in order to deceive and ultimately divide their foes and should be considered “part of the war policy,” ISIS Khorasan declared in a new issue of the group’s English-language magazine.

The article in the fifth issue of Voice of Khurasan on making the use of media and psychological warfare a core tenet of their game plan comes after the group recently emphasized that “social media warfare” is a critical part of their strategy.

“By all its types whether audio, visual, paper, satellite or internet,” using various forms of media “is a necessity and is also urgent in order to propagate and cause defeatism and demoralization of the enemy, and show the strength of the mujahideen,” said the latest issue. “…Therefore the media and all its technologies must be used by the da’ees [callers to Islam] and mujahideen to spread fear into the hearts of the enemy and to terrify them so that they do not think to stand in front of the Muslims ever.”

Deploying different types of weaponry is critical for “demonstrating strength,” ISIS argues, as is “spreading rumors to strike fear into the heart of the enemy.”

“If we can shake the chain of the enemy and divide them that is part of the war policy to divide them and defeat them,” the article continued. “…Spreading the rumors is therefore a duty upon the Muslim armies to cause fragmentation of the enemy because that disunity will demoralise them significantly.”

“Spreading fear” is another aim of disinformation that ISIS said is “very important as it will cause victory for the Muslims,” and disinformation with the goal of deception was also stressed as crucial: “There is no dispute among the fuqaha [Islamic jurists] that it is allowed to deceive the kuffar [disbelievers] as much as we can in the battlefield.”

A separate article in the issue vowed to “continue to target the nations of Kufr, without differentiating amongst them,” adding that their eyes “are fixed on neighboring countries, Iran, China, Uzbekistan, and other nations of kufr.”

“We we strike them just as we strike you while you will fail miserably to cover our actions to please your masters,” ISIS-K said to the Taliban.

In their third issue, ISIS-K declared that a concerted focus on “social media warfare” is critical to advance on the ideological battlefield but also in order to counter the pull of “enchanting” social media influencers.

“War comes in many form and targets different aspects of humans. A war can be fought militarily targeting physical self or it can be fought ideologically targeting intellect,” said that article. “As much importance the physical clashes hold ideological confrontations also matter if not more. The physical battle can be lost even before it starts if people, in our case Muslims, are defeated or at the least trapped in the battle for the hearts and minds.”

“Jihad against the crusaders and their allies is the best way to deter them. Jihad is not limited to fighting physically, and fighting with tongues are as important as fighting physically,” ISIS-K continued. “In this age, social media warfare holds the utmost importance as the medias and social media personalities are enchanting the eyes of the people. Fighting in this field needs to be done in order to incite the believers and save other Muslims from the negative impact of the enchanting battle for hearts and minds.”

Voice of Khurasan was first published in February, with a 37-page inaugural issue. The page counts have decreased since then, with the fourth issue just 10 pages long and the current issue at 19 pages.

In that first issue, the group declared that theirs is the “most important province” of ISIS after Iraq and Syria. The magazine furthered the long-running ISIS narrative that the loss of the group’s claimed caliphate in Iraq and Syria is “temporary,” adding that “although we lost the Khilafah territory and thousands of Mujahideen were martyred in a period of 5 years, there is no problem.”

The second issue similarly dedicated ample space to criticizing the Taliban and argued that “to this day no entity, no person has ever … brought forth a legit argument against the beliefs of the Khalifah” while slamming the “sheer stupidity” of al-Qaeda leadership. The magazine also brought up the Hayʼat Tahrir al-Sham merger in Syria and a frequent target of ISIS ire, HTS leader Abu Mohammad al-Jolani, saying that he has “cut off his group from al-Qaeda, rebranded his group like he changes underpants in an attempt to escape from terrorism label.”

### Memetic Warfare Extensions

#### A NATO memetic warfare strategy is essential to combat false narratives and constantly adapt to new information warfare developments

Matthew Schleupner 20 – Schleupner is a U.S. Army Foreign Area Officer with a focus on Russia and Eastern Europe and holds a master’s degree in international policy, political science, and law. (“The Power of Memes,” George C. Marshall Center, April 2020, <https://www.marshallcenter.org/sites/default/files/files/2020-09/pC_V10N2_en_Schleupner.pdf>, Accessed 07-17-22, LASA-KK)

Strategic messaging in the security space should be viewed as a debate rather than a conversation. There needs to be an aggressiveness to it that seeks to control the narrative space, much like an infantry battalion seeks to hold ground. At the same time, there must be an awareness that ethical standards preclude democracies from creating a traditional Soviet-style propaganda system. Rather, better ways must be sought for spreading the truth in these modern times. At a time when attention spans are shorter because of technology, and the amount of available information has dramatically expanded, NATO needs to redefine the way it works in the memetic space. It understands the problem; it just isn’t very good at trying to solve it. This involves a reframing of NATO’s mindset and that of its member states. NATO as an institution, along with its member states, can begin or improve this with three easy steps.

1. Get on social media

There is a hesitancy by senior political and military leaders to be active on social media. Concerns about privacy and security are real. But this is mainly a mindset problem. At the Marshall Center in 2018, leaders from security institutions and NATO/European Union nations, along with partner nations, gathered to discuss challenges to strategic communications in the 21st century. In their discussions, leaders from NATO and the EU discussed how they are combating false narratives on the internet. NATO representatives said they had set up a page labeled “NATO truths” and “NATO-Russia: Setting the record straight” to combat false narratives on NATO-Russia issues. The page was a direct response to a series of Russian messaging campaigns using memetic warfare techniques. I remember thinking: How many of these leaders are personally active on social media? How many see how quick memetic warfare can work, and how effective it really is?

A new kind of thinking is needed in the age of Twitter and Instagram. It appeared as if Alliance leaders did not understand how social media works. For example, in the 2016 U.S. presidential campaign, a meme called Pepe the Frog took off among supporters of then-candidate Donald Trump through the Reddit group /r/Donald. The supporters were tremendously successful in appropriating the meme to help their candidate. No fewer than 20 stories appeared in The New York Times about Pepe the Frog, and there was an effort by the Pepe the Frog creator to sue trolls on the internet for copyright infringement. If you simply view the comments of an internet news article critical of Russia, China or Iran, you will find them filled with odd statements, usually similar, attacking the article and working to shape the narrative in a way that negates factual reporting. The New York Times later reported that the Democratic National Committee used a false-flag campaign in the U.S. Senate race in Alabama between Roy Moore and Doug Jones, replicating what they thought were the techniques of Russian bots to create viral memes against Moore, then blaming Russia for efforts to interfere in the election.

A senior leader who is not active on social media will have a hard time understating the full effect of this activity. To be active is at least to see the battlespace. I would argue that leaders should be active, but also vocal in messaging against false, viral campaigns. For example, consider how President Donald Trump or U.S. Ambassador to Germany Richard Grenell have fought back against false narratives or have advanced the truth through their own messaging. Other examples of leaders using this type of online voice are former Deputy Prime Minister Matteo Salvini in Italy, Brexit Party leader Nigel Farage in the United Kingdom or President Jair Bolsonaro in Brazil. The list continues to grow. An example of this is when the U.S. Embassy in Russia countered publication of an altered photo of then-U.S. Ambassador to Russia John Tefft that made it appear he was attending an opposition party rally. In response, the embassy distributed a series of obviously altered photos that made it appear Tefft was speaking on the moon, on the ice at a hockey game, and standing next to U.S. Gen. Douglas MacArthur as he landed in the Philippines during World War II. These things seem small, but they set a true narrative and undermine false ones. In the world of memes, seizing the narrative and demeaning your adversaries is a total communications victory.

2. Memetic warfare as marketing

Marketing experts identify four principles necessary for success: define the strategy before the tactics, narrow the market focus, differentiate from the competition, and create a total online presence. Since marketing is a business field focused more on offensive messaging to create business and control what people are saying about a business, this fits well in the memetic model. NATO and other Western security institutions seemingly understand that a gap exists in the understanding of this new communications technique. But the strategy is in its infancy, with online trials that fail for various reasons. The strategy here needs to flow from successful marketing principles and from the fact that NATO should not overthink its memetic messaging. Each problem set, each messaging campaign should be different and depend on the market NATO is trying to reach, the hook it is trying to employ, and the total presence it is attempting to achieve. Because information on the internet moves so quickly, the messaging strategy must be flexible, with maximum leeway given to those creating the messaging program. NATO should create a committee in this communications field and not be afraid to discuss and/or employ figures who are successful at memetic messaging.

This could be controversial at times because of the types of people generally associated with spreading memes. But experts in marketing, psychology and technology could be employed for oversight. Still, reaching out to personalities in the social media realm would be an absolute must. To be clear, when I say personalities I mean trolls — from Twitter, Reddit, 4chan and other social media platforms. Even if they aren’t directly employed by NATO, their methods must be studied and understood. The power of memes is that they appear organic rather than corporately produced. Understanding what youths in Estonia or Ukraine find persuasive within their cultural context will be difficult without surveying and employing people in those domains. As Giesea points out, there is a sense of guerrilla warfare in the execution of trolling and memetic warfare. So the more NATO can develop a plan to gather bottom-fed information, the better.

3. Don’t be afraid to make mistakes

NATO commissioned a series of videos revolving around its 60-year anniversary in 2009 that attempted to adopt a memetic warfare posture, but they did not go viral in the way many expected. The U.S. State Department, in response to the success of ISIS’ online recruiting, created the “Think Again, Turn Away” program. But it ended without achieving the success many had hoped for. At least institutions are trying. The field of technology permeates with the theory that you must test and continue to test, always to the point that things break. Moving fast is critical, and that type of thinking can be antithetical to a military and political mindset that values polished and deliberative communications strategies. On the internet, there may be a need to respond to viral memes that have a maximum impact of 10 hours or less.

#### Current strategic communications fail – NATO allies must work together to embrace memetic warfare to counter ISIS and Russia

Jeff Giesea 16 – Giesea is an entrepreneur who has written many papers for NATO. (“It’s time to embrace memetic warfare,” NATO Strategic Communications Centre of Excellence, 3-1-16, <https://stratcomcoe.org/cuploads/pfiles/jeff_gisea.pdf>, Accessed 7-17-22, LASA-KK)

The term ‘memetic warfare’ has come into use on the fringes of foreign policy thinkers in the last five years to describe these types of efforts. I believe memetic warfare could be effective in countering Daesh’s recruiting and propaganda efforts and in modern conflict in general, including operations other than war. Trolling, it might be said, is the social media equivalent of guerrilla warfare, and memes are its currency of propaganda. Daesh is conducting memetic warfare. The Kremlin is doing it. It’s inexpensive. The capabilities exist. Why aren’t we trying it?

It’s no secret that the U.S. and NATO allies have done a poor job combating Daesh on social media thus far. In June 2015, the U.S. State Department conducted an internal assessment of its communications efforts that admitted that the NATO-led coalition is losing the social media war with Daesh. Existing efforts like the ‘Think Again, Turn Away’ campaign have proven ineffective against the tide of outreach coming the other way. By mid-2015 there were an estimated 30,000 foreign Daesh combatants, with the majority coming from NATO countries. Experts say Daesh’s recruiting is reaching ‘network effect’ velocity, and much of it is conducted through Twitter, YouTube, and other social media. The need to counter Daesh’s communications onslaught is urgent.

Kalev Leetaru makes a compelling case for a more muscular communication approach in a July article in Foreign Policy. The article, ‘A Few Good Internet Trolls’, argues that more aggressive and comprehensive cyber communication efforts are needed as battlefields shifts online.

What Leetaru and others seem to overlook, however, is that selling the high-level concept is not the hard part. Political leaders already understand the need for a more aggressive approach, at least at an abstract level. The hard part is actually making it happen, of transitioning the abstract concept into reality and, in turn, victory. There are numerous obstacles standing in the way: conceptual ones, financial ones, cultural ones, legal and bureaucratic ones, and strategic ones.

Here are several things we need to do to overcome these obstacles. By pursuing these, we can bring to life smarter online strategic communication practices and adapt civilian practices that can help us defeat present and potential enemies like Daesh.

