# \*\*\*INFO WARFARE AFF\*\*\*

The information warfare aff and neg was produced by: Drew Chico; Cyrus Esmailzadeh; Maggie Howerton; Sarah Kwon; Lenox Leverett; Raleigh Maxwell; Avi Shah; Ahsan Tahirkheli; Cy Turner

# 1AC

## 1AC---Information Warfare

### 1AC---Russia Advantage

#### Advantage One is Russia

#### Russia’s dramatically increasing its information operations---they’re key to its broader geopolitical goals

Mark Scott 22, Chief Technology Correspondent at POLITICO, writing about the global collision of technology and politics “As Ukraine conflict heats up, so too does disinformation,” POLITICO, 1/27-/22, <https://www.politico.eu/article/russia-ukraine-disinformation-nato-united-states-special-forces-winter-olympics-moscow-kremlin-kyiv/> //chico

Ukrainian special forces planning so-called "false flag" operations. The United States considering chemical weapons attacks in the Eastern European country. NATO preparing to attack Russia during the upcoming Winter Olympics.

The Kremlin is ratcheting up its disinformation game with claims like these amid rising geopolitical tensions between Moscow and Western capitals, according to a review of state-backed media content over the last 10 days by POLITICO.

The campaign — spread via Moscow-backed outlets like RT, domestic state-owned broadcasters and fake social media accounts in multiple Western languages — coincides with a large-scale military buildup along the Ukrainian border and increased Western military aide to support Kyiv.

Moscow's goal, according to three Western national security officials and five external disinformation researchers, is to use wedge issues to foster division among Western countries over their support for Ukraine; counter NATO's claims against Moscow; and create plausible deniability over potential atrocities including the possible use of chemical weapons.

"Where they really are moving the needle is on undermining support for U.S. internationalism," said Bret Schafer, head of the information manipulation team at the German Marshall Fund's Alliance for Securing Democracy, in reference to the Kremlin's disinformation tactics.

"Russia state media messaging is more effective at chipping away at the West's geopolitical goals than it is in dividing the West because we do that well enough on our own," he added.

In recent weeks, Western governments have been particularly vocal about outing Russian online tactics. Two of the Western security officials, who spoke on the condition of anonymity to discuss governments' internal strategies, said the amped-up response was partly because Moscow has been successful in tilting public opinion around geopolitical issues in the past.

The U.S. State Department published a "cheat sheet" seeking to explain the Kremlin's online falsehoods, while also criticizing Moscow for its "disregard for truth." In the European Union, the so-called East Stratcom team within the European External Action Service, which is tasked with monitoring Russian online propaganda, highlighted the Kremlin's tactics, although the 27-country bloc is still divided over how strongly to push back against Moscow.

The Kremlin, in turn, has pushed back against the criticism, claiming that Western governments and media are peddling mistruths about the situation in Ukraine, and that it is Moscow, not Washington or Brussels, that is pushing for a peaceful resolution.

Just like 2014, but worse

Russia is no newcomer to disinformation on Ukraine.

Since the country annexed part of its neighbor in 2014, Kremlin-backed media has pumped out a steady stream of accusations that Kyiv is run by neo-Nazis; that NATO is either too weak to defend the country or too aggressive in its military stance; and that Western citizens did not see the point in protecting Ukraine.

Those narratives are being updated amid the current tensions.

Russian broadcasters have shaped the debate at home as President Vladimir Putin defending the interests of Greater Russia, including sending Russian troops to Belarus as a routine military maneuver with a close ally. On the Kremlin's international news outlets — which collectively have millions of followers on social media — the likes of RT and Sputnik have criticized Western leaders for spending resources on Ukraine amid the pandemic and questioned how defending Kyiv plays into the national interests of either the U.S. or EU countries.

"The pro-Kremlin disinformation machine uses a well-known tactic of throwing mud against a wall to see what sticks," said one of the Western officials, who was not authorized to speak publicly about their work tracking Russian online tactics. "There are a lot of contradictions but consistency has never been a strong suit of the Kremlin's disinformation machine. It’s rather about muddying the waters."

For Monika Richter, a former EU official specializing in disinformation and current head of research at Semantic Visions, a Prague-based intelligence firm, there's a disconnect between domestic propaganda, which has focused on framing NATO as the enemy and Ukraine as a means to obtaining security assurances from Washington, and the Kremlin's foreign media operations, which have been more aggressive in claiming that the West wants war in Eastern Europe.

"The outward disinformation campaign is rattling," she said. "It appears to be a coordinated effort to lay the groundwork ahead of another attack."

Chemical weapons and blaming NATO

Yet in recent days, specific themes have started to bubble to the surface.

One relates to accusations — mostly in non-English-language outlets — that either Ukraine or NATO could use chemical weapons within the country in the hope of blaming Russia for it. These messages were then picked up either by official diplomatic accounts or American entities like SouthFront — a think tank the U.S. State Department has tied to the Kremlin — and shared hundreds of times on social media, according to POLITICO's analysis via CrowdTangle, a social media analytics tool owned by Meta.

Another is that the West, not Russia, is the main driver in the potential conflict.

Across RT and Sputnik — in English, French, German and Spanish — reports highlighted how NATO countries had provided weapons to the Ukrainian government, and claimed that U.S. President Joe Biden was using the stand-off to boost his popularity at home. In multiple reports, again heavily shared on social media, RT articles questioned why the U.S. and Europe were supporting Ukraine when the COVID-19 pandemic was rife at home.

Russian-backed media has repeatedly captured significant attention among Western audiences, particularly those in Europe where anti-American sentiment has risen since 2016, according to the Pew Research Center. But Kremlin talking points also have seeped into mainstream U.S. media, particularly promoted by right-wing influencers who have no affiliation to Moscow and have tried to use the Ukrainian stand-off to attack Biden and his domestic agenda.

That includes raising questions about why Washington would enter the conflict in the first place, concerns that U.S. involvement in Ukraine could end similarly to what happened in Afghanistan, and calls for the Biden administration to focus on domestic, not foreign, issues.

“There’s an alignment of interests between the U.S. far right and the Russian government,” said Schafer of the German Marshall Fund. "It's exceptionally beneficial to have super mainstream U.S. voices parroting lines that Russia has been saying for years.”

#### Ukraine creates a tipping point in the broader information war---now’s key

Serge Schmemman 22, Times correspondent and bureau chief in Moscow, Pulitzer Prize recipient, 5/5/2022, "The Information War in Ukraine Is Far From Over: Serge Schmemann," <https://www.nytimes.com/2022/05/05/opinion/russia-ukraine-propaganda.html> , RMax

If the first casualty of war is truth, then the corollary in Ukraine is that information is the first battlefield.

That was where the war began, in early 2022, weeks before Vladimir Putin sent the first rockets, armored vehicles and troops into Ukraine, when he claimed that the massive buildup of troops along Ukraine’s borders was but another military exercise. And that was where the United States and its allies scored their first victories, when they made public intelligence anticipating the invasion and the pretext Mr. Putin would use for it.

Then, when the invasion began in February, Ukraine’s president, Volodymyr Zelensky, opened a second information front. He donned a soldier’s olive-drab T-shirt and issued a torrent of defiant tweets, speeches and images from devastated villages, much of it targeted at Russian audiences. His metamorphosis from a relatively unpopular president to a David defying Goliath has been instrumental in solidifying popular, military and economic support for Ukraine in the United States and Europe.

In these first information battles, the Americans and Ukrainians showed that they had learned the lessons of 2014, when Russia had the upper hand in propaganda, assaulting Crimea and eastern Ukraine while claiming to be responding to pleas from Russian-speaking residents. The United States and Ukraine have also been greatly aided this time around by the fact that the evidence of the invasion and its brutal consequences has been so well documented.

But the information war, like the physical war, is far from decided. Ten weeks into the war, many Russians seem to accept Mr. Putin’s narrative. Around the world, many countries remain on the sidelines or, like China, are on Russia’s side. While Washington’s public comments have served to bolster the Ukrainians and rally their allies, some of those comments have played directly into Mr. Putin’s claims of a malign America determined to neuter Russia, as when President Biden said of Mr. Putin, “This man cannot remain in power,” and Defense Secretary Lloyd Austin declared that America’s goal is a “weakened” Russia.

Russia was surprisingly slow to prepare its population or the world for a full-scale invasion, perhaps because its leaders were convinced that Kyiv would fall quickly. But after that slow start, the Kremlin went into high gear. Domestically, it shut down independent media outlets, quashed demonstrations and threatened anyone challenging the government line with “false information” about the invasion with up to 15 years in prison.

Russia was also quick to adapt its messaging to a changing battlefield. After Moscow shifted its focus from Kyiv to southeastern Ukraine, the goal of driving Nazis out of power in Kyiv shifted to a focus on Ukraine as an existential struggle for Holy Russia against an American hegemon and its NATO sidekicks. What began as a “special military operation” has morphed into a defensive war akin to World War II, the “Great Patriotic War,” in which Russia was last compelled to defend itself against Nazis and fascists.

“We broke the back of fascism,” declared Patriarch Kirill, the head of the Russian Orthodox Church and a staunch supporter of the war against Ukraine, in a sermon on April 3 that turned an unprovoked invasion into a noble crusade. On May 3 he ratcheted up the language: “We don’t want to fight anyone,” he said in a sermon in the Kremlin. “Russia has never attacked anyone. It is amazing that a great and powerful country never attacked anyone; it only defended its borders.”

How many Russians really believe this is hard to gauge, given the danger of disagreeing. There is considerable anecdotal evidence that the notions of a hostile NATO and treacherous Ukrainians are widely held, but there are also many reports of Russians horrified by the war but no longer able to speak out without immediate repression.

The info war has also reached Asia, Africa and South America, where Russia has mobilized diplomats and state-controlled media like the global RT network to press its case. The goal isn’t necessarily to win support, but to keep unaligned countries on the sidelines. While some countries, most notably China, have taken Russia’s side, others, like India, have avoided antagonizing Russia so as not to lose Russian military or energy contracts.

Many others have done so simply because they know and care little about Ukraine. Russia’s line to them is that it is fighting to prevent the United States from creating a unipolar world that would swallow their country, with no one to support their interests. The strategy evoked memories of the assistance the Soviet Union gave to Vietnam, Angola and other postcolonial independence movements.

The United States has mounted its own diplomatic efforts to gain more support from countries like India and South Africa. And Ukraine recently posted a video on Twitter recently in which the commander of Ukrainian armed forces thanks 37 countries that, according to the tweet, have shown “assistance and unwavering support in these hard times.” The list is not entirely fair — some Asian countries missing from the list have provided nonlethal assistance — but it is still noteworthy that there were no entries from Africa or South America.

As the war rages on, attention in the United States and elsewhere is bound to flag, and questions about the impact of the war on energy and food prices worldwide are bound to intensify. A speech by Mr. Biden on Tuesday on the need to support Ukraine was lost in the brouhaha over the leak of a Supreme Court draft ruling. And the $33 billion he is seeking in military assistance and other aid for Ukraine is certain to meet resistance, especially since there is no idea when or how the war might end.

Dwindling Western commitment is part of Mr. Putin’s calculus. Though he seems to have misjudged the West’s fury and response to his invasion, his 22 years of increasingly autocratic rule have taught him that passions invariably wane and high costs erode commitment.

As a former K.G.B. agent, Mr. Putin sees the world as a battleground of conspiratorial maneuvers. In his speeches, the color revolutions in Ukraine and other former Soviet republics and the Arab Spring and other global upheavals are machinations to bolster American domination. As an heir to the Soviet worldview, he believes more than many Western leaders do in the importance of information warfare, both to give his regime a veneer of legitimacy and to challenge liberal democracy. On this battlefield, lies are ammunition in Mr. Putin’s long and increasingly personal struggle to stay in power.

As the war enters a new phase, as the images and horrors become familiar and the costs rise, it will become ever more difficult for the Biden administration and for Mr. Zelensky to sustain their early lead in the information war. That makes it all the more imperative for the West to press the message that this is not a war Ukraine chose and that the cost of allowing Mr. Putin to have his way in Ukraine would be far higher than the sacrifices required to block him.

#### Russian disinformation locks in polarization throughout NATO

Conor Cunningham 20, Conor Cunningham is an International Policy Institute Cybersecurity Fellow at the University of Washington whose research focused on Russian Cyber Operations, November 2020, "A Russian Federation Information Warfare Primer," The Henry M Jackson School of International Studies at the University of Washington, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/ //AShah

The War on Liberal Democracy and Western Dominance

Amid new and continuing global issues and conflicts, Russia wants to remain at the forefront of the creation and implementation of possible solutions. The Kremlin believes the U.S. and its allies are continuously working to isolate Russia and undermine Russian interests. These sentiments are perfectly stated in the National Security Strategy of the Russian Federation:

“The strengthening of Russia is taking place against a backdrop of new threats to national security that are of a multifarious and interconnected nature. The Russian Federation’s implementation of an independent foreign and domestic policy is giving rise to opposition from the U.S. and its allies, who are seeking to retain their dominance in world affairs. The policy of containing Russia that they are implementing envisions the exertion of political, economic, military, and informational pressure on it.[21]“

Russia’s policy not only communicates a responsibility to protect its citizens and Russian culture, but also to combat the U.S.-led unipolar system and persuade others to do the same.

In practice, Russia uses this strategy to justify its operations abroad. As an opponent of the U.S.-centric order, Russia paints itself as a sort of hero for those who are frustrated with the U.S.-led unipolar system. The U.S. Senate 2018 report on Russia’s actions outlines the real objectives and asymmetric cyber tactics of Putin’s regime. It argues that the regime’s overarching goal is the protection of its own power and stability through the expansion of Russian hegemony in various sectors.

Analysis of known Russian information operations in Western democracies illuminates three key overarching objectives: to discredit trusted democratic institutions, to divide the Western coalition, and to undermine the supranational organizations that uphold and promote these democratic values.[22] Following a short stint with democracy in the 1990’s that coincided with national embarrassment, soaring levels of poverty, widespread corruption, war, and instability; Putin has rebuilt the country without a vision of democracy. Modern Russia provides a model for an alternative form of governance, one that is focused on information sovereignty, and promotes traditionalism, nationalism, and authoritarianism. Western ideals and democratic values naturally run contrary to Putin’s own more autocratic vision. The current international order, upheld by the U.S. and its allies, is critical of modern Russia and united, hinders Putin’s ability to implement his agenda at home and abroad.[23] For this reason, the current international order is a constant hindrance and security threat to Putin’s form of government. In addition, Russia’s history of invasion from Western Europe motivates its distrust of the west and of NATO’s effect on global politics.[24]

In most Western democracies, racism and fears about immigration create fertile ground for manipulation. These fears have been targeted by Russian information campaigns to sway the outcome of elections.[25] European democracies and the U.S. face all forms of information warfare and free and fair elections are consistently targeted. Russia hopes to radicalize the populace in these countries, creating not only instability and polarization, but also weak governments. Large supranational blocks such as the EU can have a drastic impact on Russia’s economy by implementing sanctions and forming a collective front against potential military action. For this reason, a large part of Russia’s overarching international policy is focused on disrupting the unity between Western democracies.[26]

#### European polarization cements populism---it’s robustly correlated

Victor Ginsburgh 21, Victor Ginsburgh has a PHD in economics from the Free University of Brussels. He has been an Economics professor at Université Libre de Bruxelles since 1975, Sergio Perelman obtained his first degree in Economics at the University of Buenos Aires and a PhD. in Economics at the University of Liège, Belgium, where he is Professor of Economics since 1991, Pierre Pestieau is a Belgian economist. He received his B.A and M.A degrees in economics from the University of Louvain and then his PhD from Yale University, August 2021, "Populism and Social Polarization in European Democracies," CESifo Economic Studies, https://academic.oup.com/cesifo/article/67/4/371/6346855?login=true //AShah

Our aim was to explain populist attitudes (that may eventually lead to populist votes) by a number of factors, the most important being the degree of social polarization, which measures the extent of social divides that plague our societies. Polarization is significantly positively correlated with all four populist attitudes, particularly when immigration inflows are treated as an endogenous variable and the model is estimated using IV-2SLS. To the best of our knowledge, this is the first attempt to correlate populism using such indicators of polarization that reflect the socioeconomic divides better than standard measures of inequality or poverty.

To compute our measure of social polarization, in each country we fractionalize population into three groups, low, middle and high income. The distances between the income groups are the ratios of people experiencing either difficulties ‘to make ends meet,’ or ‘material deprivation’.

We show that social polarization varies dramatically across European regions. The highest scores are found in Southern and Eastern countries and the lowest scores in Northern countries, but at the same time, some convergence is observed. Our estimations confirm, in most cases, a positive and statistically significant relation between social polarization and populist attitudes.

Furthermore, our results confirm the effect of immigration inflows on populist attitudes. The only exception, unexpectedly, is the effect of immigration on anti-immigration values. We find however a positive and statistically significant relation when testing our model for the younger European age-cohorts.

Summing up, social polarization appears as a key determinant of populist attitudes among Europeans, but there is also an anti-immigration effect. These results may appear to contradict the view that economic factors only account for a limited portion in individuals’ populist attitudes and votes (Margalit 2019).22 We think that this is not the case in our study. Social polarization must not be considered as an economic variable per se, but also as a measure of potential tensions and conflicts within the society. As such, it drives populist attitudes and values like distrust of institutions, distrust of others, anti-immigration, and authoritarianism.

#### EU populism spills over globally

David Cadier 19, researcher in EU foreign policy at CERI-Sciences Po, Associate at LSE IDEAS (London School of Economics) and a Future World Fellow at the Centre for the Governance of Change (IE University), January 2019, "How Populism Spills Over Into Foreign Policy," Carnegie Europe, https://carnegieeurope.eu/strategiceurope/78102 //AShah

Even more than mainstream parties, populist leaders in office seem to regard foreign policy as the continuation of domestic politics by other means. Because they consider themselves as the only true representatives of the people, populist actors discard any political opposition as necessarily illegitimate, with repercussions on foreign policy.

Taking the opposite course of their predecessors seems, for instance, a key reference point in setting the coordinates of their foreign policy. This is perhaps best exemplified by Donald Trump’s apparent obsession with unbundling Barack Obama’s diplomatic initiatives.

This also means that under populist leadership domestic political infightings are more likely to take precedence over diplomatic considerations. Warsaw not only stood out as the only EU member state to oppose the reelection of former Polish prime minister Donald Tusk at the helm of the European Council; its foreign minister actually denounced the election as being rigged.

Rather than competing with a political opposition, populist leaders claim to fight enemies operating from the shadows, both at home and abroad. This is in part because being elected to office and becoming, themselves, the country’s governing elite risks undermining their core antiestablishment message.

To elude this contradiction, populists in power often castigate members of the old elite as being still active behind the scenes. This allegation can then be invoked to purge the civil service, as happened with the Ministry of culture of Croatia. And this has also led populist leaders to indulge in conspiracy theories, even from top policymaking positions. In the summer of 2017, former Polish defense minister Antoni Macierewicz depicted the protests against his government’s reform of the justice system as the manifestation of a hybrid war being waged against Poland.

Overall, to refer back to Matteo Salvini’s expression, populists in office have not brought about thus far a “revolution” in their country’s foreign policy. Hungary has not put into question its NATO membership. Italy has not vetoed the renewal of EU sanctions against Russia. And Poland seems to have reverted to the kind of America First policy it had followed when George W. Bush was in the White House.

But populists do not seem to bring much distinctive common sense to the table either. Contrary to sensationalist claims, they do not necessarily adopt devil-may-care attitudes in international affairs. Yet their diplomacy is often crippled by the collateral damage of their radical approach to domestic politics. And this is likely to have both direct and indirect implications for EU external action.

First, it might affect the substance of EU foreign policy. The EU has largely based its foreign policy on the promotion of norms and standards of democratic governance, particularly in its neighborhood. The fact that some member states, such as Hungary and Poland, put these norms and standards into question domestically risks weakening the EU’s legitimacy in exporting them.

More concretely, the instrumentalization of migration issues in populist parties’ domestic political strategies has impacted the common EU asylum and migration policy—or rather a lack of one. Several member states have conveniently hidden behind the uncompromising posture of Viktor Orbán. The growing number of EU capitals announcing that they will not ratify the UN Global Compact on migration is the latest example of this ripple effect.

Second, it is likely to affect the process of EU foreign policy. By overprioritizing domestic politics and showing a proclivity for “undiplomatic” diplomacy, as well as conspiracy theories, governing populist parties risk complicating even further consensus-seeking and compromise-building. On these depends EU member states’ ability to act collectively. And this risk will be even more acute if mainstream parties seek to co-opt the ideas and emulate the rhetoric of populist actors for electoral gains—as they did in the realm of migration policies.

In short, the implications of the rise of populism for Europe’s foreign policy should neither be exaggerated nor ignored. They are already salient in some member states and might be reinforced by the results of the European Parliament elections.