Develop Memetic Warfare Conceptually

The first challenge is conceptual. Neither NATO nor its individual members have fully developed a language or conceptual grounding for social media-focused Strategic Communications. Memetic warfare today is a fringe concept, but it shouldn’t be. It needs to be developed and brought into mainstream military thinking.

In doing so, it should be thought of as broader and more strategic than ‘weaponized trolling’. Memetic warfare, as I define it, is competition over narrative, ideas, and social control in a social-media battlefield. One might think of it as a subset of ‘information operations’ tailored to social media. Information operations involve the collection and dissemination of information to establish a competitive advantage over an opponent. Memetic warfare could also be viewed as a ‘digital native’ version of psychological warfare, more commonly known as propaganda. If propaganda and public diplomacy are conventional forms of memetic warfare, then trolling and PSYOPs are guerrilla versions.

Memetic warfare can be useful at the grand narrative level, at the battle level, or in a special circumstance. It can be offensive, defensive, or predictive. It can be deployed independently or in conjunction with cyber, hybrid, or conventional efforts. The online battlefield of perception will only grow in importance in both warfare and diplomacy. Regardless of what we call it, NATO countries must continue to develop a body of knowledge around social-media Strategic Communications.

Allocate Better Resources to It

Greater investment – and better investment – is required, too. As NATO members continue to aggressively invest in cyber warfare and cyber security, they should also invest in memetic warfare.

Let’s clarify how these areas relate. Cyber warfare involves attacking a nation’s computers and networks to cause disruption or gather intelligence, or defending against such attacks. Examples include the Stuxnet virus that sabotaged Iran’s nuclear program in 2010, or China’s breach of the U.S. Office of Personnel Management files in early 2015 (and the U.S.’s response). They involved no physical combat in the traditional military sense.

Cyber warfare is about taking control of data. Memetic warfare is about taking control of the dialogue, narrative, and psychological space. It’s about denigrating, disrupting, and subverting the enemy’s effort to do the same. Like cyber warfare, memetic warfare is asymmetrical in impact. It can be highly effective relative to cost. The attack surface can be large or small. Memetic warfare can be used in conjunction with troops, ships, aircraft, and missiles, or it can be employed without any kinetic military force at all. It operates in the communications battlespace.

The communications battlespace, of course, is where we are losing to Daesh. Ambassador Alberto Fernandez, former head of the U.S. State Department’s Center for Strategic Counterterrorism Communications (CSCC), gave a frank assessment of communication efforts in an outgoing interview last year. ‘It’s not that ISIS is so great’, he said. ’It is that the response to ISIS is both limited and weak.’

If the communications battlespace is where we’re losing, why aren’t we investing more in it? Why has NATO placed itself in the position of responding to Daesh rather than having prevented Daesh and similar forces from existing in the first place? Why hasn’t NATO gone on the offensive to wipe out Daesh and other jihadists as credible psychopolitical movements? (The discussion of waiting until extremists become violent before they are countered — the essence of Countering Violent Extremism (CVE) initiatives — rather than forestalling their rise in the first place is another issue entirely, but it is one that can also be addressed through memetic warfare.) NATO and many of its members individually are investing some funds in strategic communications, with the U.S. State Department alone spending $118 million in 2015. Yet the amounts, while impressive, are miniscule in proportion to what we’re spending overall.

Even at current spending levels, one must question how effectively these resources are being allocated. The civilian funds directed toward CVE and communications are relying on public diplomacy and top-down ‘conventional’ Strategic Communications, with military information operations and PSYOP showing themselves to be tepid, timid, and stale. Where is there experimentation? Where are the guerrilla efforts? Where is the innovation? Where is the war-gaming of tactical successes at the Strategic Communications level?

NATO’s communications efforts to date are like Version 1.0 of a software program. Releasing the first version is incredibly difficult and an accomplishment in its own right, but now it is time for version 2.0 and a more serious commitment to rapid learning and improvement. To get there, NATO and individual member countries must commit more physical resources and command authority to Strategic Communications, allocate existing spending more intelligently, and provide intellectual and operational space for learning and innovation.

Embrace the Memetic Mindset

Perhaps the greatest obstacle to memetic warfare is a lack of appreciation for social media as a battle space and the extent to which memetic warfare is already taking place. Perhaps this is generational: from the outside looking in, it doesn’t appear that the alliance’s military and foreign policy decision-makers truly understand social media at all, much less as a tool and weapon for the common defense. How many generals are active on Twitter and truly understand it beyond the explanations of their kids or younger colleagues?

Even for those of us who live on social media, it is sometimes difficult to appreciate how quickly information can spread, the profundity of its global scope, and the significance of its impact on perceptions, narratives, and social movements. Once one starts viewing the Internet through meme-colored glasses, you see memetic warfare everywhere — in political campaigns, in contested narratives about news events, in the thoughtless memes shared by Facebook friends, and in videos on YouTube. It shows up in movements like #BlackLivesMatter, where there’s an attempt to shape perceptions and galvanize public support. In the U.S. Republican Primary race, Jeb Bush recently attempted to paint Donald Trump as the ‘chaos candidate’. But when his campaign tried spreading a #ChaosCandidate hashtag, trolls supporting Trump took it over and used it to denigrate Jeb Bush. Hashtags, one might say, are operational coordinates of memetic warfare.

On the geopolitical stage, memetic warfare is being used in a military capacity by centralized governments like China and Russia, in addition to non-state actors like Daesh. Anyone who has read the comments on news articles related to foreign policy has probably noticed some suspiciously inauthentic, biased comments. China employs 20,000-50,000 Internet police and an additional quarter-million ‘trolls’ who spread pro-Beijing material domestically and abroad, and who help monitor citizens.

Similarly, Russia has ‘troll farms’ where Internet commentators spread pro-Moscow messages and disinformation. It tends to use memetic warfare offensively. It has been notorious in its disinformation related to Ukraine, from the ‘green men’ who were ‘not’ Russian troops, to the shoot-down of the Malaysian airliner, to the nature of the Ukrainian government itself. Moscow has also targeted domestic affairs in the U.S. In 2014, Russian trolls spread disinformation about a chemical plant explosion in Louisiana under the #ColumbianChemicals hashtag. They spread similar disinformation about an Ebola outbreak in Atlanta, under #EbolaInAtlanta. In each case, there were fake videos, photos, and Wikipedia pages, combined with outreach to journalists and buzz centered on a hashtag. As the United States has downsized its information operations and PSYOP capabilities, the Kremlin’s RT propaganda house has begun to recruit former professionals.

A ‘memetic skirmish’ involving the U.S. Embassy in Moscow demonstrates that talented and creative State Department communicators are poised to act when allowed. In August 2015, the local news in Moscow released a photo showing U.S. Ambassador to Russia John Tefft conducting a press conference at an opposition rally. The photo, according to the U.S. Embassy, was a fake. It seemed to be deliberate disinformation. The Embassy had a brilliant response. ‘Ambassador Tefft spent his day off yesterday at home’, the embassy tweeted. ‘But thanks to Photoshop, he could be anywhere.’ Shortly thereafter, various Russian twitter accounts released the same press conference photo of Ambassador Tefft against a variety of backgrounds - landing on the moon, surrounded by cats, at various weddings, at a hockey game, landing in the Philippines with General MacArthur during World War II, and elsewhere. It became a meme, and Russia’s disinformation effort backfired.

The Ambassador’s Photoshop imbroglio recalls a meme from early in 2015, when Daesh was demanding $200 million in ransom to release two Japanese journalists. The terrorists released a photo of Jihadi John wielding a sharp knife above the heads of the two Japanese men, kneeling in orange jumpsuits. As the 72-hour deadline to pay the ransom passed, Japanese Twitter accounts began sharing doctored images of the threatening photo set against darkly comic backgrounds — one with Jihadi John holding a banana instead of a knife, another of him wearing Mickey Mouse ears and the Disney Magic Kingdom in the background, and another with him wearing pink lingerie in a field of flowers. The ‘meme-ing’ of the image was viewed as a symbol of defiance among the Japanese, a classic denigration. It did not save the life of journalist Kenji Goto, but it may have helped lessen the psychological impact of Daesh’s propaganda.

For memetic warfare to succeed, decision-makers need to get into the right mindset and empower those who have it. Study what’s worked and what hasn’t. Network across civilian disciplines, particularly with Internet trolls, hackers, marketers, and PR pros. To the extent possible, experiment on social media yourself or through those close to you. Try following and influencing an issue. Embrace memetic warfare as an essential capability in modern warfare.

No one is better to support this than the NATO Strategic Communications Centre of Excellence. I recommend organizing a cross-disciplinary global summit on memetic warfare. Consider focusing it specifically on countering Daesh and giving it the feel of a TED conference (perhaps partner with them), drawing fresh ideas, perspectives, and connections from multiple disciplines and countries.

#### Memetic warfare and awareness can be used to counter disinformation

Tom Ascott 20 – Ascott is a writer at the Australian Strategic Policy Institute. (“How memes are becoming the new frontier of information warfare,” Australian Strategic Policy Institute, 02-19-20, <https://www.aspistrategist.org.au/how-memes-are-becoming-the-new-frontier-of-information-warfare/>, Accessed 07-15-22, LASA-KK)

Memes might appear as if they’re just little pranks kids play online, yet they’re anything but. In the 2016 US presidential election, many memes were made by a Russian troll farm to influence the outcome. It wasn’t an isolated incident, either—now troll farms are popping up more frequently. In November last year, an undercover reporter revealed a new one in Poland. The memes it’s producing focus on ‘the aviation and defence industries, and target key decision-makers involved in the awarding of major government defence contracts’. The memeing, it has transpired, was political.

Those memes were a form of information warfare, or what would have been thought of in the past as a psychological operation. Information warfare is often about waging an influence campaign that can change behaviour through ‘unconventional means’, such as social media. Memes play a part in a specific type of information warfare dubbed ‘memetic warfare’.

Early memetic warfare used a more ‘Dawkinsian’ concept of memes. In his 1976 book The selfish gene, Richard Dawkins coined the term ‘meme’ for a cultural product that can replicate and spread. The meme concept had immediate and clear implications for information warfare campaigns.

Meme warfare now more often refers to using memes as individual weapons of information warfare. It’s a form of disinformation that can be used to secure strategic goals. Disinformation campaigns go to back to at least 1923, when the Soviet Union had an office for ‘dezinformatsiya’ campaigns—a term coined by Stalin to describe ‘false information carefully constructed with the intention to deceive’. The internet has ushered in an age when deception can be perpetrated on a mass scale, with the click of a mouse.

The West is desperately lagging in its memetic capability. US Marine Corps Major Michael B. Prosser proposed that NATO open a meme warfare centre. In his 2006 thesis, he looked to Dawkins’s ideas of memes as units of cultural transmission that held the potential to ‘be used like medicine to inoculate the enemy and generate popular support’. He noted that information operations, psychological operations and strategic communications weren’t using memes effectively. In the following decade, NATO never did open a meme warfare centre, but the idea didn’t go away and is now starting to gain traction again.

At the same time, across the pond, DARPA funded Dr Robert Finkelstein to investigate how it might weaponise memes. In his presentation to the Social Media for Defense Summit, Finkelstein recommended memetic warfare for all public affairs units, the Central Intelligence Agency and the US Army Civil Affairs and Psychological Operations Command.

It wasn’t until 2017 that the EU and NATO established the European Centre of Excellence for Countering Hybrid Threats. While understanding memes as information warfare falls within its remit, its purpose is more analytical than proactive. Currently, it seems, the best form of defence is awareness.

Memes resemble traditional propaganda in a few ways; a hostile government can use them to spread malicious information in a way that’s advantageous to it. But there are key differences, too. Because memes are a common way for people to express themselves online, it’s very easy to make memes without their being suspected as pieces of information warfare. And they can be much more targeted. Traditional propaganda focuses on large groups of people who have some spatial or political link. The way the internet ‘fingerprints’ users allows hostile actors to draw up their own lists, looking for links even users don’t know they share.