#### Populism’s an independent existential risk and magnifies all others

Andrew Leigh 21, Australian member of Parliament, former professor of economics at the Australian National University, 2021, What's the Worst That Could Happen?: Existential Risk and Extreme Politics, unpaginated ebook version

How likely is it that humanity could end? Experts working on catastrophic risk have estimated the chances of disaster for a wide range of the hazards that our species faces. Adding up the threats, philosopher Toby Ord estimates the odds that humanity could become extinct over the next century at one in six, with an out-of-control superintelligence, bioterrorism, and totalitarianism among the largest risks. He argues that most of the risks have arisen because technology has advanced more rapidly than safeguards to keep it in check. To encapsulate the situation facing humanity, Ord titled his book The Precipice.

A one in six chance of going the way of dodos and dinosaurs effectively means we are playing a game of Russian roulette with humanity’s future. Six chambers. One bullet. Even the most foolhardy soldier usually finds an excuse not to play Russian roulette. And that’s when just their own life is at stake. In considering extinction risk, we’re contemplating not one fatality but the death of billions or possibly trillions of people—not to mention countless animals.

It can seem impossible to imagine our species becoming extinct due to a catastrophe such as nuclear war, asteroids, or a pandemic. But in reality, the danger surpasses plenty of perils we already worry about. One way to put catastrophic risk into perspective is to compare it with more familiar risks. If extinction risk poses a one in six risk to our species over the next century, then it means that it is far more hazardous than many everyday risks. Specifically, it suggests that the typical US resident is fifteen times more likely to die from a catastrophic risk—such as nuclear war or bioterrorism—than in car crash.2

Extinction risk outstrips other dangers too. Ask people about their greatest fears, and you’ll get answers like “street violence,” “snakes,” “heights,” and “terrorism."4 But in reality, these are much less hazardous than catastrophic risks. People in the United States are 31 times more likely to die from a catastrophic risk than from homicide. Catastrophic risk is 3,519 times likelier to kill than falls from a height, and 6,194 times more likely to kill than venomous plants and animals. If you have ever worried about any of these threats, you should be more fearful about cata- strophic risk. Extinction risks aren’t just more dangerous than any of them; they are more hazardous than all of them put together. Catastrophic risk poses a greater danger to the life of the typical US resident than car accidents, murder, drowning, high falls, electrocution, and rattlesnakes put together.

A one in six risk is just the danger in a single century. Suppose that the risk of extinction remains at one in six for each century. That means there’s a five in six chance humanity makes it to the end of the twenty-first century, but less than an even chance we survive to the end of the twenty-fourth century. The odds that we survive all the way to the year 3000 are just one in six. In other words, if we continue playing Russian roulette once a century, it’s probable that we blow our brains out before the millennium is halfway through, and there’s only a small chance that we make it to the end of the millennium.

Part of the reason humans undervalue the future is that it’s hard to get our heads around the idea that our genetic code could live on for millions of years. At present, the best estimates are that our species, Homo sapiens, evolved around three hundred thousand years ago.1 That means we have existed for about ten thousand generations. But we have another one billion years before the increasing heat of our sun brings most plant life to an end.1 That’s plenty of time to figure out how to become an interstellar species and move to a more suitable solar system. Humans could live to enjoy another thirty million generations on earth.

Thinking about the mind-boggling scale of these numbers, I’m reminded of the Total Perspective Vortex machine, created by Douglas Adams in The Restaurant at the End of the Universe. Anyone brave enough to enter sees a scale model of the entire universe, with an arrow indicating their current position. As a result, their brain explodes. As Adams reflects, the machine proves that “if life is going to exist in a universe of this size, then the one thing it cannot afford to have is a sense of proportion.”

Still, let’s try. Imagine your ancestors a hundred generations ago. They are your great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-great-great-great-great-great-great-great-great- great-great-great-grandparents. These people lived around 1000 BCE, at the start of the Iron Age. They might have been part of Homeric Greece, ancient Egypt, Vedic age India, the preclassic Maya, or Zhou Dynasty China.

Contemplate for a moment about what the hundred genera- tions between our Iron Age ancestors and today have achieved. They built the Taj Mahal and Sistine Chapel, the Angkor Wat and Empire State Building. Thanks to them, we can relish the poetry of Maya Angelou, novels of Leo Tolstoy, and music of Ludwig van Beethoven. An abundance of inventions has delivered us deli- cious food, homes that are comfortable year-round, and technol- ogy that provides online access to a bottomless well of entertain- ment. If time machines existed, we might pop in to visit our great100 grandparents, but few would volunteer to stay in the Iron Age.

Yet humanity is really just getting started. If things go well, it’s ten thousand generations down, thirty million to go. Imagine what those future generations could do, and how much time they have to enjoy. Here’s one way to think about what it means to have thirty million generations ahead. Suppose humanity’s potential time on the planet was shrunk down to a single eighty- year life span. In that event, we would now be a newborn baby— just nine days old. Homo sapiens is a mere 0.03 percent through all we could experience on earth.

We won’t meet most of those who follow us on the planet, but we should cherish future generations all the same. If you value humanity’s past achievements—the Aztec and Roman civiliza- tions, art of the Renaissance, and breakthroughs of the Industrial Revolution—then the generations to come are just as worthy. This is what political philosopher Edmund Burke meant when he described society as “a partnership not only between those who are living, but between those who are living, those who are dead, and those who are to be born.’- To appreciate the past is akin to admiring the achievements of distant places. Like geography, his- tory helps us better understand the way of the world.

Politicians like me like to speak fondly about looking after "our children and our grandchildren.” But it usually stops after a generation or two. Policy pays little heed to the many generations that will follow. For my own part, it took a coronavirus-induced shutdown to have the time to spend reflecting deeply about the long term. This book had been rattling around in my head for years, but it was only when all my meetings, events, and travel were canceled that I had the time to write it. Pandemics are one of the threats to humanity that I’ll discuss in this book, but in this instance, it provided a chance to reflect on the long term. It’s tempting to ignore the distant future. It’s easier to love the grandchildren whom we hug than the great-great-great-grand- children whom we’ll never get to smile on. But that doesn’t make those far-flung generations any less important. Via my wife, our children can trace their lineage to Benjamin Franklin, but I’m more excited about the potential achievements of the generations yet to be born.

For companies and governments, a major impediment to long- term thinking is the idea of discounting the future. When investing money, this is a reasonable approach. A dollar in a decade’s time is less valuable than a dollar today for the simple reason that a dollar today could be invested and earn a real return. Share markets have good and bad years, but based on returns from the past 120 years, someone who put $1,000 into the US stock market for an average year could expect it to be worth $1,065 after twelve months (accounting for dividends and inflation).2 Approximating these returns, when governments contemplate making investments, they often apply a discount rate of around 5 percent, while companies use rates that are higher still.2

When it comes to growing your greenbacks, this makes perfect sense. If Kanesha offered you $ 1,000 today, and Jane offered you $ 1,000 in a year’s time, most of us would think that Kanesha was making the more generous offer. Kanesha’s cash can be put to productive use and would be worth more than Jane’s when the year is out.

But what if we’re talking about Kanesha and Jane themselves? Suppose Kanesha is alive today, and Jane is yet to be born. When discounting is applied to lives, it suggests that Kanesha’s life to- day is worth twice as much as Jane’s life in fifteen years’ time. It implies that Kanesha today is worth 132 times as much as Jane in a century’s time. So if we’re spending money to keep them safe, a 5 percent discount rate indicates that we should spend more than a hundred times as much to protect Kanesha today than to pro- tect Jane in a century’s time.

The further we stretch the time period, the more ridiculous the results become. Discounting at a rate of 5 percent implies that Christopher Columbus is worth more than all eight billion people on the planet today.— Naturally, it also implies that your life is worth more than eight billion lives in five hundred years’ time. Even if you value the hug of a loved one over the unseen successes of next century’s generations, is it fair to ruthlessly dis- miss the distant future? Discounting is the enemy of the long term.

As philosopher Will MacAskill points out, there is something morally repugnant about concluding that the happiness of those who will be alive in the 2100s is inconsequential simply because they live in the future. MacAskill coined the term “presentism” to refer to prejudice against people who are yet unborn.” Just like racism, sexism, or other forms of bigotry, he argues that mis- treating those who live a long way in the future is unfair. To dis- criminate in favor of Kanesha against unborn Jane is a form of presentism. If you traveled back in time to the 1500s and met someone who claimed that they were worth more than everyone alive in the 2000s, you’d rightly regard them as an egomaniac. Isn’t it equally narcissistic to ignore the happiness of people in the 2500s?

Some have contended that we should favor the living over the unborn for the same reason that philanthropy favors the down- trodden over the wealthy. If incomes rise over time, the argument goes, then asking today’s citizens to help those in the future is like taking from the poor to give to the rich.— But this reasoning ignores the fact that we are talking about the survival of future generations. Theoretical riches won’t do them any good if they are practically dead—or if planetary apocalypse snuffs out their chance to be born. Similarly, it misses the possibility that future pandemics, wars, or climate disasters could make coming genera- tions significantly poorer.—

Insights from behavioral science help explain why humans aren’t good at understanding extinction risk.— Our thinking about dangers is skewed by an “availability bias”: a tendency to focus on familiar risks. Like the traders who failed to forecast the collapse of the securitized housing debt market, we are lousy at judging the probability of rare but catastrophic events. Most important, our instincts fail us as the magnitudes grow larger. In research titled "The More Who Die, the Less We Care,” psychologists Paul Slovic and Daniel Vastfjall argue that we become numb to suffering as the body count grows.— Humans’ compassionate instincts are aroused by stories, not statistics. Indeed, one study found that people were more likely to donate to help a single victim than they were to assist eight victims. This may help explain why the international community has been so slow to respond to genocide, including recent incidents in Rwanda, Darfur, and Myanmar. As artificial intelligence researcher Eliezer Yudkowsky notes, human neurotransmitters are unable to feel sorrow that is thousands of times stronger than a single funeral.— The problem is starker still when it comes to extinction risk. Our emotional brains cannot multiply by billions.

Add to this a media cycle that has become a media cyclone, in which stories explode in a matter of minutes, and “outrage porn” seems to drive the news choices of many outlets. In the 2016 US election, researchers found that for every piece of professional news shared on Twitter, there was one piece of “junk news.’’— Conflict fueled by social media keeps us in a primal state of rage and retaliation. And this isn’t the only force that makes politics myopic. Campaign contributions tend to come from donors who have an immediate interest in a “today” issue rather than from people aiming to solve long-term problems. This kind of “instant noodle” politics prioritizes quick results and sidelines fundamental challenges.

In this environment, a special style of politics has thrived: populism. The term “populist" gets thrown around a lot—typically as an insult—so it’s worth taking a moment to define it precisely.— Populists see politics as a conflict between crooked elites and the pure mass of people. Many candidates trying to defeat an incumbent will criticize “insiders,” but populists make a stronger attack on elites, claiming that they are dishonest or corrupt. Populists then claim that they—and only they—represent the “real people.” Populists combine a fierce critique of elites and personal appeal to the “silent majority.”

The political strategy of populists involves critiquing intellectuals, institutions, and internationalism. The political style of populists tends to be fierce. They do not strive for unity and calm consensus. Populists share with revolutionaries a desire for sudden and dramatic change. They have little respect for experts and the systems of government. Populists’ priorities tend to be immediate issues such as crime, migration, jobs, and taxes. Consequently, the electoral success of populists has served to sideline work on long-term dangers such as climate change and nuclear war.

Donald Trump may have lost his presidential reelection bid, but he has transformed the Republican Party, which has jettisoned its longstanding commitment to free trade, immigration, and global alliances. Many moderate Republicans, who might have served comfortably under Ronald Reagan or George H. W. Bush, have quit the party or been defeated by Trump-supporting populists. The Republican Party, which holds nearly half the seats in Congress and controls a majority of state legislatures, has embraced populism to a degree that was unimaginable when it was led by George W. Bush, John McCain, or Mitt Romney. After four years under President Trump, the Republican Party is now more cynical and isolationist, focused on immediate grievances rather than long-term challenges.

Yet while the strength of populism threatened to sideline issues of catastrophic risk, coronavirus did the opposite. The worst pandemic in a century led to the most severe economic crisis since the Great Depression. Churches and concert halls fell silent. International travel collapsed. The Summer Olympics were postponed. Stocks plunged, and for a brief moment, the price of a barrel of oil went negative. Globally, millions lost their jobs, and millions more faced famine.

COVID-19 never threatened to extinguish humanity, but it highlighted our vulnerability to infectious diseases. More than at any time in living memory, people focused on the dangers of pandemics. The popularity of Geraldine Brooks’s Year of Wonders, Stephen King’s The Stand, Emily St. John Mandel’s Station Eleven, and Albert Camus’s The Plague vividly illustrates the way in which fear of pandemics has become more acute.

We know that disasters can remake society. The black death helped usher in the Renaissance.— The Great Depression made a generation of investors more risk averse.— World War II spawned the United Nations and formed the modern welfare state. In autocracies, droughts and floods can topple dictators.—

Coronavirus is reshaping the world in numerous ways.— Handwashing is in. Cheek kissing is out. The rise of big cities is slowing as people consider the downsides of density. Firms that automated their production systems to deal with physical dis- tancing requirements and stay-at-home orders are discovering that they can get by permanently with fewer staff. More tele- working and less business travel is leading to a drop in demand for receptionists, bus drivers, office cleaners, and security guards. When it comes to our use of technology, coronavirus suddenly accelerated the world to 2030. When it comes to globalization, the pandemic took us back to 2010.

But it’s still an open question as to how COVID-19 will affect humanity’s ability to think about the long term. Most of the examples I’ve listed are instances in which crises affected societies organically: the shock came, and it changed our behavior. But accentuating the long term requires taking risk more seriously and placing greater emphasis on saving our species. Linebackers are swift to respond when an offensive player suddenly takes a step to the right. But it takes longer to recognize that a team’s offensive plays are skewed to the right and modify the defensive formation accordingly.

Like a football team that adapts its tactics, this book argues that we should lengthen our thinking. At minimal cost, society can massively reduce the odds of catastrophe. By ensuring that the big threats get the attention and resources they need, we can safeguard the future of our species. As insurance policies go, this one is a bargain.

In the chapters that follow, I’ll outline the biggest risks facing humanity. I’ll begin in chapter 2 with pandemics, such as the possibility that the next virus might combine the infectiousness of COVID-19 with the deadliness of Ebola. What can we do to shut down exotic animal markets, speed up vaccine develop- ment, and create surge capacity in hospitals? I’ll then delve into bioterrorism, and the danger of extremists developing their own versions of smallpox or the bubonic plague. How difficult is it for them to create these devilish diseases, and what can we do to prevent it?

In chapter 3, I’ll then explore climate change—perhaps the in- tergenerational issue that has received the most public attention in recent years. While much of the modeling looks at how global warming could be bad, my focus is on the chances that it’s catastrophic. This isn’t about climate change shortening the ski season; it’s about the possibility of temperatures rising by 18°F (10°C), rendering large sections of the planet uninhabitable. What does the risk of cataclysmic climate change mean for energy policy?

Next, I’ll turn to nukes. As a child in the 1980s, I vividly re- member watching The Day After. My classmates and I agreed that a nuclear war was inevitable. When the Cold War ended, the world seemed safer, but in the three decades since, the threat from new nuclear powers has made the problem less predictable. As I discuss in chapter 4, what we used to call an arms race now looks more like a bar fight, with hazards coming from unexpected directions, including terrorist groups. Yet just as there are practical ways to avoid pub brawls (don’t drink past midnight, avoid the stairs, look out for the glass), so too are there sensible strategies that can reduce the odds of nuclear catastrophe (adopt a “no first use" policy, reduce the stockpiles, control loose nukes).

A superintelligence has been dubbed the “last invention” we’ll ever make. An artificial intelligence machine whose abilities exceed our own could turbocharge productivity and living stan- dards. But it could also spell disaster. If we program our artificial intelligence to maximize human happiness, it could fulfill our wishes literally by immobilizing everyone and attaching electrodes to the pleasure centers of our brains. As chapter 5 notes, what makes artificial intelligence different from every other risky technology is its runaway potential. Once a superintelligence can improve itself, it is unstoppable. So we need to build the guardrails before the highway.

What are the odds? In chapter 6,1 complete the discussion of catastrophic danger by examining less risky risks, including asteroids and supervolcanoes. I also consider the prospect of “unknown unknowns.” For example, prior to the first atomic bomb test, some scientists thought there was a chance it could set the atmosphere on fire, destroying the planet. When the Large Hadron Collider was being built, critics warned that the particle collisions inside it could create micro black holes. Although neither situation eventuated, they raise the question of what other doomsday scenarios could be lurking around the corner. How should the prospect of these unexpected risks change our approach to cutting-edge science? Drawing together these dangers with the major hazards, I report the likely probability of each, benchmarking existential risks such as nuclear war and pandemics against individual risks such as being struck by lightning or dying on the battlefield.

Ultimately, tackling existential risks is a political problem. Private citizens can achieve many things, but preventing nuclear war, averting bioterrorism, and curbing greenhouse emissions are fundamentally problems of government. Governments control the military, levy taxes, and provide public goods. So the values of those who run the country will determine how much of a priority the nation places on averting catastrophe.

That’s why the rise of populists is crucial to humanity’s long- term survival. In chapter 7,1 discuss the factors that have led to the electoral success of populists during recent decades, and why populists tend to be uninterested in dealing with long-term threats. Populists’ focus on the short term means that—like a driver distracted by a back seat squabble—we’re in danger of missing the threats that could kill us. I’ll explore why populists around the world struggled to respond to COVID-19, and what this says about the dangers that populism poses to our species. Most critics of populism have concentrated on the present day. They’re missing the bigger picture. Populists are primarily endangering the unborn.

Bad politics doesn’t just exacerbate other dangers; it represents a risk factor in itself through the possibility of a totalitarian turn —in which democracy is replaced by an enduring autocracy. The road to democracy is not a one-way street. Over the centuries, dozens of countries have backslid from democracy into autocracy —abandoning the institutions of fair elections, protection for minorities, and free expression. Such an outcome could be deadly for dissenters and miserable for the multitudes. Chapter 8 explores why democracy dies and identifies the signs that institutions are being undermined. Chapter 9 suggests how we might strengthen democracies to allow citizens to have a greater say, and lower the chances of the few taking over from the many. Chapter 10 concludes the book.

When COVID-19 hit, many rushed out to buy life insurance.— In our personal lives, we know that spending a small amount on insurance can guard against financial ruin. Societies can take a similar approach: implementing modest measures today to safe- guard the immense future of our species. For each of the existential risks we face, there are sensible approaches that could curtail the dangers. For all the risks we face, a better politics will lead to a safer world.

Because of its focus on the urgent over the important, populist politics should perhaps bear the label, “Warning: populism can harm your children." But what is the alternative? In the conclusion, I argue that the answer lies in the ancient philosophy of stoicism. A stoic approach to politics isn’t about favoring one side of the ideological fence over another. Instead, it’s about the temperament of good political leadership. Stoicism emphasizes that character matters and holds that virtue is the only good. Decisions are based on empirical evidence, not emotion. Anger has no place in effective leadership. Strength comes from civility, courage, and endurance. Stoics make a sharp distinction between the things they can change and those they cannot.

#### Info warfare is the linchpin of Russia’s hybrid proxy conflict strategy---the Donbas model will be replicated

Tomáš Čižik 17, is a director of Centre for European and North Atlantic Affairs (CENAA), a Bratislava based international relations and security policy think-tank. Tomáš holds a PhD in Theory of Politics from Faculty of Political Science and International Relations at the Matej Bel University, May 2017, " Information Warfare - New Security Challenge for Europe.," Center for European and North Atlantic Affairs, [Information\_Warfare\_\_\_cover.pdf](https://d1wqtxts1xzle7.cloudfront.net/52519399/Information_Warfare___cover-libre.pdf?1491519289=&response-content-disposition=attachment%3B+filename%3DInformation_Warfare_New_Security_Challen.pdf&Expires=1655931419&Signature=CmnXGlGzeqNCIa91gHXR2orhJSSEDL9k8iz2cLfyuLuYSP~MSTQnrhSiDz7VgxvDQH5OzOhCxEBtPquzQtgCiG9y2diGeaSli4R~aychG79OZeT5YSKEOVUGKU-dyz7PY2F8CRH9YO7y5nW7ssQqCRbzebxVk5pI8axY7Xtbz60qKa3FTHg2weOa2QVGaMpr-EJuaIPD8Lt6u4IoNTj4S5Wiq16QgdjSqm462aZtAuIN7wJJMgBij4JOInuZNr2rbe-IhCPc4isDJszbmZfFI30tTLTfMFcHi1KGH-SkLB0qLomxi8EABElAvr4OYlQVTfh~iqXhDQ1uPg5BfiX3jA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA) //AShah

Armed insurgency, Russia's main kinetic HW tool against Ukraine, was instigated and backed by massive information warfare since it's inception. The rebels, who are mostly mobilized, trained, and armed by the Russian special services, and further supported by the Russian armed forces, have been destabilizing Donetsk and Luhansk regions since February 2014. The crisis started to unfold after the pro-Russian former president Yanukovich was forced to flee to Russia as a result of the revolutionary rally in Kiev over his decision to hinder Ukraine's association with the EU. The mass protests in Kiev's Maidan Square, which brought the new pro-European government to power, demonstrated the unequivocal support of the vast majority - 90% according to some polls - of the Western Ukrainians for European integration (IRI, 2014). In response to the undesired change of the government in Ukraine (GoU), Russia launched an aggressive information campaign blaming the government for alleged violations of the rights of the Russian speaking minorities in the country. Using this narrative, predominantly Russian-speaking Crimea was officially annexed by Russia, and Russian special services started to organize separatist outbreaks in Donbas. For these purposes, Russia used the dissatisfaction of the Russian speaking Ukrainians with the new government's attempt to drop the law making Russian the official second language of Ukraine.