Authoritarian regimes may be less susceptible to memetic warfare because they have more control over their social media systems. China employs ‘20,000–50,000 internet police and an additional quarter-million “trolls” who spread pro-Beijing material domestically and abroad’. Memetic warfare isn’t just military, but civil as well. Some 1,200 TikTok channels are run by various Chinese civil authorities such as ‘police stations, SWAT teams, traffic police, and prisons’. They’ve produced more than 13,000 videos and amassed a combined 4.8 billion views. It’s a domestic attempt to control the online narrative by the security services. It’s unlikely that a meme (such as that Chinese police are responsible for assassinating high-profile individuals) will spread there, whether produced internally or by the West.

Memes also can have dual functions. As well as acting as a form of information warfare, they can help normalise extreme behaviours through humour. For example, memes can be recruitment tools for white nationalist groups. The Christchurch mosque terrorist, Brenton Tarrant, frequently used 8chan. All chan sites require users to submit images with text. As a result, these right-wing sites are a fertile breeding ground for memes that normalise extreme behaviour and reinforce each other. Slowly, the memes seep out into more common areas of the internet, such as Twitter. That everyone on 4chan should be considered a terrorist is itself already a meme on 4chan.

## \*\*China\*\*

The story here:

China is using info warfare tactics as a threat to NATO/ US security- NATO response k2 avoid \*BIG CHINA IMPACT\* (I think that Kendall-taylor is a good card that talks about how the plan combats china info warfare)

Impact scenario ideas – Still very much a WIP

* Info warfare means china goes ahead the US - wrecks LIO??
* Info warfare means China invades Taiwan= war

### 2AC China Add-On

#### The Ukraine situation has exposed China as a threat using information warfare as it’s tool to attack the US

Dwoskin 22 Dwoskin, E. (2022, April 10). Elizabeth Dwoskin focuses on social media and the power of the tech industry in a democratic society. Before that, she was the Wall Street Journal's first full-time beat reporter covering big data, AI, and the impact of algorithms on people's lives. China is Russia's most powerful weapon for information warfare. The Washington Post. Retrieved July 11, 2022, from [https://www.washingtonpost.com/technology/2022/04/08/russia-china-disinformation//CS](about:blank)

Russian propaganda about the war in Ukraine [cratered](about:blank) last month after Russian state news channels were blocked in Europe and restricted globally. But in recent weeks, **China has emerged as a** potent **outlet for Kremlin disinformation,** researchers say, portraying Ukraine and NATO as the aggressors and sharing false claims about neo-Nazi control of the Ukrainian government. With over a billion followers on Facebook alone, China’s state-controlled channels offer Russian President Vladimir Putin a powerful megaphone for shaping global understanding of [the war](about:blank) — often called a “special operation” in line with Kremlin rhetoric. Since Russia invaded Ukraine on Feb. 24, researchers say, Chinese channels have touted the false claim that the United States runs bioweapons labs in Ukraine, have asserted that Ukrainian neo-Nazis bombed a children’s hospital which was in fact bombed by Russian troops, and have suggested that Ukrainian President Volodymyr Zelensky was being manipulated by U.S. billionaire George Soros. Chinese channels also have given airtime and amplification to high-ranking Russian government officials and to presenters from Russian government channels whose shows have been restricted or blocked. Last month, after a host on Sputnik, the Russian state news outlet, posted a video on his personal YouTube channel discussing how neo-Nazis were on the rise in Ukraine, the clip was tweeted by Frontline, a Chinese government outlet. “With governments and tech platforms moving to censor or limit the spread of Russian propaganda, pro-Kremlin talking points are now being laundered through influencers and proxies, including Chinese officials and state media outlets that obviously do not face the same restrictions that have been placed on Russian state media outlets,” said Bret Schafer, senior fellow and head of the information manipulation team at the Alliance for Securing Democracy, a nonpartisan initiative housed at the U.S. German Marshall Fund that tracks Chinese and Russian state media. “This has allowed the Kremlin to effectively skirt bans meant to limit the spread of Russian propaganda.” Putin’s success in seeding some of these misleading narratives through proxies and allies is casting doubt on the ability of Western governments and the tech giants to effectively rein in the most pernicious forms of authoritarian propaganda. With China’s help, experts say, Russia also is regaining its ability to cloud the narrative around Europe’s biggest conflict since World War II. “While the world’s eyes are still on Ukraine, and the journalists are there, it’s going to be hard for the Russian government to make great progress. But they can make progress on the edges,” said Kate Starbird, an associate professor in the Department of Human Centered Design & Engineering at the University of Washington. “And in the long run, if the public is confused enough about what happened, then we might not give our leadership a clear message to take action.” *s*ince the war’s early days, when the European Commission blocked Russian state channels and Twitter, YouTube and Facebook [restricted their reach](about:blank), Russia has raced to create workarounds. Journalists have uncovered a coordinated campaign to pay TikTok influencers to push pro-Kremlin views, while researchers from the data science company Trementum Analytics have documented pro-Russia trolls spamming YouTube videos about Ukraine with pro-Russian comments. The Russian government also has used its embassies to push out misinformation to tens of thousands of followers on Twitter, YouTube, Facebook, and the messaging app Telegram. According to the Israeli disinformation research group FakeReporter, Russian embassies have created at least 65 new Telegram channels since the war began. Twitter stopped recommending these accounts this week. Fox News and other right-leaning American outlets also have picked up Russia’s talking points — notably when Fox host Tucker Carlson last month promoted to his prime time audience the baseless claim that Ukraine was developing biological weapons with the assistance of the U.S. government. According to disinformation researchers and the fact-checking group PolitiFact, that claim, which has been circulating for years, is a misleading reference to a public health research partnership between the United States and Ukraine; the White House has called it “preposterous.” Last week, the New York Post wrote an article tying the discredited biolab claim to President Biden’s son Hunter, claiming that the younger Biden had helped secure funds for a start-up that worked on the research biolabs in Ukraine. The Washington Post [has reported](about:blank) that Hunter Biden “was not part of a decision" to invest in the start-up. Meanwhile, highly active online communities, such as anti-vaccine activists and adherents of the radicalized movement QAnon, have seized on the biolab claim and other Russian narratives. An [early, prolific spreader](about:blank) of the theory, according to the Anti-Defamation League, was a Virginia man with ties to QAnon. [*’*](about:blank) China is, by far, the Kremlin’s biggest promoter, however. The top four Chinese outlets — CGTN, Global Times, Xinhua News and T-House — command a massive audience with a combined follower count on Facebook of 283 million, according to research from the nonprofit Center for Countering Digital Hate (CCDH). All told, Chinese outlets on Facebook have over 1 billion followers, according to the Alliance for Securing Democracy — far more than the roughly 85 million total followers for Russia’s main channels. Asked how Facebook was addressing China’s emergence as a vector for Russian propaganda, Facebook shared several examples of fact checks applied to misleading pro-Russian content from Chinese state media. The company did not respond to questions about whether it has restricted Chinese state media accounts or has plans to do so. Twitter spokeswoman Madeline Broas said the company had placed some limits on Chinese state media for several years, and that — beginning last Friday — it had begun putting highly-visible labels on any tweet that contained a link to Chinese state media. (Previously, such labels were shown only to people who searched for the account.) YouTube declined to answer questions about Chinese state media. Spokeswoman Elena Hernandez said the company does fact-check misinformation and that it prohibits content that minimizes, trivializes, or denies the existence of well-documented, violent historical events. The Chinese Embassy in Washington did not respond to a request for comment. China and Russia have long been allies, extending back to the Cold War, and view their alliance as a bulwark against Western power. The two countries strengthened their bond ahead of the Ukraine invasion, issuing a joint statement on Feb. 4 describing their relationship as a “no limits” friendship. Russia has refused to acknowledge the invasion, referring to its actions in Ukraine as a “special operation.” Chinese state media immediately adopted that term, according to the Alliance for Securing Democracy’s tracker, with Chinese accounts using it 180 times between Feb. 24 and March 12. The term “invasion” was mentioned 145 times, but more than the third were references to the U.S. invasion of Iraq — an attempt to equate Russian and American military actions. [*Silicon Valley companies have been rewriting their rules during the war in Ukraine. Russia is retaliating.*](about:blank) Chinese media also began to take up neo-Nazi storylines, according to ASD. Chinese diplomats and state media have tweeted about Nazis more than 140 times since the start of the war, according to the tracker. In the year preceding the war, Chinese state- affiliated accounts tracked by the group tweeted about Nazis only twice. The Azov Battalion, a group partially made up of anti-Russian nationalists and neo-Nazis, has been part of Ukraine’s military since 2014. But experts say the [controversial battalion](about:blank) does not have major influence in the country whose president, Zelensky, is Jewish. Lately, China has focused more attention on blaming NATO for the conflict, researchers say. A recent Facebook post from T-House, a millennial-focused outlet, compared Ukraine’s potential membership in NATO to Hitler’s attempt to conquer Ukraine, according to research by the Center for Countering Digital Hate. “The moves by the US-led #NATO have pushed the #Russia-Ukraine tension to the breaking point,” said a recent tweet by China’s ambassador to the Asia-Pacific region.In late March, NATO was the tenth most used key phrase in Chinese tweets, according to the ASD tracker. Meanwhile, China’s consul general in Belfast recently tweeted a false claim from Russian state media that Zelensky is hiding in Poland, a NATO member. China also is giving a boost to Russian presenters whose audiences appear to have been limited by Western bans. The personal talk show for U.K. presenter George Galloway, host of the “Mother of All Talk Shows” on Sputnik, been shared numerous times by several large Chinese outlets such as Global Times. Currently, the Sputnik website that hosted Galloway’s show appeared to be blocked in the United Kingdom, according to ASD. But his personal YouTube channel, which does not make visible references to his Sputnik backing, continues to stream it. Galloway did not respond to a request for comment. In a tweet on Wednesday, Galloway tweeted in response to Twitter’s decision to label his account “Russian state media,” saying, “Dear [@TwitterSuppor](about:blank)t I am not “Russian State Affiliated media”. I work for NO [#Russian](about:blank) media. I have 400,000 followers. I’m the leader of a British political party and spent nearly 30 years in the British parliament. If you do not remove this designation I will take legal action.” Experts disagree about how the tech companies should police China and other Russian proxies. The tech companies have cast their crackdowns on Russian media as [drastic actions](about:blank) taken under extraordinary circumstances; they largely do not want to impose blanket bans on state outlets. Experts also have noted that if state outlets are banned for disinformation, the tech companies would face increasing pressure to ban nonstate channels that spread misinformation, such as Fox News. Instead, the tech companies more recently have opted for transparency, such as fact-checking and labeling. In 2018, YouTube began labeling state media outlets. Twitter did so in 2020, as did Facebook. But labeling is premised on the idea that informed users will make wise decisions about whether to trust content, and that has had mixed results. In 2020, George Washington University researchers studying the impact of YouTube labels on content from RT found that they were effective at making people more aware of misinformation, but only when the labels were prominently displayed. A separate study from the Election Integrity Partnership, a consortium of prominent disinformation researchers, found that labeling was inconsistent and that tech platforms failed to prominently show the labels in search results. Since the Ukraine war began, Twitter has added more prominent labels, saying the move has reduced the reach of Russian propaganda by 30 percent. But some advocates said transparency measures are insufficient in the face of China’s global disinformation campaign, and called on the tech giants to do more. “When there is clear disinformation targeted at foreign populations, the tech companies have a perfectly legitimate moral case for limiting or removing that propaganda,” said Imran Ahmed, chief executive of CCDH, which has researched Chinese state media. [*Pro-Russia rebels are still using Facebook to recruit fighters, spread propaganda*](about:blank) Not all companies have embraced the same level of transparency. TikTok, whose parent company ByteDance is Chinese-owned, started its first pilot project to label a few dozen Russian state outlets last month, and the company has plans to start labeling Chinese outlets. Researchers say state propaganda probably has a massive presence on its service — but it is difficult to detect with such limited labels and without providing researchers the ability to review the platform’s data. The company [says](about:blank) it is still developing a state media policy. Rather than adopting ad hoc policies during an emergency like the Ukraine war, platforms should have distinguished long ago between media outlets run by authoritarian governments and outlets, such as PBS or the BBC, that receive support from democratic governments, said Alex Stamos, director of the Stanford Internet Observatory, which is a member of the Election Integrity Partnership. Stamos, who once was Facebook’s chief security officer, argued that social media companies should not give a megaphone to state media outlets from countries, such as China, where free speech is suppressed. Russia would now also fall into that category, he said. “This is the time," Stamos said, “for the tech platforms to finally create rules about state media run by authoritarian governments.”

#### China is using info-warfare tactics to make invading Taiwan easier- US counter-info warfare key to prevent invasion

Newsham 21 Newsham, G. (2021, October 23). Grant Newsham is a Senior Fellow with the Center for Security Policy. He also is a Research Fellow at the Japan Forum for Strategic Studies focusing on Asia/Pacific defense, political and economic matters. Wake up: China is engaging in media warfare against Taiwan. The National Interest. Retrieved July 13, 2022, from https://nationalinterest.org/blog/buzz/wake-china-engaging-media-warfare-against-taiwan-195477 //CS

Can the People’s Republic of China (PRC) invade and conquer Taiwan? Experts differ, but the current debate considers only the military balance—and whether the People’s Liberation Army (PLA) has the weapons, hardware, and capabilities to get ashore, defeat Taiwan’s military, and force Taipei to surrender. The military match-up is important, but it misses half the picture—and half of the PRC’s strategy against Taiwan. Professor Kerry Gershaneck’s new book, Media Warfare: Taiwan’s Battle for the Cognitive Domain, details and explains a key portion of that “other half”: the **PRC’s use of “media warfare” to psychologically fracture and demoralize Taiwan and make conquest easier or, even better, to have Taiwan surrender without a fight.** Gershaneck knows the topic well. He has vast Asia experience and hands-on strategic communications experience at all levels of the U.S. government, as well as a particularly useful counterintelligence background. In 2020, he published a seminal work on PRC Political Warfare: Political Warfare: Strategies for Combating China’s plan to “Win without Fighting” In this book, Gershaneck focuses on what China has done and is doing to Taiwan on the media warfare front. Importantly, he lays out how Beijing is waging the same type of insidious warfare worldwide—especially against Taiwan’s main “ally,” the United States. To Chinese strategists, media warfare and political warfare are just as important as building the PLA into a force able to defeat the U.S. military. Indeed, the kinetic and the “informational” are considered mutually reinforcing lines of attack. Media warfare, also known as Public Opinion Warfare, leverages all instruments that inform and influence an adversary’s public and government opinion. The objective is to weaken, divide, corrode, confuse, co-opt, and demoralize an opponent. What are the instruments? Beyond the old standards such as television, radio, and newspapers, there are also books, textbooks, and, over the past three decades, the Internet and social media. Indeed, the Chinese Communists make full use of all of these and are particularly aggressive on the internet/social media vectors. This makes sense. With TV, radio, and newspapers, a propagandist must somehow lure the intended target to receive the message. With social media and the Internet, it is possible to “jam” the message into the target non-stop. And given that 90 percent of Taiwan’s public is active on social media, that democracy presents a particularly target-rich environment. What does the PRC’s media warfare campaign against Taiwan look like? To deliver its messages, Chinese entities have bought Taiwanese broadcasting outlets and newspapers, and use the lure of advertising dollars against “independent” outlets. Another key part of the effort to influence the widest audience is the aggressive use of social media platforms to affect, confuse, and deceive, often through effective profiling of users to better target messaging. How successful has Beijing been? In 2018, the PRC deployed media warfare stratagems—including heavy use of social media—to engineer the election of an absolute “nobody”: Kuomintang Party (KMT) candidate Han Kuo-yu—as the mayor of Kaohsiung, Taiwan’s second-largest city. Many in the KMT support Communist China’s plans to annex Taiwan. The surprise election of Han to this powerful mayorship was no small feat and no minor issue: Kaohsiung has historically been a stronghold of the ruling Democratic Progressive Party (DPP) that firmly opposes annexation by China. As part of the effort to elect Han, pro-Chinese Communist Party (CCP) media in Taiwan and the communist propaganda organs in China relentlessly attacked DPP leadership, including President Tsai Ing-wen, with disinformation and untrue allegations. That relentless campaign interference was enough to raise doubts with voters, especially because there were no effective means in Taiwan to detect and counter the media warfare attacks. Han ran for president two years later, once again with pro-CCP Taiwanese and Communist China-based “media warriors” hard at work on his behalf. Han had a fair shot at winning had not two things happened. First, Taiwan’s government woke up to the media warfare threat and cobbled together effective enough defenses to derail and expose Beijing’s strategy. Second, the Chinese Communist crushing of Hong Kong’s pro-freedom movement a few months before Taiwan’s election awakened a huge chunk of Taiwan’s public to the Chinese threat—and inoculated many to Chinese subversion. Gershaneck provides a concise, yet detailed introduction to media warfare in Taiwan, but with larger implications. He walks the reader through the confusing and redundant terminology and explains how media warfare fits into the larger Chinese political warfare strategy—intended to defeat an enemy via all measures short of outright kinetic warfare. While using Taiwan as the focus of his latest book, Gershaneck emphasizes that what the PRC is doing to Taiwan it is also doing to the United States and other free nations. Gershaneck wrote his most recent book to help Western nations “better detect, deter, counter, and defeat” Chinese media warfare—and political warfare writ large. And he provides a set of practical recommendations for Taiwan’s government that are applicable to any country under PRC media warfare attack. For example, Chinese state-controlled media (which is every media entity operating in China) has formed strategic alliances with western media. The New York Times, Washington Post, and even the “conservative” and “tough on China” Wall Street Journal carried China Daily media warfare inserts for several years. Gershaneck also describes how the Chinese government takes control of newspapers and broadcast media serving the Chinese “diaspora” in many, if not most, countries. At the same time, not only does the PRC flood the United States with “reporters” but it makes life miserable in China for the few foreign reporters still allowed to operate there. U.S. and other foreign outlets routinely self-censor to avoid angering Beijing. Gershaneck paints a grim picture of China’s massive, well-funded, and effective media warfare effort against Taiwan, and worldwide. Yet, many—if not most—people will say they are too smart, too well educated, and too discerning to be influenced by Chinese Communist Party media warfare. Maybe so. But if you’ve ever said or thought any of the following, you’ve been “influenced.” -Covid-19 couldn't possibly have come from a laboratory. -China wants to “reunify” with Taiwan. -The United States must have China’s help on climate change, North Korea, etc. -We simply have to be invested in the China market. -To make China an enemy, treat it like one. -China is no longer communist. It is capitalist. -China’s rise is “peaceful” and “inevitable.” -China has never attacked its neighbors. -China is not expansionist. -China is just doing what all great powers do. Gershaneck’s book is indeed alarming—though one grudgingly admires China’s industriousness and persistence on the “non-kinetic” media/public opinion/psychological fronts. But certainly, the U.S. Government has its own media warfare and political warfare effort to match and defeat whatever Beijing is doing? If only. Unlike previous administrations, the Trump administration understood the problem, and also understood China’s political warfare efforts. It had some limited success exposing and cracking down here and there—with Secretary of State Mike Pompeo (to whom the book is dedicated) and Deputy National Security Advisor Matthew Pottinger being particularly effective. But they ran out of time. The U.S. Government is once again back to doing nothing while China runs wild in the crucial “cognitive” battlefield that Gershaneck explains so well in this important book. This isn’t surprising, one supposes. The recent collapse of the Afghan government and military was as much a political warfare victory for the Taliban as a military victory. The U.S. military and civilian leadership didn’t seem to notice. **One hopes they take China’s media and political warfare threat more seriously.** And then do something about it.

#### US-NATO cooperation on Chinese cyberthreats key to deter Chinese invasion of Taiwan

Odgaard 22 Liselotte Odgaard- professor at the Norwegian Institute for Defense Studies . Her work focuses on US–China–Europe relations, including NATO–China relations; Chinese foreign, security and defense policy; Indo-Pacific security, and the geopolitics of the Arctic region. (2022) NATO’s China Role: Defending Cyber and Outer Space, The Washington Quarterly, 45:1, 167-183, DOI: 10.1080/0163660X.2022.2059145

NATO’s vague recognition in 2021 that China constitutes a challenge to the transatlantic alliance reflects an institution that has failed to take on the security threats emanating from Beijing. Russia’s invasion of Ukraine on February 24, 2022 highlights the reasons why this omission is problematic. The war in Ukraine has reignited transatlantic unity of purpose in addressing threats from Moscow toward European security. The existential shock that Europe is facing now that a Russian regime has shown itself willing to go to war against European countries carries with it the risk that China will be forgotten when NATO discusses its future priorities. During the war, China is walking a tightrope between maintaining its commitment to sovereignty and territorial integrity and keeping up cooperation with Russia. The future strength of the Chinese-Russian partnership is likely to be determined by the continued usefulness of Moscow in China’s efforts to carve out more space for a Sinocentric international order based on authoritarian regimes. Meanwhile, China will continue to engender threats to the US and Europe in all domains and across geographical regions. With the summit statement of the North Atlantic Council released June 14, 2021, NATO extended a commitment to “engage China with a view to defending the security interests of the Alliance,” since “China’s stated ambitions and assertive behavior present systemic challenges to the rules-based international order and to areas relevant to Alliance security.”1 China’s coercive policies, nuclear arsenal, military modernization, military cooperation with Russia, lack of transparency, and use of disinformation are listed as main areas of concern for the alliance. NATO takes the China challenge seriously but has yet to devise a strategy to address it. NATO takes the China challenge seriously but has yet to devise a strategy to address it Compared to the United States, Europe took a long time to acknowledge its stake in managing security challenges from China. As Beijing pushed beyond its traditional zones of interest in East and Southeast Asia toward the Indian Ocean in the 2000s, US security policies began to focus more on China as Washington sought a new geopolitical equilibrium in Asia.2 Since 2014, France and the UK have spearheaded Europe’s naval diplomacy to counter the displays of force and increasing tensions in maritime Asia to which China contributes. This engagement has focused on regular exercises with the US and its Asian allies, operations in support of freedom of navigation, and base-sharing agreements.3 In 2021, the EU recognized that these geopolitical dynamics directly impact its security and announced the establishment of supportive mechanisms in its Indo-Pacific strategy.4 However, NATO has been conspicuously absent in these transatlantic endeavors designed to counter challenges to US and European security. Reflecting NATO’s absence from the main arena of US-China strategic competition, the alliance is hardly ever mentioned in off-the-record conversations on Indo-Pacific security between diplomats and think tank personnel. NATO’s reluctance to take on the China challenge is perhaps not surprising, given its inherent assumption that the European continent is the jewel in the crown of the US alliance system, which is thought to guarantee US assistance in the event of a military threat against Europe. This assumption was challenged during the Trump administration, which openly questioned the US commitment to Article Five’s collective defense obligation. The invasion of Ukraine has given NATO a new lease on life and put it at the frontlines of transatlantic cooperation on deterring Russia from further military action in future. However, NATO’s focus on its eastern frontline carries the risk that the alliance turns into a Russia-focused European institution and ignores that China is a global great power competitor which also constitutes a major challenge to the security of all NATO member states. Washington increasingly looks to the EU rather than NATO for guidance on Europe’s future security policy. One reason is that NATO’s toolbox is lagging in domains such as cyber and outer space, although cyber and outer space operations are key enablers of actions in all domains including air, sea, and land. One indication of this is the US-EU negotiations surrounding a common response to cyber threats which took place during the first US-EU Trade and Technology Council (TTC) meeting in Pittsburgh in September 2021. In addition, during Trump’s presidency, longstanding US dissatisfaction with Europe’s modest defense spending threatened to put NATO on the backburner in transatlantic security debates.5 Since then, Russia’s invasion of Ukraine has elicited a sea change in German defense policy with the announcement in February 2022 that defense spending will increase to more than 2 percent of its gross domestic output annually.6 While this may be a convincing signal that Europe will finally devote the resources required for its own defense and revive NATO’s central role in transatlantic security, there is also a risk that China will be moved to the periphery of the alliance’s agenda. On February 11, 2022, during the runup to the Russian-Ukrainian war, the Biden administration published its Indo-Pacific strategy as US Secretary of State Anthony Blinken was in the midst of a Pacific trip to Australia, Fiji, and Hawaii.7 This US prioritization signaled that despite Moscow’s war in Europe, Washington remains committed to strengthening its presence in the Indo-Pacific and competing with China. **If the US drops the ball on the Indo-Pacific, Washington is concerned that China might use force against Taiwan**.8 Consequently, the key question for the US is how many resources can be tied up in Europe without losing sight of the long-term goal: deterrence of China. As US strategic competition with China increases while NATO is sitting on the fence, **failure to develop a transatlantic defense policy that addresses China will leave Europe vulnerable to China’s ability to exploit the weak links in European defense arrangements, which are newly fragmented by the Russian invasion of Ukraine**.9 EU efforts to build an independent regional defense profile and nurture cooperation between Europe’s defense industry and national defense communities reflect a growing recognition that the region needs to become a self-reliant defense actor. However, Europe still needs to demonstrate that self-reliance does not imply merely focusing on Europe’s periphery. Otherwise, the industrial challenges from China may outcompete Europe’s defense industry. Shipbuilding is a case in point. By 2021, China built 50 percent of all existing ships in the world. Through design collaboration agreements, cyber espionage, and acquisitions, China has copied advanced innovative ship designs. Enormous financial resources from the state allow Chinese companies to enjoy economies of scale by building dual-use factories which not only outcompete Western companies in the commercial shipbuilding industry, but also threaten the production of navy vessels. If not taken seriously, Europe and the US may soon have no choice but to buy frigates from China.10 This example demonstrates the centrality of China for global economic and security developments and should encourage Europe to manifest a position of unified strength in defending NATO member states against Chinese security challenges. This realization will help convince the US and its adversaries that Europe continues to be a credible partner in countering common threats against transatlantic security, whether they appear in or beyond the European region. China’s challenges to US and European security constitute such common threats across a broad range of sectors. These include gradual reinterpretations of principles of international law, the subversion of universal liberal market economic practices, and cyber insurgencies targeting a wide range of civilian and military entities. These Chinese policies all have major military implications because they are related to developments in the operating principles, capabilities, and priorities of China’s armed forces. Only NATO can offer an integrated transatlantic response to the military aspects of Chinese policies that threaten those sectors across the globe, including European actors. NATO’s involvement is essential if the credibility of the alliance’s security guarantees is to be preserved and an effective response to China’s encroachments on a liberal rules-based order is to be established. NATO’s involvement is essential to establish an effective response to China The omnipresent character of the China threat demonstrates that it is long overdue for NATO to position itself as a significant player in addressing Beijing’s challenges to transatlantic security. NATO is key to keeping US and European security policies coordinated when applying mechanisms of deterrence and defense against Chinese challenges. If transatlantic unity of purpose is lost, both the US and Europe are far less likely to succeed in addressing China sufficiently.