Notably, the linguistic divide between the population of the western and eastern regions of Ukraine is reflected in political preferences on the part of the population. According to the opinion polls conducted by the Kiev's International Institute of Sociology, 72.5% of the population of Donetsk region are in favor of integration of Ukraine into the Russian-led Customs Union as opposed to the 9.4% supporting EU integration (Zn. ua, 2014). The regional differences with regard to foreign policy orientation, also stimulated and well exploited by Russian propaganda, can be seen as the main source of the political disagreement between eastern and western Ukraine. As a result of effective information warfare conducted by Russia and the pro-Russian separatists on the ground, they were able to manipulate with the divides among the population against Ukraine's integration into the European and Euro-Atlantic structures by provoking violent conflict in Donbas without even having mass support.

Remarkably, unlike Ukraine, there has never been a significant Russian native speaking or ethnic minority in Georgia. According to the 2002 census published by the European Center for Minority Issues, there is a total of 1.5% Russians living on the territory of Georgia (EUMM, 2014). Therefore, to rationalize the narrative of protecting Russians abroad,' Moscow has since 2002 mass distributed Russian passports in both occupied regions of Georgia. According to various media sources, accepting Russian citizenship was mandatory for permanent residents in the occupied territories and was forcefully executed by local police units. In other words, as opposed to Ukrainian case, where Russia used existing linguistic divides to instigate separatism, in Georgia it created artificial citizens through an illegal “passportization' process in order to justify the 2008 invasion of Georgia. The narrative that was used by Kremlin to justify the aggression after the 5 days war was blaming Georgia for initiating the conflict by using force against Russian citizens in Tskhinvaly region, thus compelling Russia to respond with the “peace enforcement" operation. This analysis is very important to once again underscore that smaller and weaker states failed to deter realization of obvious patterns of Kremlin's HW and counter its strategic narratives, such as the right to protect interests of Russians abroad. As evidenced in both Ukraine and Georgia, Russia is using a new type of Hybrid Warfare to achieve its goals through controlling proxies on the ground supported by the massive information warfare. In both cases Russia, without having solid grounds, succeeded to materialize aggression through engineering new realities, which constitute dangerous precedents that can be repeatedly used against Georgia and other vulnerable countries in future.

#### Specifically, it’ll trigger invasion of the Baltics---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?

#### 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.

### 1AC---Information Ecosystem Advantage

#### Advantage Two is the Information Ecosystem

#### Accelerating info operations from authoritarian powers are corrupting institutions worldwide---but the plan solves

Andrea Kendall-Taylor 20, senior fellow and director of the Transatlantic Security Program at the Center for a New American Security; and David Shullman, the senior advisor at the International Republican Institute and an adjunct senior fellow at the Center for a New American Security, 5/26/2020, "Converging Chinese and Russian Disinformation Compounds Threat to Democracy," Power 3.0: Understanding Modern Authoritarian Influence, <https://www.power3point0.org/2020/05/26/converging-chinese-and-russian-disinformation-compounds-threat-to-democracy/>, RMax

In recent weeks the Chinese Communist Party’s (CCP) propaganda and disinformation blitz around COVID-19 has drawn increasing attention, and with good reason. In addition to promoting a narrative about Beijing’s global leadership around the pandemic, the Chinese government has adopted Russian disinformation tactics in promoting conspiracy theories purporting that COVID-19 originated in Europe, the United States, and beyond to distract from its failed initial response to contain the outbreak from spreading beyond Wuhan.

Several accounts of China’s information operations have noted the incorporation of Russian disinformation tactics. Yet the full significance of this development cannot be understood without appreciating the broader alignment between Russia and China. In other words, China’s adoption of Russian information operation techniques is about more than “authoritarian learning,” or the passive diffusion of such practices from one authoritarian regime to the next. Instead, Russia and China are deepening ties and increasing coordination on a range of economic, defense, technological, and political issues. These repeated interactions facilitate an intentional sharing of best practices and are building a foundation for sustained cooperation moving forward.

Relations between Russia and China developed gradually after the Cold War and accelerated dramatically in 2014 when Russia’s illegal annexation of Crimea and subsequent occupation of Ukraine shut down Russian opportunities in and cooperation with Western democracies. These events drove Russia toward China at a time when the latter was demonstrating greater foreign policy assertiveness under Xi Jinping. The CCP leadership was increasingly concerned about perceived Western efforts to foment “color revolutions” in the wake of the Arab Spring, the advent of the Umbrella Movement in Hong Kong, and Washington’s “pivot to Asia.” Since then, there has been an increasing convergence between Moscow and Beijing’s views of how the world should be ordered. The two governments are finding common cause in undermining liberal democratic norms and institutions, weakening cohesion among democratic allies and partners, and reducing U.S. global influence.

Historically, Beijing and Moscow have taken different approaches to advancing these shared foreign policy objectives. The Kremlin has sought to sow confusion and exploit divisions to polarize public debates, whereas China has used subtler tactics conducive to building economic ties and influence while shaping positive perceptions of China. China’s disinformation during the pandemic, however, has evinced a newfound willingness to deploy the Kremlin’s techniques. Beijing has promoted elaborate conspiracy theories about the pandemic’s origins to inject confusion into global narratives, including one particularly sophisticated scheme by the Chinese Foreign Ministry’s Information Department to pin blame on the U.S.

China’s efforts to burnish its standing as a net provider of public goods during the pandemic have also benefited from Russia’s example. During a two-week period in March 2020, for example, nearly 50,000 tweets flooded the Twittersphere with pro-China hashtags. Notably, nearly half of Tweets featuring the hashtag “forzaCinaeItalia” (Go China, Go Italy) and more than a third of Tweets featuring the hashtag “grazieCina” (thank you China) stemmed from bots—a quintessentially Russian tool that Chinese operations have increasingly leveraged—that averaged more than 50 tweets per day.

As Russia-China relations continue to deepen, the exchange of best practices and cross-border learning of disinformation tactics will become increasingly hardwired into the interactions between them. The two countries’ state media organizations are increasingly collaborating with an eye toward formulating common messaging to counter “Western influence” and promote positive stories about Russian and Chinese leadership in the world. There is a particular focus on digital media platforms, where the two countries have pledged cooperation to combat “illegal online content.”

As they work toward shared objectives, their efforts will produce dangerous synergies that will pose growing problems for democracies. Already, Russia and China have an implicit tactical division of labor. Russia propagates narratives designed to undermine trust in institutions, creating fertile ground for Chinese narratives about the failings of democracy and superiority of authoritarian systems to take root. Likewise, as Moscow and Beijing work toward shared objectives they will be increasingly singing from the same sheet of music, amplifying a common message about the flaws and failures of Western democracy and the need for an alternative, supposedly values-free vision for globalization and development. Russian state media have already propagated pro-Beijing views on a range of topics (and vice versa), forging a symbiotic relationship that supports the creation of an alternative information ecosystem in which truth is called into question. Moving forward, Russia and China will find other common causes where leveraging each other’s platforms and propaganda will broaden their collective reach and impact.

The once bright line between CCP and Kremlin disinformation tactics has grown fuzzy. During the pandemic, Beijing has demonstrated a willingness to use disinformation to confuse global audiences and maliciously discredit democracies to protect the CCP’s reputation and promote China as a responsible global leader by comparison. Democratic countries must prepare for a future where information operations are increasingly utilized by both China and Russia in their varied but compounding efforts to undermine liberal norms and democratic institutions, while also popularizing aspects of authoritarianism. Good governance, aggressive independent media, and deep understanding of disinformation tactics will be critical to exposing and countering Chinese and Russian efforts to distort the truth to advance their interests. Leading democracies must renew their global leadership and reinvest in their relationships around the world. When it comes to protecting the information environment, a good offense is truly the best defense.

#### Info warfare makes it impossible to effectively respond to climate change

Joseph Marks 20, Washington Post reporter, 1/24/20, “The Cybersecurity 202: Disinformation threat pushes Doomsday Clock closer to midnight,” https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/01/24/the-cybersecurity-202-disinformation-threat-pushes-doomsday-clock-closer-to-midnight/5e29d32d88e0fa6ea99d3426/

Online disinformation campaigns are not just a threat to the 2020 election. They may be a harbinger of the end of the world.

Metaphorically speaking, at least.

Concerns over "cyber-enabled information warfare" were one reason the Bulletin of Atomic Scientists pushed the Doomsday Clock up to 100 seconds to midnight, a metaphor for the global apocalypse. That’s first time the clock has passed the two-minute mark since it was first used to gauge civilization's existential threats soon after the dawn of the nuclear age in 1947.

Disinformation driven by swarms of computer bots and emerging technology such as deepfakes are sowing rancor across the world and making it far harder to deal with existential threats such as nuclear war and climate change, the Bulletin’s Science and Security Board writes.

“The international security situation is now more dangerous than it has ever been, even at the height of the Cold War,” the authors write. “... The Clock continues to tick. Immediate action is required.”

The authors, who include scientists, public policy experts and former politicians, are less concerned about specific disinformation campaigns, such as those Russia mounted to damage Hillary Clinton’s campaign in 2016 or those that U.S. intelligence and law enforcement agencies say Russia, China, Iran and others are likely to use in 2020. Rather, they fear the result of those campaigns will broadly undermine public faith in facts and expertise to the point that it’s impossible to tackle climate change and other pressing global problems.

“If these current trends continue, we’re looking at a world in which the information environment is so corrupt that rational and reality-based discourse is impossible,” Herb Lin, a member of the science and security board and a senior research scholar for cyber policy at Stanford University, told me.

The Bulletin first cited the threat of information warfare in a 2018 update when board members moved the clock to two minutes to midnight. For comparison, that's the same setting as in 1953 after the United States and Soviet Union first tested thermonuclear weapons, which are about 1,000 times as destructive as the atomic bombs the United States dropped on Japan during World War II. This year, the board moved the clock another 20 seconds closer.

Cybersecurity and information warfare experts I spoke with largely backed up the Bulletin’s assessment yesterday.

“Cyber-enabled information warfare and the consequent rise of a ‘there is no truth’ culture undercuts our societies’ ability to take … difficult, large scale and timely actions,” Chris Painter, the State Department’s former top cybersecurity diplomat who served during the Obama administration and early months of the Trump administration, told me.

Melanie Teplinsky, a former White House and National Security Agency official who’s now an adjunct professor at American University’s Washington College of Law, warned that “cyber-enabled information warfare poses an outsized threat because of its ability to undermine the reliability of the information on which we rely for rational decision-making in nearly every domain.”

#### Warming causes extinction

David Spratt 19, Research Director for Breakthrough National Centre for Climate Restoration, Ian Dunlop, member of the Club of Rome, formerly an international oil, gas and coal industry executive, chairman of the Australian Coal Association, May 2019, “Existential climate-related security risk: A scenario approach,” https://docs.wixstatic.com/ugd/148cb0\_b2c0c79dc4344b279bcf2365336ff23b.pdf

An existential risk to civilisation is one posing permanent large negative consequences to humanity which may never be undone, either annihilating intelligent life or permanently and drastically curtailing its potential.

With the commitments by nations to the 2015 Paris Agreement, the current path of warming is 3°C or more by 2100. But this figure does not include “long-term” carbon-cycle feedbacks, which are materially relevant now and in the near future due to the unprecedented rate at which human activity is perturbing the climate system. Taking these into account, the Paris path would lead to around 5°C of warming by 2100.

Scientists warn that warming of 4°C is incompatible with an organised global community, is devastating to the majority of ecosystems, and has a high probability of not being stable. The World Bank says it may be “beyond adaptation”. But an existential threat may also exist for many peoples and regions at a significantly lower level of warming. In 2017, 3°C of warming was categorised as “catastrophic” with a warning that, on a path of unchecked emissions, low-probability, high-impact warming could be catastrophic by 2050.

The Emeritus Director of the Potsdam Institute, Prof. Hans Joachim Schellnhuber, warns that “climate change is now reaching the end-game, where very soon humanity must choose between taking unprecedented action, or accepting that it has been left too late and bear the consequences.” He says that if we continue down the present path “there is a very big risk that we will just end our civilisation. The human species will survive somehow but we will destroy almost everything we have built up over the last two thousand years.”11

Unfortunately, conventional risk and probability analysis becomes useless in these circumstances because it excludes the full implications of outlier events and possibilities lurking at the fringes.12

Prudent risk-management means a tough, objective look at the real risks to which we are exposed, especially at those “fat-tail” events, which may have consequences that are damaging beyond quantification, and threaten the survival of human civilisation.

Global warming projections display a “fat-tailed” distribution with a greater likelihood of warming that is well in excess of the average amount of warming predicted by climate models, and are of a higher probability than would be expected under typical statistical assumptions. More importantly, the risk lies disproportionately in the “fat-tail” outcomes, as illustrated in Figure 1.

#### It broadly undermines scientific decisionmaking---extinction

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, //chico

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between state- ment A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empiri- cal data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information war- fare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti- Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

Adversaries foreign and domestic that make use cyber-enabled information warfare turn our internal cognitive processes and our external institutional and legal processes against us. Under the cover of “fair play” rubrics and the First Amendment, they have turned us against ourselves. Desperately needed are ways of countering the insidious tactics of cyber-enabled information warfare for ourselves.

How might we proceed? We need action to develop better ways of identifying adversary cyber-enabled infor- mation warfare campaigns in progress; good counter- measures to help human beings resist the use of cyber- enabled information warfare operations targeted against them; and good measures to degrade, disrupt, or expose the adversary’s use of cyber-enabled information warfare operations. All of this is easier said than done, however, as cyber-enabled capabilities for information warfare increase while human cognitive limitations remain the same. Our work is cut out for us. If we fail, the world is at increasing risk of large-scale and long-term societal frac- ture, the end of the Enlightenment, and the start of an informational Dark Age.

#### Disinformation causes truth decay----system wide approach by NATO is key to prevent it.

Kathleen J. McInnis 21, senior fellow with the Scowcroft Center for Strategy and Security's Transatlantic Security Initiative; Clementine G. Starling is the deputy director of Forward Defense and resident fellow of the Transatlantic Security Initiative at the Atlantic Council, “The Case for a Comprehensive Approach 2.0: How NATO Can Combat Chinese and Russian Political Warfare,” <https://www.atlanticcouncil.org/wp-content/uploads/2021/06/NATO-Comprehensive-Approach-Report-2021_final.pdf>, cy

Beyond these US, UK, and Finnish examples, comprehensive approaches to political warfare among NATO members and partners are less prominent. Perhaps in part owing to bureaucratic stovepiping and policymaking preferences, many capitals of NATO member states that are targets of these campaigns tend to view each of Moscow and Beijing’s actions discretely rather than as constituent parts of a holistic strategy. Failure to consider these activities and their implications holistically—and, therefore, failing to address their respective behaviors in a likewise holistic manner— risks the United States and its allies taking actions that achieve short-term successes at the expense of longer-term gains. Progress on areas like the EU-China Comprehensive Agreement on Investment (CAI), for example, which seeks to replace bilateral trade agreements between EU members and China with a common EU-wide investment framework, can present longer-term strategic risks to European states, including increased vulnerability to Chinese economic coercion and influence campaigns—not to mention heightened tensions in the transatlantic relationship due to increasingly divergent strategic approaches to China.47 In other words, a strategic-level approach between NATO, its member states and partners, the private sector, and like-minded multilateral organizations like the EU is needed, as is a framework to turn strategic consensus into concrete action. Fortunately, both by treaty and by recent operational practice, NATO is well positioned to serve as a bedrock for both. The Alliance can, therefore, usefully serve as a catalyst for developing a Comprehensive Approach to combat coercion and political warfare.

Article 2 and the Art of the Political: NATO’s Strategic Role in Countering Political Warfare

NATO stepping up to take on a larger role in countering political warfare has its trade-offs, and some might reasonably express concern about the knock-on effect that such an approach might have on the conduct of military affairs. Some concerns may include: first, if NATO is predominantly a military alliance, then it doesn’t have a significant role to play in countering political warfare, which is the realm of politicians, statesmen, home departments, departments of commerce, and so on. Second, to assign political warfare as a supporting task to militaries, and military institutions like NATO, would likely dilute their focus on their essential defense functions (which are hard enough to perform on the best of days). It might also lessen the pressure on NATO allies and partners to effectively share the costs of hard defense. In the minds of critics, adding political warfare to the growing list of NATO’s tasks means diminishing Alliance effectiveness.

These arguments—however well-intentioned—are unhelpfully divorced from both NATO’s history and current realities. NATO is, and always has been, a political-military alliance in large part because contemporary alliances are themselves an inherently political-military construct.48 To argue for the disaggregation of the military from the economic and political spheres is a conceit, arguably framed by present bureaucratic realities rather than institutional history. The post-World War II order, of which NATO is a part, was designed to be a proactive, forward-looking answer to the security dilemmas and distrust that had previously characterized alliance politics.49 “Despair, disorder, decay from within—these were the likely dangers, not a Soviet invasion.”50 As the USSR’s aggressive intentions became more clear, NATO itself became a solution to enabling European integration and economic revitalization rather than an end in and of itself.51

As NATO was established, reconstituting the economic and political health of its member states was seen as inextricably linked to military strength; military strength was one important pillar of a comprehensive strategy to counter Soviet influence and aggression. 52 NATO’s purpose, therefore, as established in the Washington Treaty, is not only to grapple with military and defense challenges, but also to foster and protect the values core to its mission and that distinguish NATO as an alliance of like-minded nations. This is why NATO not only convenes military leaders and defense ministers at regular defense ministerial meetings,53 but it also hosts foreign ministers at the same regularity54 and heads of state and government roughly once a year at summits or Leaders Meetings.55 Protecting the rights of its members as free and self-determining nations means, in essence, NATO allies have committed to upholding the integrity of the very institutions that are vulnerable to political warfare. This is why Article 2 of the Washington Treaty exists. It reads:

“The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.”56

Article 2 of NATO’s founding charter is sometimes viewed as the “Canadian clause” or a throwaway paragraph in the Washington Treaty.57 Yet negotiators of NATO agreements know that they should never discount a good diplomatic “hook,” especially when it might be used to prompt positive action. Viewed in that light, Article 2 holds enormous utility in supporting and justifying much-needed NATO action on the political warfare challenges allies face on a routine basis. NATO has forgotten how to exercise its political arm to proactively contend with political and economic coercion as effectively as it does its military arm. Article 2 is critical to establishing an effective counter-political warfare response from NATO.

Specifically, in Article 2, allies have pledged to:

■ Shore up free institutions;

■ Establish public understanding of the principles undergirding institutions;

■ Promote stability and well-being; and

■ Eliminate conflict from international economic policies

and promote economic collaboration.

These Article 2 principles are the very areas at risk from Russian and Chinese political warfare today. NATO allies and partners have fallen behind in combatting the political and economic components of political warfare across the spectrum; as a result, NATO should rethink the mandate it already has and reinvigorate Article 2 to help empower and enable a more effective, comprehensive response to future political warfare campaigns.

This leads to the second concern articulated above, namely, that expanding the aperture of NATO’s activities will inherently dilute the Alliance and its military capabilities. This logic perhaps makes sense in the narrower context of burden sharing and defense planning. Yet the military is not an end in and of itself; rather, the object of the military is to be one means toward the promotion of national security and prosperity. Promotion of stability and security—and, therefore, (if indirectly) prosperity—has been interpreted in a variety of manners over the course of NATO’s history: from deterring Soviet aggression to responding to crises in the Balkans and the Middle East to overcoming Franco-German and Greco-Turkish differences. Further, identifying and countering political warfare is largely an intellectual endeavor; organized appropriately, the cost of building a NATO counter-political warfare capability would be miniscule in comparison to the cost of purchasing defense equipment and acquiring capabilities. Given that today the stability, security, and prosperity of NATO allies and partners are being directly challenged by both Russia and China, this marginal investment would likely yield enormous strategic dividends.

Economic and political coercion campaigns have important linkages to national security—linkages that are often difficult for agencies and institutions to fully appreciate on their own. Trade ministries have a different set of priorities than defense ministries, but they both work on matters that have a direct bearing on the security and well-being of their states. A greater cross-pollination of government efforts improves assessments of the threat and development of potential solutions.

Taking Stock: Assessing Existing Alliance and Partner Efforts to Counter Political Warfare

NATO might usefully seek to build shared understandings of, and approaches to, countering authoritarian coercion in two key areas: disinformation and election interference, and coercive diplomacy and economic subversion.58 What follows is an assessment of the current state of play and areas ripe for multi-stakeholder collaboration on these key issues. Current efforts underway by the Alliance and its members tend to focus on discrete areas of political warfare rather than the full gambit. Countering disinformation and cyber defense are the two most advanced areas of the transatlantic response to hybrid warfare, yet NATO allies and partners lack advanced strategies to mitigate coercive diplomacy and predatory economic practices.

Disinformation and Election Interference

Alliance-Wide Efforts

Disinformation is one of the most nefarious challenges NATO faces. False news and the spread of “alternative” facts and narratives creates confusion, foments distrust in democratic institutions and government itself, sharpens societal divisions, and creates negative psychological and emotional responses that can be used to manipulate people’s viewpoints and beliefs. Across Europe, nations come under near-daily attack from state-supported and rogue actor disinformation, from Russian-language campaigns, Chinese propaganda, social media swarms, and online bots. As Russia and China seek to shape the information environment in their favor,59 NATO allies have put various initiatives in place to help combat disinformation and build societal resilience. Allies have pursued different national initiatives and the Alliance has worked to share best practices. It is worth noting that NATO is further advanced in its understanding and response to Russian disinformation than it is of Chinese disinformation which is much less analyzed and understood in a transatlantic context.

#### Truth decay undermines effective responses to every existential risk

Michael Rich 20. President and Chief Executive Officer of the RAND Corporation. 10-22-2020. "Think Tanks in the Era of Truth Decay," <https://www.rand.org/blog/rand-review/2020/10/think-tanks-in-the-era-of-truth-decay.html>

We are living through a moment of crisis that will define who we are as a nation; yet we can't even agree on what's real and what's rumor. Our political discourse too often amounts to opinions about opinions, shouted across a cable-television split screen. Asked to describe their feelings toward the federal government, a majority of Americans say either “frustrated” or “angry.”

All of this points to a civic disease that I've been calling “Truth Decay,” and that has enfeebled our response to everything from climate change to domestic terrorism to a global pandemic. It's the diminishing role of facts and analysis in American public life, and it cuts much deeper than any political party or demographic. It's why nonpartisan think tanks like RAND are as important now as they have ever been.

I've always said that RAND is an idea as much as a research institute—a belief that the best way to solve the most complex and difficult problems is to begin with facts and objective analysis. In our early days, that meant figuring out how to put a satellite into orbit, or how to manage the threat of global nuclear war. Today, it means saving lives and livelihoods from COVID-19, building a more just and equitable society, and responding to the ever-changing threats of an ever-accelerating world. Our goal throughout has been to make communities safer and more secure, healthier and more prosperous.

At RAND, we have never shied away from a problem because it is too difficult or too complex. We've made countering Truth Decay one of our highest priorities because it is both, and because it threatens the very foundations of our democracy.

In recent and soon-to-be-published studies, there's a growing body of evidence showing that people don't just lack trust in American institutions like Congress or the media. They actively distrust them. They expect those institutions to display some basic competence, to provide accurate information, to perform their duties with integrity. And they just don't see it.

And so, often, they just walk away from the public square. Last year, we asked hundreds of Americans where they get their news. More than a quarter of them said they know where they could go for reliable facts and information—sources like newspapers or television news shows. They just don't have the time or interest to bother.

We've made countering Truth Decay one of our highest priorities because it threatens the very foundations of our democracy.

That kind of disengagement has helped drive a wedge between what is true and what we think is true. Crime rates in American cities are far below the peaks we saw in the 1990s, but you would hardly be alone if you thought it has never been more dangerous to walk down the street. The scientific evidence for childhood vaccines has never been so strong, yet the World Health Organization recently listed vaccine hesitancy as one of the greatest threats to global health.

That's what I mean when I talk about Truth Decay. The proliferation of cable news shows and social media sites has resulted in an echo chamber of voices that agree with us—or a shouting gallery of those that don't. The switch from one-hour network news programs to 24-hour coverage did not come with a 24-fold increase in reported facts. We shouldn't be surprised when people use words like “frustrated” or “angry” to describe the national mood.

But here's why I'm optimistic.

A few years ago, RAND endeavored to review all of the evidence for and against some of the most common ideas for reducing gun violence—tougher background checks, for example, or weapon bans. We found that there was often a lack of reliable evidence either way. Federal constraints on gun research had created a factual vacuum around one of our most vociferous debates. Everyone was just shouting into the void.

That study, though, caught the attention of the Laura and John Arnold Foundation, now called Arnold Ventures. It brought together a research consortium to invest up to $50 million in gun violence research. And Congress, which had resisted funding research into gun violence for 20 years, passed a bipartisan spending bill to provide $25 million more.

We've seen periods before in American history when the truth struggled to be heard. Some of those eras ended with new forms of journalism, recommitted to chasing down facts and holding those in power to account. Others ended with government reforms aimed at earning back the trust of the governed. None of them ended without renewed faith in objective analysis to guide public policy.

As a research institute with two core values—quality and objectivity—that's our stock in trade. The problems we face, as a nation and a world, demand a workforce of people who can collect and analyze data, think through solutions, and provide insights and recommendations without spin or bias. The standards we set at RAND—research that is transparent and clear, based on the best information, and temperate in tone—are meant to ensure that the bluest of blue-state Democrats and the reddest of red-state Republicans can trust our findings equally.

When we launched a fundraising campaign for the future of RAND earlier this year, we named it “Tomorrow Demands Today.” That's a different way of saying what French writer Antoine de Saint-Exupéry once wrote, a line I've always thought spoke directly to RAND: “Your job is not to foresee the future, but to enable it.” At this moment in history, that means restoring facts and analysis to the core of American public policy.

The stakes could not be higher. As a longtime friend, a former chairman of the board at RAND, told me, RAND was established more than 70 years ago to address the existential threat of the time, the Soviet Union and its nuclear arsenal. Truth Decay, he said, is the existential threat of our time.

That, unfortunately, is the truth.

#### Information warfare is independently existential---it rips apart the seams of society.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, //chico

On the existential threat from cyber-enabled information warfare

Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reliable, trustworthy information when and where it is needed. Information is as much a part of human ecology and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems.

Today, chaos reigns in much of the information ecosystem on which societies depend. In many forums for political and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic institutions. Using unsupported anecdotes and sketchy rhetoric, denialists undermine well-established science about climate change and other urgent issues. Established institutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

The founding of the Bulletin predates by several decades the widespread availability of computers, the Internet, smart phones, search engines, and social media. Few could imagine in 1945 a technological environment that affords today’s high-speed and widespread connectivity, high degrees of anonymity, insensitivity to distance and national borders, easy and customized information searches, democratized access to publishing capabilities, inexpensive production and consumption of information content (including and increasingly importantly emotionally evocative video and audio content), disintermediation of established information sources, and ubiquitous, always-on, always-available access to information sources through mobile devices.

Such advances in information technology have heralded the arrival of the information age, a world in which taking near-immediate advantage of information opens up enormous opportunities in both the private and public sectors for improved delivery of existing products and services and, perhaps more important, the creation of entirely new products and services. Products and services can be customized to individual needs and preferences on a large scale and at more affordable costs. Transactional friction can be tremendously reduced. Through the Internet of Things, actuators and sensors can be connected to process control computers to optimize the behavior and function of physical systems. Everywhere that information can be used to create and improve new and existing functionality (that is, essentially everywhere), one can find or imagine new information technologies to do so.

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive burden that such an environment places on their thinking.

#### And, it triggers nuclear escalation by breaking down crisis decisionmaking

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, //chico

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, com- pares them, and then acts accordingly.

But the psychologically informed understanding of real- world decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflex- ive, heuristic System 1 thinking to make decisions, particu- larly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influ- ential participants in one or another of them.

It is thus easy to posit that in this information envir- onment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pres- sure on leaders to act. At the same time, leaders them- selves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted informa- tion originating from their constituencies.

### 1AC---Plan

#### The United States federal government should substantially increase counter-information-warfare cyberspace initiatives with the North Atlantic Treaty Organization.

### 1AC---Solvency

#### Solvency!

#### The plan builds on existing NATO innovation centers to bolster national resilience and support public-private partnerships---that ensures effective countering of disinformation.

Dr. Chris Dolan 22, Professor of Political Science and Director of the Masters of Science Program in Intelligence and Security Studies at Lebanon Valley College, two-time Fulbright U.S. Scholar in international security in North Macedonia and Kosovo, Ph.D. in International Relations and National Security Studies from the University of South Carolina, 2/15/2022, "NATO Must Boost Hybrid Warfare Defenses," https://www.justsecurity.org/80176/nato-must-boost-hybrid-warfare-defenses/, RMax

Russia could launch a conventional military invasion of Ukraine at any moment, but it could also destabilize and undermine it without ever firing a shot. Russian military exercises and positioning are powerful tools of unpredictability that keep NATO and Ukraine off balance while Russian operatives and their proxies wage a hybrid war through covert operations, coordinated disinformation campaigns, and cyber attacks. To build resilience against hybrid warfare, NATO should collaborate with the private sector and devote more resources to technology literacy and innovation.

Russia’s Hybrid Warfare Strategy

Russia’s strategy is centered on promoting a narrative of grievances. Russia believes the United States is using Ukraine and promoting NATO expansion to contain Russian national security interests and encroach on its traditional spheres of influence. It also contends that Ukraine should return to the Minsk Agreements and end its attempt to win back Donbas. These are false narratives because sovereign and independent states have the freedom to determine their own path and seek membership in any alliance. And it would be madness for the Ukrainian government to retake Donbas given the Russian military presence there. The Russian rhetoric is a trojan horse created by the Kremlin to renegotiate the end of the Cold War and redraw European borders the same way Russia did when it illegally annexed Crimea in 2014.

The effectiveness of the Russian narrative depends on combining conventional military positioning with hybrid tactics or “active measures.” Hybrid actions taken in the so-called “gray-zone” typically consist of measures short of conventional warfare such as limited strikes, special operations forces, raids, cyber attacks, and covert influence operations. Hybrid warfare is a central element of Russia’s military strategy, in which operatives remain just below the radar and work with proxies to stage false flags to justify an invasion. To crush the Prague Spring in 1968, Soviet operatives in Czechoslovakia planted weapons in packages labeled “Made in the USA,” which were published in Soviet state-controlled outlets as signs of a U.S.-led plot. The KGB ran active measures during the Soviet war in Afghanistan in the 1980’s, often using “false bands” of Afghan units posing as CIA-backed guerillas to justify Soviet military operations.

Misinformation and disinformation are quickly and efficiently distributed through news channels and social media to influence public opinion. Russian state-owned outlets Russia Today (RT), Tass, and Sputnik have a strong presence on Facebook, Twitter, YouTube, and Telegram, echoing the Kremlin’s position and portraying NATO and the United States as aggressors. In 2013-2014, Russian state media framed the Maidan protests that toppled Ukrainian President Viktor Yanukovych as “fomented by the U.S. in cooperation with fascist Ukrainian nationalists” that were used as a pretext for Russia’s little green men to seize Crimea.

One Russian-backed channel on YouTube is НАШ or NASH TV, which has been promoting Russia’s narrative until it was banned in Ukraine. Founded by former pro-Russia Ukraine parliament member Yevheniy Murayev, NASH TV is a Kremlin mouth piece flooding viewers with anti-American and anti-NATO falsehoods. Last month, the United Kingdom accused Russia of attempting to overthrow Ukrainian President Volodymyr Zelensky and replace him with Murayev. This is the same approach used by Russia when it seized Crimea and installed Sergey Aksyonov as the so-called Prime Minister of Crimea.

Sustained Russian information operations reinforce specific elements in Moscow’s narrative of grievances. First, NATO’s eastward expansion since the end of the Cold War is the real threat, not Russia. Second, Ukraine and Georgia joining NATO would threaten the European security order. Third, the annexation of Crimea and support for separatists in Donbas are liberations of Russian-speaking communities.

Troll factories and bots spread large volumes of fake news stories, making it almost impossible to counter the steady deluge of disinformation. On January 31, it Western media reported that Russia planted fake stories about bomb threats against Ukrainian schools and shopping malls, forcing children to online learning and closing businesses. Just last week, U.S. officials uncovered a plot by Russian intelligence to fabricate a propaganda video portraying fake explosions, corpses, and grieving women designed to legitimate a Russian invasion to protect civilians in Ukraine.

Russia supplements information operations with cyber attacks. Russian hackers recently breached Ukrainian networks, replacing publicly facing websites with messages in Ukrainian and Polish designed to look like a Polish cyber operation. Russian cyber attacks targeted Georgian networks during the 2008 South Ossetia War and again in 2015 when Sandworm, a hacking group linked with Russian intelligence, took down Ukraine’s power grid.

Russian state-sponsored cyber attacks targeting Ukraine can devastate U.S. and NATO networks. The 2017 Notpetya and WannaCry attacks spread throughout the world soon after hitting their targets. In the 2020 Solar Winds hack, cyber criminals directed by Russian intelligence inserted malicious code into updates in Orion software that infected servers used by the U.S. Treasury, Energy, and Defense Departments, as well as Microsoft, Intel, and Cisco. The U.S. Cybersecurity and Infrastructure Security Agency recently warned U.S. networks are vulnerable to more Russian cyber attacks.

Russia also uses blended cyber operations, in which governments tolerate cyber criminals and ransomware groups operating in their countries. For example, the 2021 cyber attacks against Colonial Pipeline, which controls much of the fuel along the U.S. East Coast, were launched by criminal group Darkside operating in Russia. Darkside locked up Colonial Pipeline’s networks and held data hostage until it paid a ransom of $5 million.

Steps NATO Should Take

Information warfare and cyber attacks demonstrate that NATO must get serious about building resilience against hybrid war tactics. This means prioritizing counter-hybrid measures in NATO’s next Strategic Concept, which will be developed in June. NATO should take the following steps to counter Russian information operations:

1. NATO’s next Strategic Concept should update Article V of the North Atlantic Charter, which commits NATO members to defend one another, to include hybrid war tactics in addition to conventional military actions. While the range of gray-zone operations makes it difficult to know when and how to trigger the collective defense mechanism, NATO members should engage in deterrence in the contemporary battlespace.
2. NATO must establish a network of innovation centers to expand on its existing centers of excellence. NATO developed the Strategic Communications Centre of Excellence in Latvia to identify disinformation and the Cooperative Cyber Center of Excellence in Estonia to monitor cyber operations. NATO also approved the NATO-Industry Cyber Partnership to improve the alliance’s relationship with private firms and coordinate cyber defense efforts.
3. New NATO innovation centers could engage in cutting-edge research and development on artificial intelligence, quantum computing, autonomous machines, hypersonic technologies, and information and technology literacy. Innovation centers could be modeled on the European Union’s East Stratcom Task Force, which is staffed with experts specializing in Russian propaganda through its EUDisinfo site. Innovation centers funded through NATO’s Science for Peace and Security program could partner with NATO’s Joint Intelligence and Security Division (JISD).These centers could also develop public-private partnerships with commercial firms, academic institutions, and civil society groups to build resilience through training centers, research institutes, and information technology programming.
4. Governance and rule of law among alliance members must be improved as weak institutions provide maligned external actors avenues to interfere. For example, while an innovation center can improve North Macedonia’s ability to combat disinformation and cyberattacks, it must also improve domestic governance, combat corruption, strengthen judicial practices, and enhance economic opportunities. President Biden’s executive actions targeting corruption in the Western Balkans is a significant step to promote accountability.

The most effective way to defend against Russian hybrid tactics is for NATO to partner with the private sector and academia to lead research and development initiatives that can boost alliance-wide emerging and disruptive technologies policies. Since many security-related applications of emerging and disruptive technologies are derived from private firms, partnering with companies, start-ups, and universities and research institutes is essential to securing alliance members in the 21st Century. NATO should invest in strengthening capacity and innovation against hybrid attacks as much as it invests in conventional military hardware.

#### U.S.-led centers are key---it ensures cohesion and cooperation between Allies.

David Shedd 20, professor at the Patrick Henry College, former acting director of the Defense Intelligence Agency; and Ivana Stradner, Visiting Research Fellow at the American Enterprise Institute, J.S.D. from the University of California, Berkeley,8/11/2020, "Countering Russia’s Influence Operations in the Balkans," https://www.heritage.org/europe/commentary/countering-russias-influence-operations-the-balkans, RMax

Even the pandemic has the potential for fomenting political unrest.

In recent days, thousands of Serbs have taken to the streets to protest Serbian President Aleksandar Vucic’s announced strict curfew in response to a surge in Covid-19 cases. Many have pointed a finger at pro-Russia ultra-right groups and foreign intelligence services for fueling the violent riots.

Moscow denies any “Russian trace” in the unrest. Whether Russia is behind the violent protests in Belgrade remains to be seen. One thing is for certain. The Kremlin’s efforts to sow mayhem in the Balkans would not be new; this would merely be the latest attempt by a resurgent Russia to threaten Euro-Atlantic security and challenge the United States’ ability to defend its interests in Europe.

Russia is promoting its interests in the Western Balkans through the widespread use of disinformation and cyberwarfare. The U.S., however, isn’t helpless. It has an opportunity to obtain insights into these efforts and counter Russia's influence campaigns. It is time to confront Russia's strongman Vladimir Putin's cyber games before American interests are permanently damaged in the Balkans.

The U.S. and the E.U. have long been ambivalent about defining their interests in the Western Balkans. Russia has capitalized on these years of neglect and leveraged a power vacuum in the former Yugoslavia to gain economic and political influence. The region is now at the forefront of Russia's use of low-cost strategies to expand its global influence and undermine western interests.

Russian disinformation, aided by repeated cyberattacks on government institutions, was instrumental in the 2016 Moscow-sponsored coup attempt in Montenegro. In North Macedonia, Russia spread disinformation prior to the name-change referendum that finally enabled North Macedonia to join NATO. It also established hundreds of North Macedonia-based “troll factories," from which Russia pedaled fake news against the 2016 U.S. elections. Facebook recently banned troll farms from North Macedonia that pushed COVID-19 disinformation.

Moscow has also been investing in critical sectors in Croatia. With its strategy of fomenting political divisions, the Kremlin has been exploiting internal conflicts in Albania. In Bosnia and Herzegovina, disinformation campaigns have sown ethnic and religious discord, while promoting the secession of ethnic Serb regions from Bosnia. In response, the U.S. should encourage the transatlantic integration for Bosnia and Herzegovina, the Western Balkans’ most fragile country.

Russia has used state-sponsored media to promote nationalist and anti-Western narratives in Serbia, including the opening of a Sputnik office in Belgrade. Also,  Russian-run “Humanitarian Center” in Serbia is very close to the main NATO based in Kosovo (Camp Bondsteel). Some European and American officials fear that it serves as a base for the Kremlin intelligence-gathering activities to eavesdrop on U.S. interests in the Balkans.

Russia’s preeminent goals in the Balkans have been to refine their disinformation tactics and erode Western influence in the region, including in Croatia, Montenegro, North Macedonia and Albania, which are all NATO members. The West needs to aggressively respond to this Russian posture, including using a cyber-focused campaign to counter Russia's provocations.

For crafting such a strategy, the West should look to Estonia. After the 2007 Russian cyberattack on Estonian government institutions, Estonia became a global leader in cybersecurity and home to the NATO Cooperative Cyber Defense Centre of Excellence, which is a cyber-defense hub that supports member nations with cyber-defense expertise. A similar approach by the West would benefit the Western Balkans, where information and communication technology sector is the most promising and the fastest growing economic sector in the region. In Serbia alone, the I.T. sector generates more than 10% of GDP with a similar trend in other countries in the region, which have some of the highest numbers of outsourced I.T. workers per capita in Europe.

An American-led strategy should focus on creating a regional cyber-security infrastructure in the Western Balkans, modeled on Estonia's example. Given that countries in the Western Balkans share the same cyber-security threats from Russia and, more recently, from China, a regional hub for cybersecurity would allow states to cooperate among each other in cyber deterrence, attribution of attacks and collective countermeasures.

Several countries in the Western Balkans have joined NATO, but alliances are notoriously unreliable, especially among the smaller states. Countries in the Western Balkans need strong NATO and E.U. ties to withstand Russian influence. Cyber-security is one of the areas where they can strengthen their positions in allegiance with the western democracies.