#### China-Taiwan war goes nuclear. Deterrence is key. It’s fast and more probable than European war.

Pettyjohn and Wasser 5-20-2022, \*senior fellow and director of the defense program at the Center for a New American Security, \*\*fellow in the defense program and co-lead of The Gaming Lab at the Center for a New American Security (Stacie and Becca, “A Fight Over Taiwan Could Go Nuclear,” *Foreign Affairs*, <https://www.foreignaffairs.com/articles/china/2022-05-20/fight-over-taiwan-could-go-nuclear/)//BB>

Russia’s invasion of Ukraine has raised the specter of nuclear war, as Russian President Vladimir Putin has placed his nuclear forces at an elevated state of alert and has warned that any effort by outside parties to interfere in the war would result in “consequences you have never seen.” Such saber-rattling has understandably made headlines and drawn notice in Washington. But if China attempted to forcibly invade Taiwan and the United States came to Taipei’s aid, the threat of escalation could outstrip even the current nerve-wracking situation in Europe. A recent war game, conducted by the Center for a New American Security in conjunction with the NBC program “Meet the Press,” demonstrated just how quickly such a conflict could escalate. The game posited a fictional crisis set in 2027, with the aim of examining how the United States and China might act under a certain set of conditions. The game demonstrated that China’s military modernization and expansion of its nuclear arsenal—not to mention the importance Beijing places on unification with Taiwan—mean that, in the real world, a fight between China and the United States could very well go nuclear. Beijing views Taiwan as a breakaway republic. If the Chinese Communist Party decides to invade the island, its leaders may not be able to accept failure without seriously harming the regime’s legitimacy. Thus, the CCP might be willing to take significant risks to ensure that the conflict ends on terms that it finds acceptable. That would mean convincing the United States and its allies that the costs of defending Taiwan are so high that it is not worth contesting the invasion. While China has several ways to achieve that goal, from Beijing’s perspective, using nuclear weapons may be the most effective means to keep the United States out of the conflict. China is several decades into transforming its People’s Liberation Army (PLA) into what the Chinese President Xi Jinping has called a “world-class military” that could defeat any third party that comes to Taiwan’s defense. China’s warfighting strategy, known as “anti-access/area denial,” rests on being able to project conventional military power out several thousand miles in order to prevent the American military, in particular, from effectively countering a Chinese attack on Taiwan. Meanwhile, a growing nuclear arsenal provides Beijing with coercive leverage as well as potentially new warfighting capabilities, which could increase the risks of war and escalation. China has historically possessed only a few hundred ground-based nuclear weapons. But last year, nuclear scholars at the James Martin Center for Nonproliferation Studies and the Federation of American Scientists identified three missile silo fields under construction in the Xinjiang region. The Financial Times reported that China might have carried out tests of hypersonic gliders as a part of an orbital bombardment system that could evade missile defenses and deliver nuclear weapons to targets in the continental United States. The U.S. Department of Defense projects that by 2030, China will have around 1,000 deliverable warheads—more than triple the number it currently possesses. Based on these projections, Chinese leaders may believe that as early as five years from now the PLA will have made enough conventional and nuclear gains that it could fight and win a war to unify with Taiwan. Our recent war game—in which members of Congress, former government officials, and subject matter experts assumed the roles of senior national security decision makers in China and the United States—illustrated that a U.S.-Chinese war could escalate quickly. For one thing, it showed that both countries would face operational incentives to strike military forces on the other’s territory. In the game, such strikes were intended to be calibrated to avoid escalation; both sides tried to walk a fine line by attacking only military targets. But such attacks crossed red lines for both countries, and produced a tit-for-tat cycle of attacks that broadened the scope and intensity of the conflict. For instance, in the simulation, China launched a preemptive attack against key U.S. bases in the Indo-Pacific region. The attacks targeted Guam, in particular, because it is a forward operating base critical to U.S. military operations in Asia, and because since it is a territory, and not a U.S. state, the Chinese team viewed striking it as less escalatory than attacking other possible targets. In response, the United States targeted Chinese military ships in ports and surrounding facilities, but refrained from other attacks on the Chinese mainland. Nevertheless, both sides perceived these strikes as attacks on their home territory, crossing an important threshold. Instead of mirror-imaging their own concerns about attacks on their territory, each side justified the initial blows as military necessities that were limited in nature and would be seen by the other as such. Responses to the initial strikes only escalated things further as the U.S. team responded to China’s moves by hitting targets in mainland China, and the Chinese team responded to Washington’s strikes by attacking sites in Hawaii. A NEW ERA One particularly alarming finding from the war game is that China found it necessary to threaten to go nuclear from the start in order to ward off outside support for Taiwan. This threat was repeated throughout the game, particularly after mainland China had been attacked. At times, efforts to erode Washington’s will so that it would back down from the fight received greater attention by the China team than the invasion of Taiwan itself. But China had difficulty convincing the United States that its nuclear threats were credible. In real life, China’s significant and recent changes to its nuclear posture and readiness may impact other nations’ views, as its nuclear threats may not be viewed as credible given its stated doctrine of no first use, its smaller but burgeoning nuclear arsenal, and lack of experience making nuclear threats. This may push China to preemptively detonate a nuclear weapon to reinforce the credibility of its warning. China might also resort to a demonstration of its nuclear might because of constraints on its long-range conventional strike capabilities. Five years from now, the PLA still will have a very limited ability to launch conventional attacks beyond locations in the “second island chain” in the Pacific; namely, Guam and Palau. Unable to strike the U.S. homeland with conventional weapons, China would struggle to impose costs on the American people. Up until a certain point in the game, the U.S. team felt its larger nuclear arsenal was sufficient to deter escalation and did not fully appreciate the seriousness of China’s threats. As a result, China felt it needed to escalate significantly to send a message that the U.S. homeland could be at risk if Washington did not back down. Despite China’s stated “no-first use” nuclear policy, the war game resulted in Beijing detonating a nuclear weapon off the coast of Hawaii as a demonstration. The attack caused relatively little destruction, as the electromagnetic pulse only damaged the electronics of ships in the immediate vicinity but did not directly impact the U.S. state. The war game ended before the U.S. team could respond, but it is likely that the first use of a nuclear weapon since World War II would have provoked a response. The most likely paths to nuclear escalation in a fight between the United States and China are different from those that were most likely during the Cold War. The Soviet Union and the United States feared a massive, bolt-from-the-blue nuclear attack, which would precipitate a full-scale strategic exchange. In a confrontation over Taiwan, however, Beijing could employ nuclear weapons in a more limited way to signal resolve or to improve its chances of winning on the battlefield. It is unclear how a war would proceed after that kind of limited nuclear use and whether the United States could de-escalate the situation while still achieving its objectives. AN OUNCE OF PREVENTION The clear lesson from the war game is that the United States needs to strengthen its conventional capabilities in the Indo-Pacific to ensure that China never views an invasion of Taiwan as a prudent tactical move. To do so, the United States will need to commit to maintaining its conventional military superiority by expanding its stockpiles of long-range munitions and investing in undersea capabilities. Washington must also be able to conduct offensive operations inside the first and second island chains even while under attack. This will require access to new bases to distribute U.S. forces, enhance their survivability, and ensure that they can effectively defend Taiwan in the face of China’s attacks. Moreover, the United States needs to develop an integrated network of partners willing to contribute to Taiwan’s defense. Allies are an asymmetric advantage: the United States has them, and China does not. The United States should deepen strategic and operational planning with key partners to send a strong signal of resolve to China. As part of these planning efforts, the United States and its allies will need to develop war-winning military strategies that do not cross Chinese red-lines. The game highlighted just how difficult this task may be; what it did not highlight is the complexity of developing military strategies that integrate the strategic objectives and military capacities of multiple nations. Moving forward, military planners in the United States and in Washington’s allies and partners must grapple with the fact that, in a conflict over Taiwan, China would consider all conventional and nuclear options to be on the table. And the United States is running out of time to strengthen deterrence and keep China from believing an invasion of Taiwan could be successful. The biggest risk is that Washington and its friends choose not to seize the moment and act: a year or two from now, it might already be too late.