The timing is excellent for the U.S. to establish a regional cyber-security hub in the Western Balkans. Immediate steps need to be taken to halt malign Russian influence. With elections approaching this year in the U.S., North Macedonia, Croatia and Montenegro, countries should continue cooperating to counter malicious Russian cyber activities.

The U.S. can learn more about Russian cyber tactics at the same time. One way to send a strong message would be to deploy a cyber-team to strengthen NATO’s countries’ cyber-capabilities in an effort to thwart future Russian network intrusions such as the one that was undertaken by Russian intelligence operators in Bulgaria in 2017.

Serbia, a key ally to Moscow in the region, remains the biggest obstacle to countering Russian influence. Serbia just had parliamentary elections boycotted by the opposition that resulted in Vucic's Serbian Progressive party winning a landslide victory and further strengthening his power. The close Russia-Serbian relationship can make it difficult to detect Russia's subversive activities.

Of all the Western Balkans countries, Serbia had the highest military expenditure in 2019, and President Vucic thanked Russia for making Serbia’s military 10 times stronger since NATO intervention in 1999. After Russia employed an S-400 missile system in Serbia for a military drill, the Pantsir S1 air-defense systems were delivered this past February, despite a looming U.S. sanctions threat.

Should Serbia continue obtaining Russian weapons, Washington should impose sanctions. Serbia must understand that its strategy of neutrality is unacceptable to the U.S., as are its claims to balance their interests among Russia, China and the West. The U.S. should remain solidly committed, leading efforts to solve the Kosovo dispute and wrest control of that narrative from Russia.

While variances in the national interests may complicate cooperation among the Western Balkan countries, they share similar vital objectives that make cooperation possible and even attractive under U.S. leadership. Among these are the historical fear of Russian domination and a desire for E.U. and NATO membership. A U.S.-led strategy with NATO country participation to enhance their cyber-capabilities will improve their security in countering nefarious Russian influence while enhancing cooperation between Balkan nations.

Moscow is determined to expand its influence in the Western Balkans, using cyber-warfare at the expense of U.S. and western interests. To prevent it, the U.S. should design a new strategy for the Western Balkans that demonstrates that the U.S. is committed to countering Russia's disruptive activities in the Western Balkans and beyond. The time for that response is now.

#### U.S. security cooperation streamlines NATO capabilities to prevent Russian disinformation.

Allison Heiser 17, leader in Booz Allen’s joint combatant command business, experience supporting security cooperation efforts with clients in the Office of the Secretary of the U.S. Air Force, U.S. Marine Corps Headquarters, and U.S. Africa Command; Peter Walpole, principal at Booz Allen, experience cooperating with NATO, the Marine Corps, the Navy, the Air Force, and the Army; and Alex D’Agostino, principal in the Joint Combatant Commands account at Booz Allen, supports clients at the DSCA, sometime during or after 2017, "The Security Cooperation Landscape in Europe," https://www.boozallen.com/markets/defense/security-cooperation/the-security-cooperation-landscape-in-europe.html, RMax, Note: the date of the article was impossible to find, so I determined that the article had to be sometime after or during 2017, when the “Countering Russian Influence Fund” that the card mentions was enacted, if you have any questions about the process of dating this article email me: raleighdebate@gmail.com

Interoperability for integrated partner resilience

U.S. allies and partners are facing a range of multidomain challenges and multidimensional asymmetric threats, from cruise missiles to cyber attacks. Now more than ever, effective security cooperation is critical to ensure collective regional defense. Just as essential, U.S. national security strategic guidance calls for revitalized alliances and partnerships to address shared threats in an era of great power competition.

Interoperability of U.S. and European forces—the ability to effectively shoot, move, and communicate together—strengthens regional deterrence, enhances relationships, and is a powerful component of foreign policy. Enhancing multilateral security cooperation initiatives in strategic regions, such as the Black Sea and the Baltics, is especially important to bolster integrated partner resilience. This helps enable the U.S. to reduce its military footprint in Europe while enabling NATO allies to steadily improve collective defensive capabilities and address shared regional threats.

Security Cooperation Across the Lifecycle

The U.S. European Command and its theater components work together with partner and allied security forces across the lifecycle of security cooperation—from planning to implementation, integration, and sustainment. Through the Offices of Defense Cooperation in each European capital, our team supports the development and execution of diverse security cooperation programs. We have broad experience helping increase partner capability and expanding capacity to mitigate shared security threats.

Booz Allen plays a key role in a range of critical regional security cooperation programs in Europe. Here are some key examples:

* We strengthen regional programs to enable integrated air and missile defense and maritime domain awareness in the Baltics. These solutions leverage low-cost, disruptive, and immersive technologies that are scalable, tailorable, and not reliant on expensive proprietary systems which become obsolete in a few short years.
* Our experts help multiple European allies and partners develop their cyber defense capabilities. The team’s work includes recruiting, training, and retaining top talent to build and defend critical networks and infrastructure. This protects not only U.S. technology embedded in increasingly complex weapons systems, but also shared coalition networks that support combined operations.
* As a U.S. strategic partner, we support the Ukraine Security Assistance Initiative. We’re helping Ukraine develop a national strategy and focus on areas such as supply chain and logistical coordination. In addition, we have played a key role in sustainment planning and capacity building. This is a critical priority, as Ukraine has received increasingly sophisticated equipment to address regional security threats.

Combating Disinformation

Growing Russian and Chinese influences in Europe must be addressed by sustained U.S. security cooperation investment in that region. The need is accelerated by ongoing campaigns that use false and misleading information to shape opinion against the collective interests of the U.S. and its allies and partners in the region. Allies and partners must develop interoperable capabilities to counter mis- and disinformation designed to undermine regional cohesion.

Enhancing partners’ strategic communications capabilities by leveraging security cooperation programs such as the Counter Russia Influence Fund benefits U.S. strategic interests by combating malign influence and improving the resilience of alliance cohesion. U.S. security cooperation initiatives must continue to focus on combating hybrid threats in the information domain, in addition to investing in technological solutions for allied interoperability.

#### Current NATO doctrine fails to comprehensively respond to Russian disinformation---coordinating responses solves and serves as a model for national governments.

Tomasz Chłoń 22, Director of NATO Information Office in Moscow, postgraduates diplomas in international relations and European integration from the Polish Institute of International Relations, the University of Maastricht, and the University of Warsaw, co-author of the book “Counter-Disinformation Education and Research Platform – Building Social Resilience,” May 2022, “NATO and Countering Disinformation The Need for a More Proactive Approach from the Member States,” https://www.globsec.org/wp-content/uploads/2022/05/NATO-and-Countering-Disinformation-ver1-spreads.pdf, RMax

Towards a Consistent Response to 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 Plan4 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)6 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.7 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.8

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 20229 . 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.

Strategic Context

The Alliance’s new Strategic Concept could therefore reflect more comprehensively the key tenets of an enhanced approach to disinformation, encompassing public diplomacy, strategic communication and social resilience. Such an approach could also consider new and innovative tools to combat disinformation, given that these can fit into a broader strategic context of NATO’s work.

In 2019, the Alliance approved not only the first secret military strategy in over 50 years but also a strategy for developing the necessary military and technological potential in connection with the changing nature of conflicts (NATO Warfighting Capstone Concept). With its stronger deterrence and defence approach to security, NATO began implementing a policy that enabled the coordinated development of breakthrough technologies, recognising that technology development will be a priority in seven areas: (i) artificial intelligence, (ii) advanced big data analysis, (iii) autonomous technologies, (iv) quantum computing technologies, (v) biotechnology, (vi) hypersonic capabilities and (vii) space technologies. In February 2021, the Allies approved the Coherent Implementation Strategy on Emerging and Disruptive Technologies. Eight months later, in October, the first NATO strategy on artificial intelligence was approved. From the perspective of disinformation activities, the future of artificial intelligence can be seen as a dual-purpose tool. Depending on human decisions, it can become a sword in the hands of opponents of freedom or a shield that protects societies and individuals against the consequences of their actions.

NATO Strategic Concept and Recommendations

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 practices10.

# ADV---Russia

## UQ

### UQ---Russia---AT: Squo Solves

#### All empirics show that Russian attacks are frequent and becoming more destabilizing.

Ian Thornton-Trump 22, Chief Information Security Officer for Cyjax Ltd, “RUSSIA: THE CYBER GLOBAL PROTAGONIST,” The EDP Audit, Control, and Security Newsletter, Vol. 65, No. 3, pp. 19-26, cy

Russian disinformation operations are currently a cyber cornerstone of the country’s efforts to wield influence worldwide. Whether trying to weaken the EU, NATO, individual countries, or other groups, Russian operations perpetrated by cyber-espionage groups such as APT28 and APT29 have fostered anxiety, fear, and division throughout the world. Disinformation efforts have their roots in “active measures”, or propaganda efforts invented by the Soviet Union and embraced by the current Russian foreign intelligence services. Russian disinformation operations were credited with sowing discontent in the United States and damaging Hillary Clinton’s electoral chances in 2016; boosting support for far-right Italian political parties among those consuming alternative news stories in 2018; and prompting a decline in the Spanish leaders’ ability to influence public opinion during the 2017 Catalan crisis.19,20 In a CSIS article “Did Russia Influence Brexit?”, Russian cyber influence operations in the UK are elaborated on:

The UK Government is accused of making a deliberate effort not to find out how Russian influence may have affected the June 2016 vote. This is more incredulous because the government admits there was Russian interference in the 2014 Scottish referendum, declaring it the first time that Russia directly interfered in a Western election. The government also admits that Russia interfered in the [UK] December 2019 general election.21

### UQ---Russia

#### Russian “Troll Farms” are accelerating at breakneck speeds --- Ukraine is the brink --- that gets parroted by the far right and undermines U.S internationalism

Mark Scott 22, Chief Technology Correspondent at POLITICO, writing about the global collision of technology and politics “As Ukraine conflict heats up, so too does disinformation,” POLITICO, 1-27-22, <https://www.politico.eu/article/russia-ukraine-disinformation-nato-united-states-special-forces-winter-olympics-moscow-kremlin-kyiv/> //chico

Ukrainian special forces planning so-called "false flag" operations. The United States considering chemical weapons attacks in the Eastern European country. NATO preparing to attack Russia during the upcoming Winter Olympics.

The Kremlin is ratcheting up its disinformation game with claims like these amid rising geopolitical tensions between Moscow and Western capitals, according to a review of state-backed media content over the last 10 days by POLITICO.

The campaign — spread via Moscow-backed outlets like RT, domestic state-owned broadcasters and fake social media accounts in multiple Western languages — coincides with a large-scale military buildup along the Ukrainian border and increased Western military aide to support Kyiv.

Moscow's goal, according to three Western national security officials and five external disinformation researchers, is to use wedge issues to foster division among Western countries over their support for Ukraine; counter NATO's claims against Moscow; and create plausible deniability over potential atrocities including the possible use of chemical weapons.

"Where they really are moving the needle is on undermining support for U.S. internationalism," said Bret Schafer, head of the information manipulation team at the German Marshall Fund's Alliance for Securing Democracy, in reference to the Kremlin's disinformation tactics.

"Russia state media messaging is more effective at chipping away at the West's geopolitical goals than it is in dividing the West because we do that well enough on our own," he added.

In recent weeks, Western governments have been particularly vocal about outing Russian online tactics. Two of the Western security officials, who spoke on the condition of anonymity to discuss governments' internal strategies, said the amped-up response was partly because Moscow has been successful in tilting public opinion around geopolitical issues in the past.

The U.S. State Department published a "cheat sheet" seeking to explain the Kremlin's online falsehoods, while also criticizing Moscow for its "disregard for truth." In the European Union, the so-called East Stratcom team within the European External Action Service, which is tasked with monitoring Russian online propaganda, highlighted the Kremlin's tactics, although the 27-country bloc is still divided over how strongly to push back against Moscow.

The Kremlin, in turn, has pushed back against the criticism, claiming that Western governments and media are peddling mistruths about the situation in Ukraine, and that it is Moscow, not Washington or Brussels, that is pushing for a peaceful resolution.

Just like 2014, but worse

Russia is no newcomer to disinformation on Ukraine.

Since the country annexed part of its neighbor in 2014, Kremlin-backed media has pumped out a steady stream of accusations that Kyiv is run by neo-Nazis; that NATO is either too weak to defend the country or too aggressive in its military stance; and that Western citizens did not see the point in protecting Ukraine.

Those narratives are being updated amid the current tensions.

Russian broadcasters have shaped the debate at home as President Vladimir Putin defending the interests of Greater Russia, including sending Russian troops to Belarus as a routine military maneuver with a close ally. On the Kremlin's international news outlets — which collectively have millions of followers on social media — the likes of RT and Sputnik have criticized Western leaders for spending resources on Ukraine amid the pandemic and questioned how defending Kyiv plays into the national interests of either the U.S. or EU countries.

"The pro-Kremlin disinformation machine uses a well-known tactic of throwing mud against a wall to see what sticks," said one of the Western officials, who was not authorized to speak publicly about their work tracking Russian online tactics. "There are a lot of contradictions but consistency has never been a strong suit of the Kremlin's disinformation machine. It’s rather about muddying the waters."

For Monika Richter, a former EU official specializing in disinformation and current head of research at Semantic Visions, a Prague-based intelligence firm, there's a disconnect between domestic propaganda, which has focused on framing NATO as the enemy and Ukraine as a means to obtaining security assurances from Washington, and the Kremlin's foreign media operations, which have been more aggressive in claiming that the West wants war in Eastern Europe.

"The outward disinformation campaign is rattling," she said. "It appears to be a coordinated effort to lay the groundwork ahead of another attack."

Chemical weapons and blaming NATO

Yet in recent days, specific themes have started to bubble to the surface.

One relates to accusations — mostly in non-English-language outlets — that either Ukraine or NATO could use chemical weapons within the country in the hope of blaming Russia for it. These messages were then picked up either by official diplomatic accounts or American entities like SouthFront — a think tank the U.S. State Department has tied to the Kremlin — and shared hundreds of times on social media, according to POLITICO's analysis via CrowdTangle, a social media analytics tool owned by Meta.

Another is that the West, not Russia, is the main driver in the potential conflict.

Across RT and Sputnik — in English, French, German and Spanish — reports highlighted how NATO countries had provided weapons to the Ukrainian government, and claimed that U.S. President Joe Biden was using the stand-off to boost his popularity at home. In multiple reports, again heavily shared on social media, RT articles questioned why the U.S. and Europe were supporting Ukraine when the COVID-19 pandemic was rife at home.

Russian-backed media has repeatedly captured significant attention among Western audiences, particularly those in Europe where anti-American sentiment has risen since 2016, according to the Pew Research Center. But Kremlin talking points also have seeped into mainstream U.S. media, particularly promoted by right-wing influencers who have no affiliation to Moscow and have tried to use the Ukrainian stand-off to attack Biden and his domestic agenda.

That includes raising questions about why Washington would enter the conflict in the first place, concerns that U.S. involvement in Ukraine could end similarly to what happened in Afghanistan, and calls for the Biden administration to focus on domestic, not foreign, issues.

“There’s an alignment of interests between the U.S. far right and the Russian government,” said Schafer of the German Marshall Fund. "It's exceptionally beneficial to have super mainstream U.S. voices parroting lines that Russia has been saying for years.”

### UQ---Future of War

#### The pandemic reveals that hybrid warfare through disinformation is the future of war.

Gill and Goolsby 22, Ritu Gill has a PhD in psychology from Carleton university, Rebbeca Goolsby is the co-Lead of a NATO Research Technology Group on cyberdiplomacy and communications, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. XXII, 213 (under “Foreword”) //chico

In a world of significant global challenges, from an increasingly assertive Russia and terrorism to disruptive technologies and the rise of China, the Transatlantic Alliance is more important than ever. NATO has been, is, and will continue to be a unique exercise in human history. We are an alliance of nations based on fundamental common values, with our values an essential part, and the agility to adjust and adapt to ever-changing circumstances key ingredients of NATO’s enduring success. This strategic narrative, defined by our values and actions, is the bond, the glue, the foundation that keeps us together. Sustaining and protecting that narrative is an essential aspect of our Alliance.

Our narrative is clear and straightforward: there is no foundation for decent lives, economic activities, or fulfillment of individual or collective dreams and ambitions without shared security. There is no way to build a prosperous, democratic society without ensuring the foundation of security in the broader sense of that term, built on our shared values and freedom. Ensuring this security has been our raison d’être.

This is our history.

Still, history is not static. The narrative is not linear. As we are witnessing in these challenging times, history shows NATO responding to difficult situations, as well as pleasant and unpleasant geopolitical surprises. It has done so by an innate yet fragile capacity to adjust, be proactive, and show agility. This is also in the genes, in the DNA of our great organization. Yet overall this history, the essential mission remains, that is, to keep 1 billion citizens living in NATO, allied nations, safe.

This is our story.

As long as history and nations exist, there will be some form of traditional military threat to our security. NATO will need to understand and adapt to these conventional threats. But we also see today a broader definition of security. The pandemic has only accelerated and highlighted this trend. We see a considerable spike in the intensity and scale of hybrid activities, including increased use of disinformation and propaganda. If we look at the world now and into the future, we see security has become more complex, more transversal in this quest for permanent adaptation.

## IL

### IL---Russia---Broad

#### The pandemic signals a water-shed moment in hybrid warfare. Russian desires a return to greatness and will use info-warfare to undermine Alliance cohesion. That collapses unipolarity and constitutes an existential threat.

D. F. Reding & B. Wells 22, Dale F. Reding and Bryan Wells are both Chief Scientists at NATO, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 25-43 (under the ch. titled, “Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies,”) //chico

The COVID-19 pandemic is not a consequence of geostrategic conflict. Never- theless, the pandemic has had a direct and adverse effect on all Alliance nations, particularly their medical, political, and economic systems. Exploiting this crisis, several countries and groups with partisan agendas attempted to create a watershed moment in global security by undermining Alliance cohesion and national resolve. As noted by the World Health Organization’s (WHO) Director-General at the 2020 Munich Security Conference, “We’re not just fighting an epidemic; we’re fighting an infodemic” (Zarocostas, 2020).

The COVID-19 pandemic presented an information exploitation opportunity for some strategic actors as part of existing grey zone conflicts. At the same time, this has raised awareness of the enduring challenge of countering misinformation, disinfor- mation and outright propaganda. These attacks can, and have, imposed considerable costs to the nations and has needlessly increased the death rate from COVID-19. However, in any complex crisis, such as that experienced during pandemics, infor- mation transparency and open communication builds trust and ultimately saves lives.

Over the initial phases of the COVID-19 crises, Russian disinformation campaigns focused on stories such as (EEAS, 2021): COVID-19 was developed in NATO labo- ratories, global elites are imposing tyranny, and the EU is disintegrating. As time went on, these attacks expanded to include those designed to increase doubt on vaccine efficacy, safety and availability, accusing countries of genocide for not using the Russian vaccine (Sputnik V), suggesting that migrants (or NATO) have been spreading the virus across Europe, as well as implying that degenerate geopolit- ical and commercial interests were over-riding the interests of European and North American citizens. While some of these attacks are homegrown, there has also been a trend towards amplifying attacks from secondary sources (e.g., right & left-wing groups, Iran, ISIS, China, anti-vaxxers, etc.). This approach maintains a veneer of plausible deniability and evades responsibility for accurate reporting. At the same time, these efforts have presented an inflated narrative of Russian (and to some extent Chinese) generosity and scientific, military and societal strength. This narrative was supported by logistics and medical support provided to groups with deep historical and linguistic ties to Russia or Kremlin-friendly forces (Ozawa, 2020).

In late April of 2020, Russia launched three harmonised disinformation attacks on NATO (NATO, 2020b). First, a fake letter was published, purportedly from Jen Stoltenberg, NATO’s Secretary-General, to Raimundus Karoblis, Lithuania’s Minister of Defence. The letter noted that NATO had decided to withdraw its multi- national battlegroup from Lithuania due to rising COVID-19 infections. The letters were posted on blogs in English and Lithuanian and were later picked up by various websites and social media platforms. Fake accounts, created days before, were used to spread the disinformation further. Following this, an edited YouTube video was released suggesting that COVID-19 within the multinational battlegroup was the single agenda item for a recent NATO Defence Ministers meeting. Finally, the letter was sent directly to NATO Headquarters via a spoofed NATO e-mail address. Surprisingly, given the care taken to orchestrate this attack, the letter contained many formatting, structural and grammatical mistakes, and was recognized quickly as a fake.

Ultimately the attack was a failure and died out quickly. NATO responded rapidly to discredit the story, as did the Lithuanian Defence Ministry. Early identifica- tion (understand) and rapid reaction (engage) nullified the attack. As noted by the Secretary-General, “They have not been successful because, first of all, it has been clearly revealed that this is a fake letter; secondly, we’ve seen that NATO allies remain committed, remain united, and are actually helping each other in the midst of the coronavirus crisis” (NATO, 2020b).