## \*\*Cyber Scenarios\*\*

### 2AC Iran Cyber

#### The US’s cybersecurity sucks---Iran has been conducting successful OCOs and is more progressed than the US

Eric Rosenbaum, senior editor of CNBC.com, 11-18-2021, “Iran is ‘leapfrogging our defenses’ in a cyber war ‘my gut is we lose’: Hacking expert Kevin Mandia ,” CNBC, https://www.cnbc.com/2021/11/18/iran-leapfrogging-our-defenses-in-cyber-war-hacking-expert-mandia-.html

On Thursday, a federal grand jury indicted two **Iranian hackers** for **election interference** that included obtaining confidential voter information from at least one state’s election website for a **cyber-based disinformation campaign** targeting 100,000 Americans. Earlier this week, the U.S. government warned that Iranian hackers also have been on the **ransomware offensive**. To Kevin Mandia, the CEO of cybersecurity firm Mandiant, Iran’s success in the hacking realm is no surprise, as the nation has been upping its **cyber-offensive capabilities** for years to take advantage of U.S. weaknesses. Iran has progressed well beyond the first few stages of **cyber evolution** — defending its government in cyberspace and targeting its closest geographic foes, the immediate threats, which in Iran’s case would include the back and forth between itself and Israel in the cyber realm. “There was a time when we responded to Iran, their operators looked like they just got out of the classroom,” Mandia said during an interview with CNBC’s Eamon Javers at the CNBC Technology Executive Council Summit in New York City on Wednesday. “And we’re like god, you know ... they just compressed the C drive, why not just compress what you’re going to steal?” “But that was 14 years ago,” said Mandia, who has been monitoring cyber campaigns by Iran since 2008. “Come today, they’re **operating with efficiency**, they’re operating with **malware** that can be updated. They have a framework where they can update their malware super fast,” he said. “So they can be very efficient ... **leapfrogging** our **defenses** as they learn. And that’s kind of a frustration. I’ve seen most modern nations do have that capability ...a framework where they can update quickly. Iran does have that framework.” He said Iran also is part of a group of nation-state actors that have **zero day capabilities** — referring to a disclosed vulnerability for which no official patches or security updates yet exist even though exploitation by hackers can have severe consequences — the most frustrating of all types of cyberattacks. “Russia, Iran, Israel, China, they all have zero day components and zero day capability, whether they develop themselves or buy from someone, Iran’s gone through that rites of passage is well,” said Mandia, whose firm was the first to warn the U.S. government about the SolarWinds hack last year, the largest-ever attack on a software supply chain hitting both government agencies and private enterprise. The U.S. government alleges Russia was behind the hacking group that pulled off the cyberattack. Mandia, who served in the U.S. Air Force, said the nation’s physical military assets are ahead of its cyber assets, and there is no clear advantage in the real of cyber warfare. “In the cyber domain, we **don’t have dominance**,” he said. A U.S. workforce that is increasingly deployed on a global scale, as well as our early adoption of the internet economy and its evolution, all contribute to increased vulnerabilities as geopolitical rivals become more sophisticated in the cyber realm. Even if the U.S. has the best zero day capabilities, the nature of cyber warfare doesn’t favor a win for the U.S., he said. “My gut is we lose, because we’re in a glass house attacking mud huts. It’s just too asymmetric. And I don’t want to liken another country’s economy to a mud hut. But I’m saying in the cyber domain, the asymmetry, I think more people are **taking advantage** of the United States, and our openness. ... In my opinion, cyberattacks are also **more effective** against United States than against other nations.”

**Iran will escalate GPS attacks, causing escalation**

Micah **Halpern 19**, former lecturer at Yale, political and foreign affairs commentator, 8-8-2019, “Iran Plays a Dangerous Hi-Tech Game,” https://www.newsmax.com/micahhalpern/strait-of-hormuz-jamming-centcom/2019/08/08/id/927875/

Iran is playing dirty tricks in and around the Strait of Hormuz. To begin with, they are **jamming the GPS of tankers**, causing ships to wander off course —and in to their waters. They are also **spoofing andradioing the vessels**, proporting to be friendly and even **U.S. navy ships**. Over the years the Iranian leadership has perfected the art of mixing and matching partial truths with outright lies in order to advance their agenda. They want to convince global observers that it is the Iranian leadership who are the innocent victims, innocent victims targeted by organized Western aggression. In this case Iranians are deliberately dogging, misleading and **luring ships off course**. Their actions have turned into **a war of jamming**. Like most everything else they engage in, for Iran this is serious business. Globally this is **extremely dangerous**. We are seeing signs **all over the Mideast**. The U.S. Department of Transportation Maritime Division published a public warning to all ships and companies traveling in the region alerting them that Iran "spoofed bridge-to-bridge communications from unknown entities falsely claiming to be U.S. or coalition warships." U.S. Central Command (CENTCOM) said in a statement, "Due to the heightened regional tensions, **the potential for miscalculation** or misidentification **could lead to aggressive actions** against vessels belonging to US, **allied** and coalition partners operating in the **Arabian Gulf**, **Strait of Hormuz**, **and Gulf of Oman** . . . **GPS interference**, bridge-to-bridge communications **spoofing**, and/or other communications jamming with little to no warning." Bridge-to-bridge communication is when ships speak to one another. Iran has been become **expert** at jamming. That shouldn’t come as a big surprise given that as far back as 2012 the Iranian government has been jamming their own citizens. Back then, Iran replaced a series of short flagpoles scattered around their country with huge flagpoles – all the better to hide their jamming devices. The newer, taller, flagpoles sprouted up almost everywhere. The Iranian regime was attempting to stop all forms of social media and messaging. Their citizens were using satellites to communicate and find out the truth about what was happening in the world and that was not what Iranian leadership wanted. The **Russians**, too, have become **very good at GPS jamming**. Intelligence analysts report that Russia is jamming not waterways, but airspace, specifically the airspace around **Syria**. And that means that Russia is now capable of jamming communication for the **new US stealth fighter jet, the F-35**. This may be an exaggeration -I am skeptical that Russia is that sophisticated. Even more worrisome than all of this is a report that was issued this summer by the International Federation of Airline Pilots Association. The report details that pilots, landing in Tel Aviv’s Ben Gurion Airport in Israel, have lost GPS and that it is a recurring phenomenon. Thankfully, there are alternative tools that can be used to land and take off. Israel has said that they are dealing with the issue. But the mere presence of this issue demonstrates that we now live in a world hampered — **dangerously so**, **by a significant threat of jamming**. And this jamming can and is affecting more than ships at sea and military drones and jets in the sky, it is also targeting civilian aircraft with hundreds of civilian passengers aboard. When it comes to tech, Iran is highly skilled. They are developing their own tools and are using and adapting Russian and North Korean tech. **Jamming** and **spoofing by Iran** explains quite a lot of what has been happening in the Strait of Hormuz. Iran does not play games for fun. And this time, as always, the Iranians are playing by their own rules and they are playing **to win**.\

**Goes nuclear**

Kaveh L. **Afrasiabi &** Nader **Entessar 19,** Afrasiabi is an Iranian-American political scientist, Entessar is a professor of the department of political science and criminal justice at the University of South Alabama, 2-7-2019, “A nuclear war in the Persian Gulf?” https://thebulletin.org/2019/07/a-nuclear-war-in-the-persian-gulf/

Tensions between the **U**nited **S**tates and Iran are **spiraling toward a military confrontation** that carries a **real possibility** that the **U**nited **S**tates will use **nuclear weapons**. Iran’s assortment of asymmetrical capabilities—all constructed to be effective against the **U**nited **S**tates—nearly assures such a confrontation. The current US nuclear posture leaves the Trump administration at least open to the use of **tactical nuclear weapons** in **conventional theaters**. Some in the current administration may well think it to be in the best interest of the United States to seek a quick and decisive victory in the oil hub of the Persian Gulf—and to do so by **using its nuclear arsenal**. We believe there is a heightened possibility of a US-Iran war triggering a US nuclear strike for the following reasons: The sanction regime set against the Iranian economy is so brutal that it is likely to force Iran to take an action that will require a US military response. Unless the United States backs down from its present self-declared “economic warfare” against Iran, this will likely escalate to an open warfare between the two countries. In response to a White House request to draw up an Iran war plan, the Pentagon proposed sending 120,000 soldiers to the Persian Gulf. This force would augment the several thousands of troops already stationed in Iran’s vicinity. President Trump has also hinted that if need be, he will be sending “a lot more” troops. Defeating Iran through conventional military means would likely require a half million US forces and US preparedness for many casualties. The US nuclear posture review is worded in such a way that the use of tactical nuclear weapons in conventional theaters is envisaged, foreshadowing the concern that in a showdown with a menacing foe like Iran, the nuclear option is on the table. The United States could once again justify using nuclear force for the sake of a decisive victory and casualty-prevention, the logic used in Hiroshima and Nagasaki. Trump’s **cavalier attitude toward nuclear weapons**, **trigger-happy penchant**, and **utter disdain for Iran**, show that he would likely have no moral qualm about issuing an order to **launch a limited nuclear strike**, **especially in a US-Iran showdown**, one in which the oil transit from the Gulf would be imperiled, impacting the global economy and necessitating a speedy end to such a war.

### 2AC NoKo Cyber

#### North Korea is becoming increasingly capable at cyberattacks and will increase U.S. tensions and end any chance for US-North Korean coop

Benjamin R. Young 19, an assistant professor at the Wilder School of Government & Public Affairs at Virginia Commonwealth University, author of *Guns, Guerillas, and the Great Leader: North Korea and the Third World*, 2-4-2019, "North Korea Knows How Important Its Cyberattacks Are," Foreign Policy, https://foreignpolicy.com/2022/02/09/north-korea-knows-how-important-its-cyberattacks-are/

**No**rth **Ko**rea’s **cyberattacks** became famous in 2014, when Pyongyang’s **hackers targeted Sony** Pictures, seemingly in **retal**iation for a satirical movie about North Korean leader Kim Jong Un. But the reclusive regime’s greatly **improved cybercapabilities** are not a joke. They’re a serious threat to the stability of the **global economy** and **critical infrastructure** systems. North Korean hackers have gone on to **bigger** and more **financially profitable** targets. Since 2014, North Korean hackers have attacked Bangladesh’s **central bank**, the U.K. National **Health Service**, and, more recently, **cryptocurrency** exchanges. And the odds are that many more major North Korean cyberattacks are to come in the near future. In internal regime discourse, Pyongyang proudly refers to its cyberoperations as its “all-purpose sword.” According to testimony from a South Korean intelligence chief, Kim reportedly stated: “Cyberwarfare, along with nuclear weapons and missiles, is an ‘all-purpose sword’ that guarantees our military’s capability to strike relentlessly.” Subversive, criminal operations are a style of asymmetric warfare long embraced by the North. The country’s founding leader, Kim Il Sung, earned his nationalist credentials by fighting Japanese colonialists in the 1930s. His guerrilla band later became the political elite of the North Korean state. During the Cold War era, Kim regularly deployed guerrillas to subvert and instigate the South Korean government. North Koreas hackers are the 21st-century version of guerrilla fighters, moving in the dark and striking at the most vulnerable points. Historically, guerrillas often depended on banditry and robbery to survive—and one reason for the recent amping up of cyberattacks is financial worries. While Kim Jong Un’s recent missile tests garner international condemnation and head-shaking in Washington and Seoul, Pyongyang’s cyberoperatives work in the shadows. Due to the COVID-19 pandemic, North Korean borders have been sealed shut for the past two years. North Korean trade with China has largely stalled, and many foreign diplomats have left the country, making the already reclusive state even more isolated. Nonetheless, North Korean hackers work diligently in an effort to bolster the depleted coffers of the party elite. Between 2011 and 2020, **No**rth **Ko**rea **cybercriminals** stole more than **$1 billion** worth of **cryptocurrency**. In 2021, North Korean hackers allegedly stole close to **$400 million** worth of **crypto coins**. The blockchain analysis company Chainalysis wrote in a recent report that “North Korean cybercriminals had a banner year in 2021.” The regime’s investment in its cyberoperations is likely providing a vital economic buffer for the isolated and paranoid leadership. According to an unclassified 2021 report from the U.S. Office of the Director of National Intelligence (ODNI), North Korea’s cybercrime likely **funds** “government priorities, such as its **nuclear and missile programs**.” North Korea is also engaged in more **conventional espionage**. A cybersecurity firm recently uncovered that the North Korean hacking group Lazarus used two decoy Microsoft Word documents that resembled Lockheed Martin employment information in order to deliver payloads on unsuspecting users. Using spear-phishing attacks, the Lazarus group has **increasingly targeted** job-seekers in the **U.S. defense** and aerospace industries with fake documents that are **infected with malware**. Despite relatively good relations between Pyongyang and Moscow, North Korean hackers have even **targeted Russia**’s foreign ministry **with malware**. In what seems to be a counterstrike against the analysts who uncover their hacking operations, Pyongyang’s cyberagents are using fake social media profiles to infect the computers of cybersecurity researchers with custom backdoor malware. So, why have foreign-policy experts and policymakers themselves largely ignored North Korea’s increasingly sophisticated cyberoperations? Well, firstly, cyberattacks are less obvious than missile tests. Kim’s numerous missile tests are a frequent and unignorable reminder of his regime’s nuclear arsenal and military capabilities. Cyberattacks take place in the dark corners of the internet and are not always obvious to even the targets. Secondly, most policymakers **struggle** with understanding that North Korea is a technological peer nation in cybersecurity. Despite being a deeply impoverished country with a crumbling health care system and less than 10 percent of its non-highway roads paved, the North Korean leadership has attained significant expertise and development in its cybersector. As part of its militaristic worldview, North Korea prioritizes investment in regime stability and the defense industry over economic improvement for its citizens. North Korea’s asymmetric capabilities have allowed a nation with a GDP roughly equivalent to that of Mozambique to be able to compete with the world superpowers in cyberspace. The stereotype of North Korea’s Kim Jong Un as a buffoonish character on the international stage has impeded U.S. strategic thinking toward North Korea as a very real threat in cyberspace. And finally, fearing financial loss and public relations fiascos, companies and businesses are **hesitant to release information** to the public about North Korean cyberattacks. Since many CEOs solely prioritize their company’s bottom line, details of cyberattacks often get swept under the rug. In 2016, the FBI’s Internal Crime Complaint Center estimated that only 15 percent of cybertheft victims in the United States reported their crimes to law enforcement. So, what can be done to bolster defenses against North Korean hackers? Cyberattacks are part of North Korea’s historical commitment to asymmetric warfare, and it will not change course no matter how much we publicly condemn its actions. Rhetoric won’t work unless it has teeth. Guerrilla warfare, in cyberspace and the physical world, has long been embraced by the regime. The United States needs to **address** the role and complicity of the Chinese Communist Party (**CCP**) in North Korea’s **cyberoperations**. From hosting North Korean cyberunits in border cities such as Shenyang to training them at Chinese technology universities and research institutes, the CCP enables North Korea’s **maliciousness** in cyberspace. In 2016, a South Korean cybersecurity researcher estimated that around 600 to 1,000 North Korean cyberwarfare agents operate in China. In addition, most, if not all, of the internet traffic from North Korea runs through Chinese access providers. Many North Korean hackers get their education in China’s tech universities and then bring back their skills to their homeland. We need to cut off this supply of North Korean hackers and address the fact that the Chinese government knowingly enables North Korea’s malicious cyberoperations. In October 2020, John Demers, then the U.S. assistant attorney general for national security, mentioned at a think tank event that “there is support through Chinese cyberinfrastructure. There’s likely support in terms of sharing expertise and training from the Chinese side.” Since the U.S. national security apparatus seemingly acknowledges this Sino-North Korean cyberpartnership, the U.S. government should sanction the Chinese entities that enable and assist North Korean cybercrime, such as the Harbin Institute of Technology, which hosts North Korean computer science students. In 2019, China’s education minister signed an agreement with the North Korean government on the continuation of educational exchanges and partnerships from 2020 to 2030. The Chinese government will continue to see North Korean cybercapabilities as a useful proxy force to weaken and frustrate U.S. interests. Finally, U.S. companies and businesses need to **share information** about North Korean cyberattacks with the general public so that others can act to prepare themselves. As noted in the ODNI report, North Korea “probably possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks in the United States.” The last thing anyone needs during the pandemic is an already brittle critical infrastructure to be at the mercy of Kim Jong Un.