Disinformation has been a constant threat to the Alliance since its inception. Nevertheless, with the increased use of asymmetric (hybrid) warfare and the attendant growth of social media, disinformation and its institutional twin of propaganda have significantly increased in volume and precision. Moreover, these efforts are part of more significant military and geopolitical trends, such as those presented by hybrid or grey zone warfare, where success is defined through operations in the cognitive sphere.

This infodemic has presented an existential crisis to Alliance nations on par with the COVID-19 pandemic itself. Throughout this crisis, NATO undertook to sustain its military and political mission, operations, and activities while maintaining opera- tional readiness. This included using NATO strategic lift to ensure medical equipment supplies were delivered to the Alliance and partner nations. After the initial stages of the pandemic, NATO developed a refined operational plan, took stock of lessons learned, restocked medical supplies, identified funding and explored ways and means to support Alliance and national resilience. These activities created a solid narrative of an Alliance coming together to support national COVID-19 responses. Never- theless, this positive narrative was challenged by misinformation, overt propaganda, and weaponised information campaigns, i.e., targeted disinformation.

2.4 Countering Disinformation: Engagement in the Cognitive Domain

2.4.1 A Successful Counter-Strategy

Drawing on long experience gained over its seventy-two-year history, NATO has developed a simple bifurcated strategy for countering disinformation. This strategy, built upon the classic OODA loop or Boyd Cycle (observe-orient-decide-act) (Osinga, 2005), consists of understand (observe-orient) and engage (decide-act) phases. Expanding on this (NATO, 2020b):

Understand: NATO “Information Environmental Assessments” systematically track, monitor and assess the information environment germane to NATO operations or policies. This observe-orient function allows NATO to identify information attacks and evaluate the impact of counter-narratives. Engage: Once an attack is understood, a strategic approach is identified, and a fact-based counter-narrative developed. Over the longer term, this builds upon the success and lessons learned from previous disinformation counter-strategies. These counter-narratives and information products are “fact-based, timely, transparent and coordinated” (NATO, 2020b). This enables NATO to deliver a targeted effect within the contested cognitive domain.

The success of these efforts is greatly enhanced when coordinated across the Alliance. Consistency of message, clarity of meaning, rapid and agile reaction, and a fact-based counter-narrative are crucial to building trust and confidence. Ensuring consistency of this narrative and sharing cognitive domain awareness within the Alliance, EU, UN and other allies or partners increases the likelihood of countering a sustained and reactive disinformation campaign while building societal resilience to such attacks. Nevertheless, there are inevitably groups or populations resistant to such measures preferring conspiracy theories or biased narratives. The goal is not to convince everyone but to reach an audience receptive to a facts-based approach, thereby building trust within such communities and minimising the damage inflicted by misinformation, disinformation, or propaganda. In the end, “Sunlight is said to be the best of disinfectants; electric light the most efficient policeman” (Brandeis, 2014).

2.4.2 Understand: Cognitive Domain Situational Awareness (CDSA)

Situational awareness is the key to operational success, or more generally, success- fully applying the instruments of national power, be they diplomatic, information, military or economic (DIME) (Worley, 2012). The famous military theorist Sun Tzu noted, “if you know the enemy and know yourself, you need not fear the results of a hundred battles” (Tzu, 2018). However, the modern cognitive information battle- ground exists in a complex web of worldwide intersecting and interconnected socio- technical networks, with state, non-state actors and empowered individuals seeking influence and attention. NATO’s cognitive domain situational awareness provides it with actionable insights, helping to shape its communication response and inform the nations and partners. To counter disinformation attacks, NATO recommends that consumers of information: check the credibility of the source; assess the emotional tone; look for alternate sources, check for doctored images/video and curb their own biases (NATO, 2020b).

Regarding COVID-19, many state, non-state and agenda-driven individuals have used the crisis to spread misinformation, disinformation, and outright propaganda. These efforts are often not accidental or ill-considered. In many cases, they are delib- erate actions designed to exploit modern marketing stratagems and are highly devel- oped, employing sophisticated cyber and psychological warfare approaches. They seek strategic effects, attempting to provide a (false or misleading) narrative to create an alternative worldview for calculated impact. Such attacks are also characterised by inconsistent messaging, rapid evolutionary improvements based on message success and a shotgun approach, i.e., wide-area attacks. However, building upon modern methods, these attacks are also developing in sophistication, becoming even more targeted and effects oriented as they build upon commercial approaches, including automation.

State actors, such as Russia, employ a broad spectrum of such approaches in remarkably sophisticated fashion. Media outlets, controlled by the Russian govern- ment, such as RT (Russia Today) or Sputnik, use a broadband strategy of disinfor- mation through a mix of news stories that blend fact with demonstrable falsehoods (NATO, 2020b). At the same time, they employ fakes sites, automated bots, and burner accounts to amplify and normalise narratives while creating momentum and uptake by other media. These later approaches may be highly targeted at specific receptive groups defined by ideology, geography, or demographics. However, the aims of such attacks are long-term and strategic, aiming to discredit NATO, the nations and Alliance values or the value of the Alliance. Sadly, in this regard, not much has changed since the cold war, except the volume, automation and targeting effectiveness of such disinformation attacks. Trust has always been challenging to build and harder to maintain.

At the start of the COVID-19 crisis, several actors took the opportunity to launch disinformation attacks on the Alliance. A surge in such attacks occurred between March and June of 2020, although the volume and nature of these attacks morphed over time. To put this in perspective, from December 2019 to April 2020, over eight thousand cases of disinformation were noted (Ozawa, 2020) by the European External Action Service’s East StratCom Task Force (European External Action Service, 2021b). A review of the same database for December 2019 to May 2021 notes 11,787 instances of pro-Kremlin disinformation, with approximately 203 related to COVID or the pandemic and 1388 associated with NATO.

2.4.2.1 Russia

The use of disinformation as a Russian strategic weapon was honed during the cold war. Then again, Russia’s skilful use of propaganda and disinformation goes back to Lenin (Ball, 2017) and arguably even further back to Potemkin (Montefiore, 2005). Indeed Lenin is quoted as saying, “A lie told often enough becomes the truth” (DiResta, 2018). Using disinformation as a strategic tool returned, with a vengeance, following the ascension of Vladimir Putin. In 2014, Russian—NATO relations were seriously strained due to the Russian annexation of Crimea. This territorial appropri- ation was built upon a long campaign of disinformation in the region (Ball, 2017) as part of the skilful use of hybrid warfare tactics, which included the use of “little green men” (Pifer, 2019) to spearhead the process. As noted at the Wales summit in 2014, by General Philip Breedlove, Supreme Allied Commander Europe (SACEUR) at the time, “[Russia is conducting] the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare” (Pomerantsev, 2014). Lever- aging new technologies and social media has enabled highly effective information campaigns whose implications are only beginning to be appreciated and understood (Chabuk & Jonas, 2018).

Since that time, Russian disinformation campaigns have focused on the predictable goals of undermining Alliance cohesion and stability, bring into disrepute NATO’s military or political actions, spreading panic and undermining democratic processes (Monaghan, 2020; Ozawa, 2020). Strategically these efforts are designed to weaken the economic and military capability and capacity of the Alliance while creating a multi-polar world order more conducive to Russian interests as well as leaving Russia and others in a more advantageous military, economic and political position (Ozawa, 2020). In the context of COVID-19, disinformation activities that ultimately delay, weaken, prolong, or confuse will extend and amplify the pandemic and its adverse effects while provoking panic. This could eventually undermine soci- etal bonds and degrade the geopolitical strength of Europe and North America. As noted (Pomerantsev, 2014), “The new Russia doesn’t just deal in the petty disinfor- mation, forgeries, lies, leaks, and cyber-sabotage usually associated with informa- tion warfare. It reinvents reality, creating mass hallucinations that then translate into political action.” Given the insignificant resource costs and minimal negative consequences of such a disinformation campaign, such a strategy is being pursued vigorously. Consequently, it is no surprise that the COVID-19 crisis became just another opportunity to be exploited.

In Spring 2021, Latvia was subject to a Russian disinformation attack, accusing Canadian Forces troops operating in Latvia of spreading COVID-19 to Latvia (NATO, 2020b). This disinformation attack consisted of a fake interview, modified screen- shots from the battlegroup’s FaceBook page, and an attempt to solicit a nega- tive response from the Latvian Minister of Defence through a spoofed journalist’s account.

Poland was also targeted at the same time (NATO, 2020b). In this case, a forged letter was planted, via a cyber-attack, on the Polish War Studies academy’s website from Brigadier General Ryszard Parafianowicz. This letter criticised US forces in Poland, and in particular, the associated DEFENDER-Europe 20 military exercise. Once again, multiple blogs and sympathetic media outlets were used to spread the message, spoofing an e-mail from a former Polish parliamentarian to Polish media outlets.

While these targeted disinformation attacks were ongoing, in the spring of 2020, Russia continued to spread disinformation through state-influenced or controlled media channels on the nature and scope of NATO exercises in Eastern Europe in the Spring of 2020 (NATO, 2020b). NATO was accused of continuing to hold large- scale exercises with no regard for the health and safety of national populations. NATO forces were also accused of ignoring travel restrictions and safety protocols, spreading COVID-19 throughout Europe. Starting in early January of 2020, and perhaps in an even more egregious disinformation attack, pro-Kremlin media explic- itly accused NATO (and the US in particular) of having engineered the COVID-19 as a biological warfare agent in secret laboratories in Latvia, Georgia, Kazakhstan, Moldova or Ukraine. The COVID-19 pandemic was portrayed as a “biological Cher- nobyl”. As late as May 2020, the Russian Minister of Foreign Affairs Sergey Lavrov was quoted as saying, “Washington’s unwillingness to ensure the transparency of its military biological activities in various parts of the world raises questions about what is really going on there and what the actual goals are” (NATO, 2020b).

Across all these targeted attacks, NATO worked with the countries involved to identify and counter the disinformation attempts before they could gain a foothold within broader media circles (NATO, 2020b). NATO also provided facts to counter the information wide-area attacks made through Russian media. In all cases, these have helped build a more fact-oriented narrative within the Alliance and Eastern Europe more specifically. However, the impact on counter-NATO narratives within Russia has perhaps been less successful (e.g. Schaffner & Flood, 2020), in no small measure due to state control or influence on major media outlets (Ball, 2017).

These Russian targeted disinformation campaigns follow a broadly similar pattern (NATO, 2020b). Such attacks employ forgeries (doctored letters, fake social media posts and bogus interviews), use burner accounts to create false personas or exploit that of a credible individual, generate explicit falsehoods and amplification of disin- formation by arms-length but pro-Russian news and social media sites, engineer leaps from the originating language to English language media, and spoof e-mails to NATO, as well as governmental or media sources to provoke a reaction designed to add fuel to the controversy.

Russian disinformation has also taken on a more threatening tone (NATO, 2020b). In March of 2020, Russia offered and deployed aid supporting Italy’s COVID-19 response, building upon a narrative of a responsible global actor reaching out to help Italy in its hour of need after having been abandoned by its NATO allies. Such donation diplomacy was arguably staged as a pure propaganda exercise (Weiss, 2020). Still, it must also be noted that NATO and the EU were slow in responding to Italian requests for aid, thus creating an opportunity to be exploited. As such, the Italian government initially welcomed this assistance as a good-faith gesture. Soon, however, questions were being asked in mainstream Italian media about the usefulness of such aid, initial deployment near a NATO airbase far from the centre of the outbreak and the potential embedding of GRU agents within such support (NATO, 2020b; Braw, 2020). Following a strategy of “the best defence is a good offence”, senior Russian officials condemned the reporting, accusing the Italian media of spreading false news and disinformation (NATO, 2020b). The original author of the critical reporting was threatened on Facebook by the Russian Ministry of Defence Spokesperson, Igor Konashenkov. Soon after the Spokeswoman for the Ministry of Foreign Affairs of the Russian Federation, Maria Zakharova, accused multiple US media outlets of spreading disinformation on Russian COVID mortality rates, threatening action unless the articles were retracted. In the context of these events, NATO leadership reiterated that the fourth estate has a responsibility to check and assess information on behalf of free societies. By taking an open and fact-based approach to disinformation NATO demonstrated its willingness to put itself under a microscope. Action, ultimately, it is hoped, speaks louder than words. Disinformation is a strategic priority within Russia. Such disinformation has two strategic objectives. First, Russia’s return as a great power, with a commensurate return of Russian influence in Eastern Europe and the collapse of NATO as an effective organisation (Ball, 2017). Second, to preserve the Putin regime by protecting it from the contagion of western-oriented revolutions (Ball, 2017). To achieve these objectives, a false narrative is presented where the US is a demonic military-industrial force for global tyranny, EU members are at each other’s throats, Eastern Europe is a hotbed of ethnic tension, NATO is threatening an imminent attack on Mother Russia, Ukraine (with a population approximately 28% of Russia) presents a credible military threat, Alliance democracies have failed to tackle the COVID crisis and western vaccines are dangerous and produced by corrupt manufacturers. This picture is contrasted with a militarily and politically strong Russia, prepared to counter NATO aggression, a friend always willing to lend a hand during a crisis, leading the world in developing COVID-19 vaccines, and providing an effective national response to the situation. Such a Potemkin narrative has real power based on a blend of carefully selected facts, half-truths, cultural bias, outright falsehoods and wish fulfilment. Note that while there is an overarching strategy to use disinformation, there is also an element of opportunism. “Putin is not a “cool genius ... His system is ‘adhocracy,’ in which lackeys do not receive direct instructions but instead rely on hints and guesses to determine what will please the boss” (Galeotti, 2019; Lipman, 2019). Putin is an opportunist without a master plan, but with a commitment to restoring Russian greatness. Russian actions during the COVID-19 crisis are simply the most recent example of this ad hockery.

Beyond the COVID-19 crisis, Russia views disinformation campaigns as a funda- mental aspect of ongoing grey-zone or hybrid warfare. In this world, “truth is nego- tiable ... a popular uprising a fascist coup and ... [support to] a Syrian dictator becomes an anti-terrorist operation” (Ball, 2017). The Russian Chief of the General Staff, Valery Gerasimov, is quoted as saying, “interstate confrontation’s foundation has come to consist of non-military measures including political, economic, and informational ... [Total conflict] has spread to all spheres of activity in modern society, diplomatic, scientific, sport, and cultural and, in fact, has become total in scope” (Ozawa, 2020). This comment contains the echoes of a cold-war long thought confined to history.

#### Only combatting Kremlin-based disinformation solves. Russia operates as a blueprint for other actors---China proves.

Jakub Kalenský 22, Senior Fellow at the Atlantic Council's Digital Forensic Research Lab, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 171-172 (under ch. titled, “Chapter 7: How to Defend Against Covid Related Disinformation,”) //chico

7.4 “It’s Not Just About Russia”

Before diving into specific countermeasures, it is useful to clarify one point. Many of the countermeasures mentioned below are based on the author’s previous work regarding pro-Kremlin disinformation campaigns. While this approach is specific to Kremlin-based disinformation, it is applicable to other actors as Kremlin-based disinformation often serves as a blueprint for other disinformation campaigns and is often amplified by other actors. First, the Kremlin’s disinformation ecosystem is far bigger than commonly perceived. Russia is responsible for roughly two thirds of foreign influence efforts documented globally (Martin et al., 2020). In other words, Russia conducts twice as many information operations against other countries as the rest of the world combined. Moreover, the Kremlin controls an astronomical number of disinformation channels that are not accessible to the majority of other actors. This extends farther than just using “trolls” on social media, but also to thousands of information professionals in the Russian government, including within its embassies all over the world and its very active secret services. Thousands of other professionals affiliated with the state’s “pseudomedia” are also exporting the Kremlin’s disinforma- tion campaigns outside of Russia, including through both witting and unwitting local helpers, like certain NGOs and GONGOs (government-organized non-governmental organizations), extremist politicians (Wesslau, 2016), etc. (Kalenský, 2019a).

Russian disinformation campaigns are also increasingly focused on “information laundering”, which blurs the original source of given information, and instead finds local sources that spread the disinformation for them.6 Many seemingly “domestic” sources, an attribution usually based on nationality alone and which disregards the origin of the disinformation they are spreading, are in fact just multipliers of the Kremlin’s disinformation campaigns, knowingly or not. Such sources may even be highly respected (Kalenský, 2020b; Weiss & Goldsmith, 2021), making the impact all the more powerful. As was recently made public by the US intelligence commu- nity, the Kremlin deliberately targets domestic actors to support their influence and disinformation operations (Barnes, 2021).

This mechanism of information laundering has also been present during the COVID-19 infodemic, wherein Chinese official sources have amplified disinforma- tion narratives originating in Russia, giving them a boost (Semantic Visions, 2020). The possibilities available to the Kremlin, an actor that has launched “the most amazing information warfare blitzkrieg we have ever seen in the history of informa- tion warfare” in 2014 (Vandiver, 2014), and who continues to improve its capabilities regarding their information campaign, as well as the resultant threat of these disin- formation campaigns, are simply incomparable to the mythical “400-pound person sitting on his bed” (Calamur, 2018). Moreover, other actors, in particular, China, are replicating Kremlin tactics to the degree that researchers now discuss the “Rus- sianization” of Chinese information operations (Vilmer & Charon, 2020). There is an ever-increasing level of cooperation between Russian and Chinese state pseudo- media (European Values Center, 2021). The Kremlin is by far the most aggressive, experienced, innovative and emulated disinformation actor in the world right now. The ease and success with which they conduct their campaigns clearly inspires other such adversaries to use similar weapons, even if just on a more limited scale.

### IL---Russia---Ukraine War

#### Counter-disinformation prevents further escalation of the Ukraine invasion.

Todd Helmus 22, senior behavioral scientist at the RAND Corporation, member of the Pardee RAND Graduate School Faculty, 3/14/2022, "Keeping Russians Informed About Ukraine Could Help End This War," No Publication, https://www.rand.org/blog/2022/03/keeping-russians-informed-about-ukraine-could-help.html, RMax

“Light will win over darkness.” President Volodymyr Zelensky of Ukraine spoke these words in his stirring address to the United Nations, and U.S. President Joe Biden cited these same remarks during his State of the Union address in emphasizing U.S. support for Ukraine.

Russian President Vladimir Putin, on the other hand, is placing his bets on darkness. He is shielding his people from what is actually happening in Ukraine, the casualties inflicted by the Ukrainian Army, the mayhem unleashed by Russia on Ukrainian civilian centers, and the West's rationale for inflicting damaging sanctions. Increasing Russian access to this information, however, could be key to undermining Russian support for the war and undermining the political standing of Putin.

Short of an all-out victory against Russian forces by the Ukrainians, it could be essential to galvanize public opposition to the war and impact Putin's decision calculus.

This is in part the goal of U.S. and EU sanctions against the Russian state, which have led the ruble to tumble in value and in turn raised the cost of living for everyday Russian citizens. Russian casualties, reaching an estimated 2,000 for the first five days of war, may also achieve such ends. Casualties and the public grief they inflicted on the mothers of dead soldiers were crucial in ending Soviet involvement in Afghanistan. Russian citizens also have long-standing connections with the Ukrainian people through family ties and shared language and history, and so they may be particularly sympathetic to the high civilian death toll in Ukraine.

Information operations will play a decisive role in this battle. Information operations cannot fabricate a nonexistent reality so much as crystalize a real truth. In this case, information can help the Russian population stay focused on the true cause of sanctions and the true cost of war.

Russia knows this, of course, and has taken steps to protect Russians from such content. It has blocked Russian access to Facebook and Twitter, shut down access to U.S. Radio Free Europe/Radio Liberty's Russian language news broadcasts, and shuttered the independent Russian news service Meduza to name a few. It has also blocked two prominent independent media sites, Echo Moscow and Dozhd, and has passed laws that criminalize the spreading of “fake news” with up to 15 years in prison.

The cracks, however, are apparent. Russian and Ukrainian influencers on TikTok have begun posting content, even if it is quickly removed, that expresses opposition to the war. Anonymous, the hacker group, has successfully motivated fans on Twitter to start posting anti-war themed Google reviews of Russian restaurants and outright internet hacks have defaced Russian government websites with anti-war messages. The Ukrainians have also gotten in the game, creating a Russian language website providing information about Russian casualties and POWs.

The United States, European Union, and NATO, as well as civil society groups, could directly support such efforts—not through the creation of fake social media accounts, the spread of disinformation, or the conveyance of simplistic pro-Western messages—but by supporting the dissemination of accurate news and information about the war and its cost.

First, the United States and others could get out of the way of those in Ukraine and elsewhere who are applying innovative methods to inject information into the Russian market. The Ukrainian information operators are leading the charge with a stunningly successful information campaign, including by speaking natively in Russian. However, there may be helpful ways to provide assistance, possibly by amplifying the message across broadcast channels that can reach Russian audiences. The West should also ensure that Ukrainians retain the capability to disseminate online content.