**Cooperation is key to prevent US-North Korean nuclear war**

**Ikegami 17** Masako Ikegami is a professor in the Department of Innovation Science at the School of Technology and Environment at the Tokyo Institute of Technology. Previously, she was director of (and a professor at) the Center for Pacific Asia Studies at Stockholm University. Her research interests include Asian security; conflict prevention and confidence building; arms control, disarmament, and nonproliferation; and science, technology, and society issues. She holds a doctorate in sociology from the University of Tokyo and a Ph.D. in peace and conflict research from Uppsala University in Sweden. Ikegami has been an active member in the Pugwash Conferences on Science and World Affairs, and was Abe Fellow at the East-West Center in Washington, D.C. and Honolulu in 2011–2012. By Masako Ikegami, June 15, 2017 Prevent nuclear catastrophe: Finally end the Korean War https://thebulletin.org/2017/06/prevent-nuclear-catastrophe-finally-end-the-korean-war/

The long-simmering confrontation between the United States and North Korea has reached a moment of unprecedented tension. The risk that unintended war will break out due to misjudgment is high. Indeed, as others have observed, East Asia is witnessing a “Cuban Missile Crisis in slow motion.”

According to Graham Allison, director of Harvard University’s Belfer Center for Science and International Affairs, it is now time “to examine previously unthinkable options” on the Korean Peninsula—such as scaling back joint US-South Korean military exercises in exchange for a freeze on North Korean tests of intercontinental ballistic missiles. Considering these “unthinkable” options, Allison writes, would follow in a tradition established during the Cuban Missile Crisis by John Kennedy and Nikita Khrushchev, who both “blinked,” and whose behavior ultimately amounted to cooperative crisis management. One of the most unthinkable options for the Korean Peninsula—but perhaps the most promising—is for the United States and China to finally pursue a formal end to the Korean War.

Two main stakeholders. The situation on the Korean Peninsula today is fraught, to say the least. North Korea remains in diplomatic isolation. It has continued testing nuclear weapons and ballistic missiles, resulting in further escalation of tensions. The United States and South Korea have exhibited increasing hawkishness, stepping up joint military exercises that center on striking key facilities in North Korea as well as the country’s leadership (“decapitation”). Washington and Seoul’s combined forces have enhanced their preemptive strike capability—but if US-South Korean forces attacked the North in the name of counterproliferation or regime change, the result would inevitably be all-out war and region-wide catastrophe.

Arguably, the US-North Korea confrontation has reached the level of mutually assured destruction. The two sides’ military capabilities are not rigorously balanced, as Washington and Moscow’s nuclear second-strike capabilities were balanced during the Cold War. But a military confrontation would cause intolerable damage to both sides and catastrophe for the whole region. Seoul would become an inferno. In Japan, nuclear power plants and US military bases would be targeted with missiles. North Korea’s special forces might resort to guerrilla or terrorist tactics involving weapons of mass destruction. Perhaps even Yanbian, a Chinese region near the North Korean border with a large population of ethnic Koreans, would be destabilized. The use of force is therefore not an option. The only viable solution to the North Korean nuclear crisis is cooperative crisis management. Previously unthinkable options simply must be explored.

But the stakeholders who can end the nuclear crisis are not the United States and North Korea. Instead, as Allison has correctly suggested, they are the United States and China. This is not merely because the United States, as the region’s predominant military power, is exerting military pressure on North Korea, or that Beijing provides Pyongyang an economic lifeline (making China the gatekeeper for international economic sanctions against the North). Rather, Washington and Beijing hold the key to ending the crisis because they are the key signatories of the Korean War Armistice Agreement—which brought Korean War hostilities to an end but left the war itself in a state of suspended animation.

To this day, despite rhetorical frictions between Beijing and Pyongyang, China and North Korea share a “blood alliance” forged during the Korean War. The latest research on the war—based on declassified North Korean military documents that US and UN forces seized during the war, as well as on archival materials from Russia and China—reveals that Mao Zedong played a more active role in initiating the war than previously understood. China is usually portrayed as entering the war in October 1950, after UN forces, pursuing a counterattack against North Korea, reached the neighborhood of the Yalu River, which forms the border between China and North Korea. But well before then—indeed, well before the outbreak of war in June 1950—Mao had made a strategic decision to support Kim Il-sung’s invasion of the South. Kim badly needed a larger army if he was to invade the South, and in the summer of 1949 Mao granted him approximately 30,000 ethnic Korean troops from the People’s Liberation Army (PLA), fully equipped with modern arms left by the Soviet Red Army upon its departure from the country in 1948, and with additional supplies from the PLA. In the early stages of China’s civil war, the 166th Division—an elite PLA force comprised of ethnic Koreans—had formed the backbone of Communist forces fighting Chiang Kai-shek’s Nationalist forces in Manchuria. Now these troops were transferred to Kim’s command, reappearing as the 6th Division of the Korean People’s Army (KPA). The 6th Division played a decisive role in the Korean War—launching an initial surprise attack against Kaesong on June 25, 1950, paving the way for the KPA’s 3rd Division to mount a lightning attack against Seoul on June 28, with the fighting then continuing south to Taejon. (Much of this only became clear with the 1993 publication of a study by Ryo Hagiwara known in English as The Korean War: A Conspiracy of Kim Il-sung and MacArthur.)

More than just a blood alliance, however, explains China’s behavior on the Korean Peninsula today. Just as Nikita Khrushchev deployed nuclear-armed missiles in Cuba to strengthen the Soviet Union’s strategic position vis-à-vis the United States, China depends on heavily-armed North Korea to help neutralize US forces in East Asia. The only real difference is that Beijing is savvy enough to disguise its actions—to let the confrontation on the Peninsula be perceived as involving merely the United States and North Korea.

In fact, as Graham Allison has pointed out with considerable insight, the real animating force behind the North Korean nuclear crisis, and indeed behind tensions on the Korean Peninsula since the end of the Korean War, is strategic confrontation between the United States and China. It is therefore the responsibility of Beijing and Washington to reduce the tensions that could cause a catastrophic war. The two sides would do well to heed the lesson that Kennedy drew from the Cuban Missile Crisis—that “while defending our own vital interests, nuclear powers must avert those confrontations which bring an adversary to a choice of either a humiliating retreat or a nuclear war.”

Now is the time. Among previously unthinkable measures to end the North Korean nuclear crisis, the most effective would be simply to formally end the abnormally protracted Korean War. After all, the root cause of the North Korean nuclear crisis is an ongoing Korean Cold War—contested between the United States and China (and at one time, discreetly, by the Soviet Union) but disguised as an ideological battle over Korean unification, with North and South contending for regime legitimacy. But the Korean Cold War has now reached the threshold of nuclear catastrophe, and it must end. Ending the war would reduce North Korea’s motivation to assert the legitimacy of its regime, or guard against “US nuclear blackmail,” by equipping itself with nuclear-armed missiles. And China, freed from concerns that war would break out on the peninsula or that the North Korean regime would collapse, would be able to implement more effective economic sanctions against North Korea and thereby contain nuclear proliferation.

If Washington and Beijing committed themselves to the project, negotiations toward a formal peace treaty would not have to be exceedingly complicated. The parties could agree to minimal preconditions: North Korea would stop its missile and nuclear tests while the United States and South Korea would agree to constrain their joint military exercises (an idea already proposed by Chinese Foreign Minister Wang Yi). Kim Jong-un, meanwhile, could be sidelined during the talks, just as Fidel Castro was left completely out of communications between Washington and Moscow at the critical moments of the Cuban Missile Crisis. After the crisis, Castro and his regime survived for more than half a century, contending with economic sanctions and causing the rest of the world only modest problems.

When the Korean War is finally concluded, a new regional confidence-building framework, based on the erstwhile six-party talks, could be established—in much the same way that Washington and Moscow established a crisis hotline following the Cuban Missile Crisis. Formally ending the Korean War should be the beginning, not the end, of a years-long process of denuclearizing North Korea. It could even lead to the establishment of an East Asian nuclear-weapon-free zone. In any event, now is the time for Presidents Donald Trump and Xi Jinping to cooperate, as Kennedy and Khrushchev cooperated before them, to prevent nuclear catastrophe and negotiate a peace agreement for the Korean Peninsula.

### 2AC Cyberterror

#### Emerging tech makes terrorist cyberattacks a viable option

Antonio Missiroli 19, the Assistant Secretary General for Emerging Security Challenges, a professional journalist, taught Boston University, Johns Hopkins, College of Europe (Bruges) and Sciences Po (Paris), 1-7-2019, “NATO and the South,” <http://www.realinstitutoelcano.org/wps/portal/rielcano_en/contenido?WCM_GLOBAL_CONTEXT=/elcano/elcano_in/zonas_in/missiroli-nato-and-the-south>

Terrorists are also making an increasing use of modern technologies. While there have been no cases of ‘cyber-terrorism’ –ie, no proved terrorist act carried out through cyber means only– terrorist groups have indeed used cyberspace for recruitment and funding as well as operational purposes. This is an area where intelligence agencies are very busy and alert, although these activities are unlikely to reach the level of sophistication and disruption that only State-sponsored groups can achieve in this domain. There is, however, a growing concern about the possible use of unmanned vehicles for kinetic terrorist attacks –and not only on the battlefield (where they have already occurred) but also in civilian and especially urban environments–. What happened around Christmas 2018 at Gatwick airport in London was quite telling, especially in light of the commercial affordability and availability of such tools and their potential impact on civilian life. NATO has just launched a specific initiative to counter –on the battlefield but potentially also elsewhere– such a misuse of new technologies by terrorists.