The West could offer assistance and support to online personalities and influencers who have access to the Russian social media market and reach out to and support Russian diaspora populations residing in the West who are intent on passing information to family and friends in Russia.

They could also explore creative ways to promote Russian access to independent Russian-language media, such as the Latvia-based Medusa, Ukraine-based sites, or Western-funded media such as Radio Free Europe/Radio Liberty.

The West also could help sympathetic Russians gain access to the free internet, possibly through sharing access to virtual private network technologies that can break through the firewalls installed by the Russian government.

Russia has taken increasingly aggressive actions to restrict access of information about the war in Ukraine. The United States and the West could help neutralize this by developing new techniques for ensuring Russian access to accurate and truthful information. Ensuring that the Russian people know the truth about what their government is doing in Ukraine could bring this war to an end soon rather than later. To quote a verse from Ecclesiastes, “Wisdom has an advantage over folly, as the advantage of light over darkness.”

#### NATO is at a tipping point in Russia’s information war against Ukraine support---now is key.

Serge Schmemman 22, Times correspondent and bureau chief in Moscow, Pulitzer Prize recipient, 5/5/2022, "The Information War in Ukraine Is Far From Over: Serge Schmemann," No Publication, https://www-proquest-com.proxy.lib.umich.edu/docview/2659748494?pq-origsite=primo, RMax

If the first casualty of war is truth, then the corollary in Ukraine is that information is the first battlefield.

That was where the war began, in early 2022, weeks before Vladimir Putin sent the first rockets, armored vehicles and troops into Ukraine, when he claimed that the massive buildup of troops along Ukraine’s borders was but another military exercise. And that was where the United States and its allies scored their first victories, when they made public intelligence anticipating the invasion and the pretext Mr. Putin would use for it.

Then, when the invasion began in February, Ukraine’s president, Volodymyr Zelensky, opened a second information front. He donned a soldier’s olive-drab T-shirt and issued a torrent of defiant tweets, speeches and images from devastated villages, much of it targeted at Russian audiences. His metamorphosis from a relatively unpopular president to a David defying Goliath has been instrumental in solidifying popular, military and economic support for Ukraine in the United States and Europe.

In these first information battles, the Americans and Ukrainians showed that they had learned the lessons of 2014, when Russia had the upper hand in propaganda, assaulting Crimea and eastern Ukraine while claiming to be responding to pleas from Russian-speaking residents. The United States and Ukraine have also been greatly aided this time around by the fact that the evidence of the invasion and its brutal consequences has been so well documented.

But the information war, like the physical war, is far from decided. Ten weeks into the war, many Russians seem to accept Mr. Putin’s narrative. Around the world, many countries remain on the sidelines or, like China, are on Russia’s side. While Washington’s public comments have served to bolster the Ukrainians and rally their allies, some of those comments have played directly into Mr. Putin’s claims of a malign America determined to neuter Russia, as when President Biden said of Mr. Putin, “This man cannot remain in power,” and Defense Secretary Lloyd Austin declared that America’s goal is a “weakened” Russia.

Russia was surprisingly slow to prepare its population or the world for a full-scale invasion, perhaps because its leaders were convinced that Kyiv would fall quickly. But after that slow start, the Kremlin went into high gear. Domestically, it shut down independent media outlets, quashed demonstrations and threatened anyone challenging the government line with “false information” about the invasion with up to 15 years in prison.

Russia was also quick to adapt its messaging to a changing battlefield. After Moscow shifted its focus from Kyiv to southeastern Ukraine, the goal of driving Nazis out of power in Kyiv shifted to a focus on Ukraine as an existential struggle for Holy Russia against an American hegemon and its NATO sidekicks. What began as a “special military operation” has morphed into a defensive war akin to World War II, the “Great Patriotic War,” in which Russia was last compelled to defend itself against Nazis and fascists.

“We broke the back of fascism,” declared Patriarch Kirill, the head of the Russian Orthodox Church and a staunch supporter of the war against Ukraine, in a sermon on April 3 that turned an unprovoked invasion into a noble crusade. On May 3 he ratcheted up the language: “We don’t want to fight anyone,” he said in a sermon in the Kremlin. “Russia has never attacked anyone. It is amazing that a great and powerful country never attacked anyone; it only defended its borders.”

How many Russians really believe this is hard to gauge, given the danger of disagreeing. There is considerable anecdotal evidence that the notions of a hostile NATO and treacherous Ukrainians are widely held, but there are also many reports of Russians horrified by the war but no longer able to speak out without immediate repression.

The info war has also reached Asia, Africa and South America, where Russia has mobilized diplomats and state-controlled media like the global RT network to press its case. The goal isn’t necessarily to win support, but to keep unaligned countries on the sidelines. While some countries, most notably China, have taken Russia’s side, others, like India, have avoided antagonizing Russia so as not to lose Russian military or energy contracts.

Many others have done so simply because they know and care little about Ukraine. Russia’s line to them is that it is fighting to prevent the United States from creating a unipolar world that would swallow their country, with no one to support their interests. The strategy evoked memories of the assistance the Soviet Union gave to Vietnam, Angola and other postcolonial independence movements.

The United States has mounted its own diplomatic efforts to gain more support from countries like India and South Africa. And Ukraine recently posted a video on Twitter recently in which the commander of Ukrainian armed forces thanks 37 countries that, according to the tweet, have shown “assistance and unwavering support in these hard times.” The list is not entirely fair — some Asian countries missing from the list have provided nonlethal assistance — but it is still noteworthy that there were no entries from Africa or South America.

As the war rages on, attention in the United States and elsewhere is bound to flag, and questions about the impact of the war on energy and food prices worldwide are bound to intensify. A speech by Mr. Biden on Tuesday on the need to support Ukraine was lost in the brouhaha over the leak of a Supreme Court draft ruling. And the $33 billion he is seeking in military assistance and other aid for Ukraine is certain to meet resistance, especially since there is no idea when or how the war might end.

Dwindling Western commitment is part of Mr. Putin’s calculus. Though he seems to have misjudged the West’s fury and response to his invasion, his 22 years of increasingly autocratic rule have taught him that passions invariably wane and high costs erode commitment.

As a former K.G.B. agent, Mr. Putin sees the world as a battleground of conspiratorial maneuvers. In his speeches, the color revolutions in Ukraine and other former Soviet republics and the Arab Spring and other global upheavals are machinations to bolster American domination. As an heir to the Soviet worldview, he believes more than many Western leaders do in the importance of information warfare, both to give his regime a veneer of legitimacy and to challenge liberal democracy. On this battlefield, lies are ammunition in Mr. Putin’s long and increasingly personal struggle to stay in power.

As the war enters a new phase, as the images and horrors become familiar and the costs rise, it will become ever more difficult for the Biden administration and for Mr. Zelensky to sustain their early lead in the information war. That makes it all the more imperative for the West to press the message that this is not a war Ukraine chose and that the cost of allowing Mr. Putin to have his way in Ukraine would be far higher than the sacrifices required to block him.

#### Russia is winning the Ukraine info war NOT the other way around.

Dr. Jill Goldenziel 22, professor at U.S. Marine Corps University, Affiliated Scholar at the University of Pennsylvania’s Fox Leadership International Program, Ph.D. from Harvard, March 2022, "The Russia-Ukraine Information War Has More Fronts Than You Think," https://www.forbes.com/sites/jillgoldenziel/2022/03/31/the-russia-ukraine-information-war-has-more-fronts-than-you-think/?sh=165dd3faa1e2, RMax

The West has proclaimed Ukraine’s victory in the information war. Memes like the Ghost of Kyiv and the soldiers of Snake Island, impassioned speeches by Ukraine’s President Volodymyr Zelenskyy, horrific images of Russian-wrought destruction, photos of millions of Ukrainians fleeing their homes, and tales of Miss Ukraine laying down her tiara and picking up a machine gun beside millions of her countrymen have captivated the West. No doubt this narrative is partially responsible for the outpouring of Western munitions and military assistance to Ukraine, sanctions against Russia, and aid to displaced Ukrainians. If the objective of Ukraine’s information war was to gain sympathy and assistance from the West, Ukraine has certainly succeeded.

However, the information war has more than just a Western front. While the West dismisses Russian narratives, other influential actors are listening and embracing them. Russia’s narrative is carrying sway in the developing world and in China – and some of its disinformation is being parroted by conspiracy theorists within the U.S. Russia’s war disinformation will have consequences for international relations long after the war. The West must act to counter it.

The Global South has been reluctant to condemn Russia for the war and to counter its disinformation. Forty countries did not support the UN General Assembly’s extraordinary resolution condemning the Russia invasion of Ukraine. Belarus, Eritrea, North Korea, and Syria chose to stand with Russia. The 35 abstentions unsurprisingly included China and Iran, but also included India, Iran, Iraq, Pakistan, South Africa, South Sudan, and Vietnam—states which the U.S. has supported or had partnerships, or warmed relations with in recent years. The U.S. has been dismayed by many African states’ refusal to condemn the conflict, causing a strain in their relationships. A total of 17 African nations abstained on the UN General Assembly vote, and eight were absent. Of the 28 African states that supported the resolution, none elaborated on their position, with the notable exception of an impassioned anti-colonialist speech by the Kenyan ambassador. South Africa’s President, Cyrial Ramaphosa, has continued to parrot the Russian official position that it perceived a “national existential threat” from NATO and has criticized NATO’s rumored expansion into Ukraine. Correspondingly, a social media analysis conducted in mid-March by the firm CASM Technology has found that pro-Russian narratives are trending in language groups found in much of South Asia, South Africa, Nigeria, Pakistan, and Iran. Putin appears to be targeting these countries with his message to gain influence there. Based on their leaders’ positions, it appears to be working.

China, which more tightly controls its Internet than any other country in the world, has relentlessly promoted Moscow’s narrative. While China may be officially ambiguous about its support for Putin’s war, its state-controlled media lays its position bare. China and Russia resolved to strengthen their cooperation in media in 2015, and the war has shown the success of this initiative. Within hours of the invasion on February 24, the Chinese Communist Party’s Global Times posted a video saying that a large number of Ukrainian soldiers had surrendered, citing the Russian state-controlled media network RT. China’s state Central Television Station (CCTV) then promptly reported and spread on social media that Zelenskyy had fled Kyiv. Chinese media has repeated Russia’s positions that the war opposes the West, NATO expansion, Nazisim, and fascism, and is therefore justified. Meanwhile, it has reported that Ukraine is using civilians as human shields and torturing captured soldiers. Perhaps most dangerously for the U.S., Chinese government officials has spread Russia’s claims that the Pentagon was financing biological weapons in Ukraine. Chinese government officials repeated the conspiracy theory at news conferences, in the press, and on official social media accounts—in Chinese, Arabic and English. The White House called out both countries for their coordinated disinformation campaign and expressed concern that they might be providing cover for a Russian biological or chemical weapons attack. Conspiracy theorists within the U.S. have picked up on the lab disinformation and begun to spin it for their own propaganda campaigns, including Fox News host Tucker Carlson and QAnon followers. Journalist and national security critic Glenn Greenwald has opined that the theory might be true.

Ukraine has achieved important strategic and military objectives through its information campaigns, and has rightly convinced most of the world of the morality of its cause. However, is has lost some important information battles. Russia has won important information battles in China, India, and most of Africa. And since the information war will go on long after the shooting stops, Russia’s victories have ramifications for international relations going forward. States who continue to buy into the Russian narrative may continue to have strained relationships with the U.S. and the West. As the U.S. and its NATO allies strive to develop stronger relationships with resource-rich African states—in no small part so they can reduce resource dependence on Russia and China, they may find that they are not trusted as political and business partners. The Russian narrative may also harm the U.S.’s long quest for greater security cooperation with India.

#### Ukraine is a target of information warfare – it’s a “crystal ball” for future problems

Associated Press 6/21/2022 (Associated Press, independent global news organization dedicated to factual reporting, 6-21-2022, "Google Exec Warns U.N. Security Council: Ukraine Is 'A Crystal Ball' For Information Warfare," Time, https://time.com/6189556/google-security-ukraine-information-warfare/, DOA: 6-22-2022//Smarx Ahsan)

UNITED NATIONS — A Google executive warned the U.N. Security Council Tuesday that cyberattacks, disinformation and other forms of information warfare being waged in Ukraine are a “crystal ball” for future problems elsewhere.

“States must find a way to turn the volume down and settle on some kind of deterrence doctrine for the cyber domain,” Jared Cohen said at a council meeting on hate speech, incitement and atrocities in Ukraine.

He argued that while tech companies have needed expertise, “there is no magical algorithm or single fix for this,” and finding a solution will take a lot of experimentation.

Cohen heads Jigsaw, a part of Google that aims to build technology to combat disinformation, censorship and extremism online.

He said Ukraine “has been disproportionately targeted” by advanced cyberattacks since Russia’s annexation of Crimea in 2014, adding: “It is essentially our crystal ball for what is likely to come.”

The war in Ukraine upped pressure on tech companies to work harder to combat hate speech, disinformation and other harmful content online. The European Union is working on sweeping new rules that would require Google, Facebook parent Meta and other tech giants to police their platforms more strictly.

Western powers on the Security Council have accused Russia of a campaign of propaganda, disinformation and hate directed at undermining Ukraine. A recent report from Mandiant, a cyber security firm, found that Russia used disinformation, fear and propaganda to demoralize Ukraine and divide its allies.

“Hate speech can also be a war crime,” British deputy U.N. Ambassador James Kariuki said Tuesday, calling on Russia to “stop making such statements.”

Russian Ambassador Vassily Nebenzia repeated his country’s counterclaims that Ukrainian authorities’ rhetoric has poisoned citizens against Russia and Russian-speaking populations in Ukraine, with Western encouragement.

“We see, from our side, a real incitement to violence and Russophobia in Ukraine,” he said.

Albania, which currently holds the council’s rotating presidency, called for Tuesday’s meeting.

### IL---Russia---Baltics

#### Russia will use information warfare tactics to justify an invasion of the Baltics - absent information warfare capabilities the attack fails but if not, it quickly escalates because it activates Article 5

Brent M. 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.”

#### Russian invasion of the Baltics causes nuclear war

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?

### IL---Russia---Expansionism

#### Russian disinformation enables enlargement

Marco Marsili 21, research specialist at the Centro de Investigação do Instituto de Estudos Políticos, Ph.D. in History, Security Studies, and Defence, 2021, “The Russian Influence Strategy in Its Contested Neighbourhood,” Russian Federation in Global Knowledge Warfare: Influence Operations in Europe and its Neighbourhood, <https://link.springer.com/book/10.1007/978-3-030-73955-3>, RMaxP

5 Conclusions

Information superiority is considered essential to achieving victory on the physical battlefield in modern war. Information operations, for which it is difficult to attribute responsibility and which are not specifically regulated by international law, fall below the threshold of armed conflict and are convenient to be used to destabilize a government or to try to legitimize a (unlawful) action.

The Kremlin has developed information capabilities, clustered under the umbrella concept of “hybrid warfare”, that make a fundamental contribution to accomplish foreign policy goals. Disinformation, propaganda, and cyber capabilities have been employed in Russian influence campaigns to support a new nationalist ideology. The Russian strategy makes a large use of media outlets to inspire nationalist Russian sentiment and identify loyalists and supporters.

Through flag propaganda operations, the Russian Federation has caused political instability and poisoned bordering countries with the purpose to regain regional dominance and counteract the enlargement of Western powers. It is expected that Moscow will continue to use this strategy that, so far, was successful to weaken neighbouring nations and increase its regional influence.

To be effective the hybrid strategy of Moscow, which makes extensive use of information and psychological operations, requires a combination of favourable circumstances: the presence of ethnic Russian and Russian-speaking population on foreign soil and the border with Russia, that is necessary for military intervention. Without both requirements Moscow’s strategy is ineffective and represents neither a deterrent nor a real threat.

#### Information Warfare allows Russia to manipulate marginalized populations into supporting aggression - it represents a dangerous precedent that will be replicated in other countries

Tomáš Čižik 17, is a director of Centre for European and North Atlantic Affairs (CENAA), a Bratislava based international relations and security policy think-tank. Tomáš holds a PhD in Theory of Politics from Faculty of Political Science and International Relations at the Matej Bel University, May 2017, " Information Warfare - New Security Challenge for Europe.," Center for European and North Atlantic Affairs, [Information\_Warfare\_\_\_cover.pdf](https://d1wqtxts1xzle7.cloudfront.net/52519399/Information_Warfare___cover-libre.pdf?1491519289=&response-content-disposition=attachment%3B+filename%3DInformation_Warfare_New_Security_Challen.pdf&Expires=1655931419&Signature=CmnXGlGzeqNCIa91gHXR2orhJSSEDL9k8iz2cLfyuLuYSP~MSTQnrhSiDz7VgxvDQH5OzOhCxEBtPquzQtgCiG9y2diGeaSli4R~aychG79OZeT5YSKEOVUGKU-dyz7PY2F8CRH9YO7y5nW7ssQqCRbzebxVk5pI8axY7Xtbz60qKa3FTHg2weOa2QVGaMpr-EJuaIPD8Lt6u4IoNTj4S5Wiq16QgdjSqm462aZtAuIN7wJJMgBij4JOInuZNr2rbe-IhCPc4isDJszbmZfFI30tTLTfMFcHi1KGH-SkLB0qLomxi8EABElAvr4OYlQVTfh~iqXhDQ1uPg5BfiX3jA__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA) //AShah

Armed insurgency, Russia's main kinetic HW tool against Ukraine, was instigated and backed by massive information warfare since it's inception. The rebels, who are mostly mobilized, trained, and armed by the Russian special services, and further supported by the Russian armed forces, have been destabilizing Donetsk and Luhansk regions since February 2014. The crisis started to unfold after the pro-Russian former president Yanukovich was forced to flee to Russia as a result of the revolutionary rally in Kiev over his decision to hinder Ukraine's association with the EU. The mass protests in Kiev's Maidan Square, which brought the new pro-European government to power, demonstrated the unequivocal support of the vast majority - 90% according to some polls - of the Western Ukrainians for European integration (IRI, 2014). In response to the undesired change of the government in Ukraine (GoU), Russia launched an aggressive information campaign blaming the government for alleged violations of the rights of the Russian speaking minorities in the country. Using this narrative, predominantly Russian-speaking Crimea was officially annexed by Russia, and Russian special services started to organize separatist outbreaks in Donbas. For these purposes, Russia used the dissatisfaction of the Russian speaking Ukrainians with the new government's attempt to drop the law making Russian the official second language of Ukraine.

Notably, the linguistic divide between the population of the western and eastern regions of Ukraine is reflected in political preferences on the part of the population. According to the opinion polls conducted by the Kiev's International Institute of Sociology, 72.5% of the population of Donetsk region are in favor of integration of Ukraine into the Russian-led Customs Union as opposed to the 9.4% supporting EU integration (Zn. ua, 2014). The regional differences with regard to foreign policy orientation, also stimulated and well exploited by Russian propaganda, can be seen as the main source of the political disagreement between eastern and western Ukraine. As a result of effective information warfare conducted by Russia and the pro-Russian separatists on the ground, they were able to manipulate with the divides among the population against Ukraine's integration into the European and Euro-Atlantic structures by provoking violent conflict in Donbas without even having mass support.

Remarkably, unlike Ukraine, there has never been a significant Russian native speaking or ethnic minority in Georgia. According to the 2002 census published by the European Center for Minority Issues, there is a total of 1.5% Russians living on the territory of Georgia (EUMM, 2014). Therefore, to rationalize the narrative of protecting Russians abroad,' Moscow has since 2002 mass distributed Russian passports in both occupied regions of Georgia. According to various media sources, accepting Russian citizenship was mandatory for permanent residents in the occupied territories and was forcefully executed by local police units. In other words, as opposed to Ukrainian case, where Russia used existing linguistic divides to instigate separatism, in Georgia it created artificial citizens through an illegal “passportization' process in order to justify the 2008 invasion of Georgia. The narrative that was used by Kremlin to justify the aggression after the 5 days war was blaming Georgia for initiating the conflict by using force against Russian citizens in Tskhinvaly region, thus compelling Russia to respond with the “peace enforcement" operation. This analysis is very important to once again underscore that smaller and weaker states failed to deter realization of obvious patterns of Kremlin's HW and counter its strategic narratives, such as the right to protect interests of Russians abroad. As evidenced in both Ukraine and Georgia, Russia is using a new type of Hybrid Warfare to achieve its goals through controlling proxies on the ground supported by the massive information warfare. In both cases Russia, without having solid grounds, succeeded to materialize aggression through engineering new realities, which constitute dangerous precedents that can be repeatedly used against Georgia and other vulnerable countries in future.