#### Nuclear terror causes extinction

Irma Arguello and Emiliano Buis, 18 – \*Irma, Founder and Chair of the NPSGlobal Foundation (Non-proliferation for Global Security), degree in Phyisics Science from the University of Buenos Aires, Master degree in Business Administration from IDEA/Wharton School, Defense and Security studies (Master level) at the Escuela de Defensa Nacional, Argentina; \*\*Emiliano, lawyer and associate professor of public international law, international humanitarian law, international law of disarmament, and the origins of international law in antiquity (Irma Arguello & Emiliano J. Buis, **“**The global impacts of a terrorist nuclear attack: What would happen? What should we do?,” *Bulletin of the Atomic Scientists*, 2018, https://doi.org/10.1080/00963402.2018.1436812)

But the consequences would go far beyond the effects in the target country, however, and promptly propagate worldwide. Global and national security, economy and finance, international governance and its framework, national political systems, and the behavior of governments and individuals would all be put under severe trial. The severity of the effects at a national level, however, would depend on the countries’ level of development, geopolitical location, and resilience. Global security and regional/national defense schemes would be strongly affected. An increase in global distrust would spark rising tensions among countries and blocs, that could even lead to the brink of nuclear weapons use by states (if, for instance, a sponsor country is identified). The consequences of such a shocking scenario would include a decrease in states’ self-control, an escalation of present conflicts and the emergence of new ones, accompanied by an increase in military unilateralism and military expenditures. Regarding the economic and financial impacts, a severe global economic depression would rise from the attack, likely lasting for years. Its duration would be strongly dependent on the course of the crisis. The main results of such a crisis would include a 2 percent fall of growth in global Gross Domestic Product, and a 4 percent decline of international trade in the two years following the attack (cf. Figure 3). In the case of developing and less-developed countries, the economic impacts would also include a shortage of high-technology products such as medicines, as well as a fall in foreign direct investment and a severe decline of international humanitarian aid toward low-income countries. We expect an increase of unemployment and poverty in all countries. Global poverty would raise about 4 percent after the attack, which implies that at least 30 million more people would be living in extreme poverty, in addition to the current estimated 767 million. In the area of international relations, we would expect a breakdown of key doctrines involving politics, security, and relations among states. These international tensions could lead to a collapse of the nuclear order as we know it today, with a consequent setback of nuclear disarmament and nonproliferation commitments. In other words, the whole system based on the Nuclear Non- Proliferation Treaty would be put under severe trial. After the attack, there would be a reassessment of existing security doctrines, and a deep review of concepts such as nuclear deterrence, no-firstuse, proportionality, and negative security assurances. Finally, the behavior of governments and individuals would also change radically. Internal chaos fueled by the media and social networks would threaten governance at all levels, with greater impact on those countries with weak institutional frameworks. Social turbulence would emerge in most countries, with consequent attempts by governments to impose restrictions on personal freedoms to preserve order – possibly by declaring a state of siege or state of emergency – and legislation would surely become tougher on human rights. There would also be a significant increase in social fragmentation – with a deepening of antagonistic views, mistrust, and intolerance, both within countries and towards others – and a resurgence of large-scale social movements fostered by ideological interests and easily mobilized through social media.

### 1ac Russian Cyberattacks Extension

#### Escalation is likely

Mathew J. Schwartz, executive editor, DataBreachToday and for European news coverage, 5-13-2022, "Russia-Ukraine War: Cyberattack Escalation Risk Continues," No Publication, https://www.bankinfosecurity.com/blogs/russia-ukraine-war-cyberattack-escalation-risk-continues-p-3231

While Ukraine remains at risk, of course, so too do any countries whose governments have been siding against Russia. Thankfully, however, so far the impact of online attacks has been much less than many analysts had feared, as Russia appears to remain much more focused on physical attacks. "Perhaps the concept of a 'cyber war' was over-hyped," Jeremy Fleming, director of the U.K.'s security, intelligence and cyber agency, GCHQ, said earlier this week with classic British understatement. "But there's **plenty of cyber** about, including a range of activity we and partners have attributed to Russia," Fleming said Tuesday at the CyberUK conference in Wales. "We've seen what looks like some **spillover** of activity affecting other countries. And we've seen indications that Russia's cyber operatives continue to look for targets in countries that oppose their actions." "What we were expecting was, of course, a massive cyber campaign with more spillovers," Juhan Lepassaar, executive director of the EU Agency of Cybersecurity, known as ENISA, said at the conference. Satellite Communications Disrupted Of course, there has been some **notable Russian hacking**, including the attack on **Viasat's KA-SAT satellite** communications terminals on Feb. 24 - the day Russia invaded Ukraine. This week, the EU, U.K., Ukraine and U.S. attributed that attack to Russia. "So yes, we've seen that, but we haven't seen a sustained effort," Lepassaar said (see: Russia-Ukraine War: 7 Cybersecurity Lessons Learned). Multiple strains of wiper malware have also been launched by Russia against Ukraine, experts say, including against energy facilities. But part of the challenge facing Moscow is that Ukraine has been devoting significant energy to shoring up its online defenses, backed by support from allies, as well as NATO. "The Ukrainians have been stress testing involuntarily since 2014," Lepassaar said of their online defenses. Likewise, Rob Joyce, the head of cybersecurity at the U.S. National Security Agency, has lauded the state of Ukraine's online defenses and told CyberUK attendees that Ukraine offers a model for others to emulate. "One of the things they've done is, they have emergency plans, having been under pressure for years," he said at the conference. "They have been able to practice and they understand what good incident response is." Even though so-called cyber war has failed to transpire, experts say the risk of inadvertent or intentional spillover remains high, especially for **critical infrastructure** sectors (see: 9 Essentials for Global CISOs During Russia's Ukraine War). "I'm still very worried about the threats emanating from around the Russia-Ukraine situation," Joyce told the BBC. This threat is being tracked at the highest levels of government. Joyce said the White House is continuing to closely monitoring the situation, not least given the ongoing risk that there would be "spillover of nation-state activity … continuing on to impact civil society." CISO Mandate: Stay Alert Hence while there's so far been no all-out cyber blitzkrieg, CISOs should - and must - continue to carefully track the conflict, given the risk that organizations might be affected by cyberattack spillover, if not directly targeted. Threat intelligence firm Flashpoint, for example, says it's been hearing this question regularly from the CISOs and other clients it continues to brief on the war: "How might decisions made by Western governments and commercial entities, such as economic sanctions, lead to an escalation in cyberspace and the physical world?" Another top concern, it says, remains which industries are most at risk and the types of attacks they should most beware. "When it comes to the cyber domain and the potential attacks on cyber infrastructure, it's something that we have to be very concerned about," said Max Bergmann, the Europe program director at the Center for Strategic and International Studies, in a Tuesday press briefing held by the Washington-based, bipartisan, nonprofit policy research organization on Tuesday. Likely Targets Flashpoint says the most likely targets for Russia remain Ukrainian **government and financial services** sites and "**military communication networks**" but that any escalation would likely focus on other countries' **financial services sectors** and likely include distributed denial-of-service attacks, phishing campaigns and worse. "Russian state-backed activity has so far focused on Ukrainian banks - Privatbank and Oschadbank were targeted before the February invasion - likely with the purpose of diminishing trust in the Ukrainian financial sector both in the Ukrainian population and among Western partners," Flashpoint says. "The likeliest form of attacks include those that were used against the Ukrainian banks - DDoS attacks, self-propagating wiper attacks, or attacks leveraging banks' compromised email infrastructure - as well as attacks focusing on cyberespionage with the purpose of aiding sanctions evasion." But Russia faces "some real challenges" if it tries to escalate, said Bergmann at CSIS. "It's a very different environment than last year when … Russia-linked cyber actors attacked the Colonial Pipeline and took that down when the Biden administration was in the midst of trying to sort of establish a detente with Russia," he said. "That is not the environment now, and as Russia has bogged down in Ukraine, I don't think they're going to want sort of an escalatory cycle when it comes to sort of provoking us to get more involved in the conflict or to take direct action in the cyber domain against them."

### 1ac NATO Cohesion Extension

#### NATO is key to avert all existential threats

Nicholas Burns 18, Barbara Goodman Family Professor of the Practice of Diplomacy and International Relations, Harvard Kennedy School; Director, American Secretaries of State Project, “Assessing the Value of the NATO Alliance.” Harvard’s Belfer Center. 9-5-2018. https://www.belfercenter.org/publication/assessing-value-nato-alliance

Mr. Chairman and Mr. Menendez, you have asked for an assessment of NATO’s value to the United States. In my judgment, NATO continues to be of vital importance to American security interests in five principal ways. First, NATO is at the core of one of the most significant foreign policy accomplishments in American history—the creation of a long-term peace in Europe following the close of the Second World War. Because of NATO and the emergence of the European Union, Europe is united after centuries of division and war. NATO’s military strength has been a major reason for the absence of war with the Soviet Union and Russia since 1949. A recent Atlantic Council study reminds that America spent 14.1 percent of its GDP on defense during the First World War, 37.5 percent during the Second World War and 13.2 percent during the Korean Conflict. We spend nothing close to those levels now in large part due to the great power peace we have enjoyed for over seventy years. NATO has been a major factor in that peace. And due to the expansion of NATO and the European Union eastward after the fall of the Soviet Union, millions of East Europeans now live in free, democratic societies—a significant success for U.S. diplomacy. Second, NATO delivers additional benefits to U.S. military objectives and operations beyond our shores. NATO is at the heart of our defense of North America and Europe from nuclear and conventional threats. British and French nuclear weapons join ours in deterring aggression in the North Atlantic area. Since the late 1940s, every Administration has believed that the best way to defend our country is through American forces forward deployed in Europe with the NATO allies. This strategy remains right for today given Russia’s invasion of Georgia in 2008, of Crimea and Eastern Ukraine in 2014 and its current pressure on Estonia, Latvia, Lithuania and Poland. NATO remains our primary vehicle for deterring Putin in Eastern Europe. The NATO allies host a great number of critical bases for U.S. forces—Ramstein in Germany, Aviano in Italy, Rota in Spain, Souda Bay in Greece and Incirlik in Turkey—that serve as a platform for our presence in Europe, as well as for U.S. force projection against terrorist groups in North Africa and the Middle East and for our continued military operations in Afghanistan. Europe is a critical link in the development of our Ballistic Missile Defense network focused on the Middle East with Turkey, Romania, Poland, Germany, Spain, the Netherlands, Denmark, the UK and other allies all hosting elements of this system. NATO allies continue to participate in the U.S.-led coalition against the Islamic State in the Middle East. Many of the allies play lead roles in other counter terror operations such as French forces in Mali supported by the U.S. In Afghanistan, the NATO allies remain with us in combat operations and in training the Afghan military. Over 1000 soldiers from European and other partner nations have died there during the last seventeen years. NATO continues to maintain the hard-earned peace in Kosovo with European troops bearing the large share of the burden. An EU-led force has taken on all of the peacekeeping responsibility in Bosnia, freeing up the U.S. for other activities. Third, the NATO allies are among our closest and most supportive global partners as we confront the great transnational challenges that define this century—the fight against terrorism, the entire complex of cyber threats, climate change, the risk of pandemics, mass migration and others. The NATO allies and our partners in the European Union act together with us on these and other issues. This is of incalculable benefit to the U.S. Neither Russia nor China have treaty allies. NATO is a significant advantage for the United States when it acts as a force multiplier for American interests.