### IL---Russia---European Populism

#### Russian disinformation campaigns are relentless and seek to reshape the world order - they exacerbate polarization in the Europe and create distrust of democratic institutions

Conor Cunningham 20, Conor Cunningham is an International Policy Institute Cybersecurity Fellow at the University of Washington whose research focused on Russian Cyber Operations, November 2020, "A Russian Federation Information Warfare Primer," The Henry M Jackson School of International Studies at the University of Washington, https://jsis.washington.edu/news/a-russian-federation-information-warfare-primer/ ; //AShah

The War on Liberal Democracy and Western Dominance

Amid new and continuing global issues and conflicts, Russia wants to remain at the forefront of the creation and implementation of possible solutions. The Kremlin believes the U.S. and its allies are continuously working to isolate Russia and undermine Russian interests. These sentiments are perfectly stated in the National Security Strategy of the Russian Federation:

“The strengthening of Russia is taking place against a backdrop of new threats to national security that are of a multifarious and interconnected nature. The Russian Federation’s implementation of an independent foreign and domestic policy is giving rise to opposition from the U.S. and its allies, who are seeking to retain their dominance in world affairs. The policy of containing Russia that they are implementing envisions the exertion of political, economic, military, and informational pressure on it.[21]“

Russia’s policy not only communicates a responsibility to protect its citizens and Russian culture, but also to combat the U.S.-led unipolar system and persuade others to do the same.

In practice, Russia uses this strategy to justify its operations abroad. As an opponent of the U.S.-centric order, Russia paints itself as a sort of hero for those who are frustrated with the U.S.-led unipolar system. The U.S. Senate 2018 report on Russia’s actions outlines the real objectives and asymmetric cyber tactics of Putin’s regime. It argues that the regime’s overarching goal is the protection of its own power and stability through the expansion of Russian hegemony in various sectors.

Analysis of known Russian information operations in Western democracies illuminates three key overarching objectives: to discredit trusted democratic institutions, to divide the Western coalition, and to undermine the supranational organizations that uphold and promote these democratic values.[22] Following a short stint with democracy in the 1990’s that coincided with national embarrassment, soaring levels of poverty, widespread corruption, war, and instability; Putin has rebuilt the country without a vision of democracy. Modern Russia provides a model for an alternative form of governance, one that is focused on information sovereignty, and promotes traditionalism, nationalism, and authoritarianism. Western ideals and democratic values naturally run contrary to Putin’s own more autocratic vision. The current international order, upheld by the U.S. and its allies, is critical of modern Russia and united, hinders Putin’s ability to implement his agenda at home and abroad.[23] For this reason, the current international order is a constant hindrance and security threat to Putin’s form of government. In addition, Russia’s history of invasion from Western Europe motivates its distrust of the west and of NATO’s effect on global politics.[24]

In most Western democracies, racism and fears about immigration create fertile ground for manipulation. These fears have been targeted by Russian information campaigns to sway the outcome of elections.[25] European democracies and the U.S. face all forms of information warfare and free and fair elections are consistently targeted. Russia hopes to radicalize the populace in these countries, creating not only instability and polarization, but also weak governments. Large supranational blocks such as the EU can have a drastic impact on Russia’s economy by implementing sanctions and forming a collective front against potential military action. For this reason, a large part of Russia’s overarching international policy is focused on disrupting the unity between Western democracies.[26]

#### Polarization in Europe creates fertile grounds for the proliferation of populist attitudes

Victor Ginsburgh 21, Victor Ginsburgh has a PHD in economics from the Free University of Brussels. He has been an Economics professor at Université Libre de Bruxelles since 1975, Sergio Perelman obtained his first degree in Economics at the University of Buenos Aires and a PhD. in Economics at the University of Liège, Belgium, where he is Professor of Economics since 1991, Pierre Pestieau is a Belgian economist. He received his B.A and M.A degrees in economics from the University of Louvain and then his PhD from Yale University, August 2021, "Populism and Social Polarization in European Democracies," CESifo Economic Studies, https://academic.oup.com/cesifo/article/67/4/371/6346855?login=true ; //AShah

Our aim was to explain populist attitudes (that may eventually lead to populist votes) by a number of factors, the most important being the degree of social polarization, which measures the extent of social divides that plague our societies. Polarization is significantly positively correlated with all four populist attitudes, particularly when immigration inflows are treated as an endogenous variable and the model is estimated using IV-2SLS. To the best of our knowledge, this is the first attempt to correlate populism using such indicators of polarization that reflect the socioeconomic divides better than standard measures of inequality or poverty.

To compute our measure of social polarization, in each country we fractionalize population into three groups, low, middle and high income. The distances between the income groups are the ratios of people experiencing either difficulties ‘to make ends meet,’ or ‘material deprivation’.

We show that social polarization varies dramatically across European regions. The highest scores are found in Southern and Eastern countries and the lowest scores in Northern countries, but at the same time, some convergence is observed. Our estimations confirm, in most cases, a positive and statistically significant relation between social polarization and populist attitudes.

Furthermore, our results confirm the effect of immigration inflows on populist attitudes. The only exception, unexpectedly, is the effect of immigration on anti-immigration values. We find however a positive and statistically significant relation when testing our model for the younger European age-cohorts.

Summing up, social polarization appears as a key determinant of populist attitudes among Europeans, but there is also an anti-immigration effect. These results may appear to contradict the view that economic factors only account for a limited portion in individuals’ populist attitudes and votes (Margalit 2019).22 We think that this is not the case in our study. Social polarization must not be considered as an economic variable per se, but also as a measure of potential tensions and conflicts within the society. As such, it drives populist attitudes and values like distrust of institutions, distrust of others, anti-immigration, and authoritarianism.

### Impact---Conventional Deterrence

#### Conventional deterrence prevents nuclear war.

John Mearsheimer 18, Professor of Political Science at the University of Chicago, Ph.D. in government from Cornell University; interviewed by Robert Haffa, interviewer for Strategic Studies Quarterly, Winter 2018, “The Future of Conventional Deterrence: Strategies for Great Power Competition,” *Strategic Studies Quarterly*, Vol. 12, No. 4, link.gale.com/apps/doc/A580345007/AONE?u=umuser&sid=bookmark-AONE&xid=b5a5d678, RMax

SSQ: Your book Conventional Deterrence was published in 1984. What is your definition of conventional deterrence?

JJM: Conventional deterrence is all about persuading an adversary not to initiate a war because the expected costs and risks outweigh the anticipated benefits. When I wrote Conventional Deterrence, I was specifically interested in examining situations where two large armies face each other and at least one of them is thinking about attacking the other.

Throughout the first three decades of the Cold War, virtually all the literature on deterrence dealt with nuclear deterrence. Hardly any attention was paid to conventional deterrence. Indeed, I think I am the first person to ever write an article or book dealing explicitly with conventional deterrence. My goal, of course, was to think systematically about how deterrence works when there is a possibility of a major conventional war, but nuclear weapons are not part of the equation.

SSQ: Early in the book you discuss how conventional deterrence is obtained and state, "Conventional deterrence is largely a function of military strategy" (p. 63). Later on you write, "Military calculations will not always deter decision-makers" (p. 209). Can you explain this difference?

JJM: As Clausewitz makes clear, war is an extension of politics by other means. In other words, states invariably go to war in pursuit of specific political goals. The intensity of the political forces pushing a state to countenance war varies from case to case, but sometimes they are especially powerful. States also pay careful attention to purely military considerations. They want to know what is going to happen when the fighting starts and what they are likely to achieve at the end of the conflict. They also want to know how much risk is involved in pursuing their chosen military strategy. Sometimes states will assess that the likelihood of military success is very low, but still go to war, because political calculations dictate that it is worth taking the risk. The two classic cases of this kind of logic at work are the Japanese attack against the United States in December 1941 and the Egyptian attack against Israel in October 1973.

SSQ: On p. 16 you state, "Since WWII, the nature of conventional war has not changed and there is no reason to expect a change." Does the idea of war being characterized by clashing mass armies remain true?

JJM: The only reason to rule out the possibility of clashing mass armies is the presence of nuclear weapons. While there is no question that nuclear weapons reduce the possibility of a large-scale conventional war between two nuclear-armed states, there is still a real possibility that such a war might happen. This possibility was a matter of great concern on the central front in Europe during the Cold War, and it is a concern today on the Korean peninsula and on the border between India and Pakistan.

SSQ: How does military reluctance to engage in conflict affect political decisions concerning conventional deterrence?

JJM: There are some cases where political leaders want to go to war, but their country's military leaders resist, mainly because they are not confident they can achieve their goals on the battlefield. In those cases, deterrence is likely to hold. This logic explains why the German generals initially prevented Hitler from attacking France soon after Poland fell in September 1939.

SSQ: A quote from p. 211 says, "Although a limited aims strategy is hardly ever an attractive option, it is usually not so unattractive that deterrence obtains in a crisis." Are nations doomed to continue with limited aims strategies?

JJM: Limited aims strategies are not attractive, because limited wars tend to escalate in the modern world. Limited wars usually turn into unlimited wars. Nevertheless, there are sometimes circumstances where the political imperative for war is so powerful that states will pursue a limited aims strategy anyway. This logic explains why the Egyptians pursued a limited aims strategy when they attacked Israel in October 1973.

SSQ: Have determinants of the success of conventional deterrence changed?

JJM: I think the basic determinants remain unchanged. One could argue, however, that conventional deterrence between China and the United States largely involves air and naval forces, whereas conventional deterrence during the Cold War was more about the clashing of large armies supported by tactical air power. My book, of course, focused mainly on the latter scenario, and thus one could say we need to think more about the former scenario.

SSQ: Is your definition of deterrence the same for nuclear and conventional, and how is conventional deterrence complicated by nuclear weapons?

JJM: The definition for conventional and nuclear deterrence is the same if you are talking about the overarching relationship between military and political calculations and how they interact to affect deterrence. But the military calculations are different in those two realms. For example, it is difficult to see how a military can employ nuclear weapons on the battlefield to achieve meaningful success. That is certainly not the case, however, with conventional weapons. Furthermore, inflicting --or threatening to inflict--immediate and massive punishment on the other side's civilian population is of central importance in the world of nuclear deterrence. It is not an important consideration in the conventional realm, which is not to deny that civilians sometime end up suffering greatly in conventional wars. But it rarely happens immediately and it is not the equivalent of being vaporized, which is a serious possibility in a nuclear war.

SSQ: Is it possible today to achieve strategic surprise?

JJM: I think it is more difficult to achieve strategic surprise today than it was when I wrote about conventional deterrence in the 1980s. The main reason is that the ability of countries to penetrate each other's various communications networks has markedly improved in recent decades. Still, one does not want to underestimate how clever states bent on achieving surprise can be, or how obtuse potential victims can be sometimes.

SSQ: Is the concept of conventional deterrence still relevant given terrorist adversaries, and how does regime type relate to conventional deterrence?

JJM: Terrorism is a minor factor in international politics, and it has little to do with conventional deterrence. Regime type has hardly any effect on conventional deterrence. The underlying logic applies equally to democracies and authoritarian states.

SSQ: How have technological improvements such as precision-guided munitions (PGM), stealth, and missile defense affected conventional deterrence?

JJM: PGMs and missile defense were around when I first started writing about conventional deterrence. Indeed, the first article I ever published was on PGMs and how they affect conventional war. When it comes to weaponry, militaries operate in a very dynamic environment, and the particular constellation of weapons that states have at their disposal at any particular point in time affects the military calculations that underpin deterrence in important ways. What is crucial, however, is how militaries employ the different weapons in their arsenals. Doctrine and strategy matter greatly for both deterrence and war fighting. This has always been the case and always will be.

SSQ: How do you see autonomous weapons systems and artificial intelligence affecting conventional deterrence? Positive or negative?

JJM: While I recognize that autonomous weapons and artificial intelligence add a new twist to warfare, I do not see them making conventional deterrence more or less likely to work.

SSQ: Can we apply the concept of conventional deterrence to conflicts in space and cyber?

JJM: Given that it is possible to have a conventional war in space, one could surely apply basic deterrence theory to that realm, although I have never thought much about how one would do that. It is also possible to imagine two sides waging a nonnuclear war that only involved cyberattacks. One could also apply the logic of conventional deterrence to that realm, although again, I have not studied that issue. One can also imagine both space and cyber being bound up with more traditional military forces in a potential conflict situation. It seems likely, for example, that two large armies facing off against each other in a crisis will be heavily dependent on communications networks that are vulnerable to cyberattacks. Does this create a situation where the side that strikes first wins because it effectively paralyzes the other side's armies, thus weakening conventional deterrence? Or does it create a situation where it does not matter who strikes first, because the victim will retain the capability to wreck the attacker's command and control? Thus, there is no difference between first strike and second strike, which strengthens deterrence. I do not know the answers to these questions, but there is no doubt we need good answers, because questions of this sort are of central importance for understanding conventional deterrence in the contemporary world.

# ADV---Information Ecosystem

## IL---Info Ecosystem

### IL---Info Ecosystem

#### Revitalizing the *information ecosystem* is key to prevent miscalculation, sustain competitiveness, and solve serial policy failure.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 modified language indicated in brackets, ¶ indicates start of a new paragraph //chico

¶ The infrastructure for human civilization is undeniably tangible (that is, physical, chemical, and biological), but it is increasingly virtual as well, and the virtual aspects of that infrastructure – the information ecosystem (or, equivalently, environment) – in many ways has become central and often critical to the way people now live all over the world. As Balkin (2012) describes, “it is not an exaggeration to say that modern states are informational states: states that recognize and solve problems of governance by collecting, analyzing, and distributing information.” Consider that nations require good information to allo- cate benefits and social services to the populace; to administer mechanisms for public safety (e.g. law enfor- cement, court systems, fire-fighting); to provide for national security; to gather revenue to support national expenditures; and to engage with other nations in ways that support national interests. Businesses and nonprofit entities in turn are also highly dependent on information. They use it to develop products and services for customers and cli- ents; to understand markets and audiences for their products and services; to inform customers and clients about their products and services; to comply with laws and regulations applicable to their products and ser- vices; and to maintain their accounting and finances. Construction and manufacturing projects entail the coordination of dozens, hundreds, or thousands of par- ties – all of whom must have a justifiable confidence in the information they are sharing and relying upon. ¶ Contextualized, reliable, trustworthy information is as important to the thinking of human beings as clean air is to human breathing. Human beings depend on good information for making informed decisions about politi- cal candidates standing in elections; to know as consu- mers which specific products and services will best serve their needs; for managing their finances; in making health-related decisions about themselves and their loved ones; in learning to perform their jobs more effec- tively or efficiently; and in truly countless other ways. ¶ Nations also engage extensively in information pro- duction. They provide education for young people; sup- port scientific research that undergirds economic growth and prosperity; and collect, curate, and disseminate large- scale statistical data that influence decisions at every level of society. Imagine what life would be like if citizens could not count on the validity and trustworthiness of the informa- tion underlying any of these activities. In some cases, the result would be no more than minor annoyance. In others, however, the result could be life-threatening. Nations could be [devastated], as they could and likely would make bad or at least sub-optimal decisions about war and peace, the economy, law enforcement, housing, food production, energy, and the many other important mat- ters for which governments have some responsibility.

#### Cognitive warfare makes nuclear miscalculation more likely. Competing narratives lock in polarization AND becomes impossible for political leaders to distinguish between real and manufactured threats.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, //chico

Nuclear conflict

On the risks of nuclear conflict, theories and approaches to nuclear deterrence and strategic stability developed prior to the collapse of the Soviet Union in the late 1980’s and early 1990’s rest on the presumption of rationality in national decision makers. In particular, they assume that adversaries are deterred from attacking by a threat of retaliation that would impose costs on the adversary that would outweigh any conceivable benefits that it would gain from an attack (Morgan 2003). Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, com- pares them, and then acts accordingly.

But the psychologically informed understanding of real- world decision making described above was not accepted widely in the scientific literature until approximately the same time as the collapse of the Soviet Union, and the seminal work in such understanding occurred only in the decade previous to that. What a psychologically-informed understanding of real-world decision making tells us is that the rationality assumption at the base of much traditional thinking on deterrence and strategic stability is untenable, given that humans have evolved to rely on intuitive, reflex- ive, heuristic System 1 thinking to make decisions, particu- larly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking (Kahneman 2011). Psychology tells us that – more often than not – the fast, intuitive judgements of System 1 often take precedence over the slower, more analytical thinking of System 2.

The challenges posed by reflexive reliance on System 1 thinking are greatly accentuated by characteristics of today’s information environment. Social media networks in particular are optimally designed to stimulate System 1 thinking – emotional, reflexive, immediate – and they rapidly transmit content among like-minded individuals, creating the ideal conditions for public polarization and divisiveness to occur (Pfeffer, Zorbach, and Carley 2014). Multiple narratives rapidly emerge around complex events; citizens splinter into their own informational universes and are unable to agree on an underlying reality. Political leaders themselves are subject to these conflicting narratives and may even be active and influ- ential participants in one or another of them.

It is thus easy to posit that in this information envir- onment, manipulated information – either artificially constructed or adopted by a strong grassroots base – could be used by interested parties to generate pres- sure on leaders to act. At the same time, leaders them- selves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted informa- tion originating from their constituencies.

#### Combatting misinformation is key. Overwhelming scientific evidence concludes we’re psychologically hard-wired to be susceptible.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, ¶ indicates start of a new paragraph //chico

Research in the fields of cognitive and social psychol- ogy has formalized what Hitler knew intuitively. We now understand that human cognitive processing cap- ability is not unlimited; humans have finite cognitive resources that can be “used up” under mentally stress- ful circumstances. Findings from the same cognitive psychology that has transformed neoclassical econom- ics into behavioral economics (and resulted in three Nobel Prizes in economics) have made clear the “bounded rationality” of human thought and the simul- taneous existence in every individual of the capability to engage in two types of cognitive processing.

Specifically, heuristic dual-system cognitive theory posits that human beings have two systems for cogni- tive processing – an intuitive, reflexive, and emotionally driven mode of thought (often designated as System 1) and a slower, more deliberate, analytical mode of thought (often designated as System 2). Kahneman (2011) provides a primer on System 1 and System 2 thinking. (See Petty and Cacioppo 1986; Chaiken 1987 for other variants of dual-system cognitive theory; see Kruglanski and Thompson 1999 for a contrary view on dual-system cognitive theory.)

System 1 is designed to operate rapidly, but it can do so because it does not take account of all available information and is thus more prone to error (also called bias). System 2 operates more slowly but is more likely to take into account the available information and is less prone to error. People engaging in System 1 infor- mation processing respond more emotionally and less rationally or critically than in System 2 processing.

Most important, System 1 thinking is the default mode of thought for human beings – it uses smaller amounts of cognitive resources, relies on simple gut- based judgments, and is used more often when humans are under stress. For most situations encoun- tered in everyday life, System 1 thinking is adequate and produces mostly valid and useful outcomes, but it often fails when a situation requires complex inferences for understanding. For such situations, System 2 think- ing, which is effortful and consumptive of cognitive resources, is more often appropriate – and when indi- viduals fail to use System 2 when it is appropriate to do so, they are easily misled.

Most individuals are capable of both System 1 and System 2 thinking; thus, the important operative question is the circumstances under which they select one or the other type of thinking. Psychology has accumulated considerable evidence relevant to this question. For example, Taber and Lodge (2006) show that an individual tends to be less critical of information that is favorable to [their] position than of information that is not favorable – that is, [they are] more likely to engage in System 1 thinking for favorable information. People have a confirmation bias in their information seeking and processing behavior – they preferentially seek out information that is consistent with their beliefs and they are highly critical of (or ignore) information that contradicts their beliefs. In a meta-analysis of 91 studies, Hart et al. (2009) considered two motivations for how an individual might select information to consume – the desire to gain an accurate understanding of reality and the desire to feel validated in [their] beliefs. These two motivations conflict when an accurate understanding of reality does not validate one’s beliefs, and such a situation motivates the question of which of these motivations is more powerful. Hart et al. concluded that both motivations drive human information- seeking behavior, thus moderating each other to a certain extent, but that on balance, humans do exhibit a tendency towards the validation of their beliefs. People are also subject to belief perseverance (a.k.a. a continuing influence effect) – a cognitive bias through which individuals do not revise beliefs based on erro- neous information even when they know for sure that such information is erroneous (Lewandowsky et al. 2012).

Maintenance of an individual’s social identity is an important influence on his or her invocation of System 1 or System 2 thinking. Evidence suggests that indivi- duals tend to adopt the views of the peer groups that are most salient to them, even if the “objective” or “factual” information available to them contradicts those views. (Asch 1951 performed the classic “confor- mity experiments” that demonstrated this phenomenon in the early 1950s.) Uncritical System 1 thinking is active in processing information that is consonant with the beliefs and attitudes of those peer groups. Critical and skeptical System 2 thinking is active in processing infor- mation that is dissonant to those groups’ beliefs. These effects (that individuals tend to accept salient group norms) are even more pronounced in an anonymous environment, such as that which characterizes much online interaction (Postmes et al. 2001).

Lastly, there is evidence that emotion and motivation affect cognition. For example, people who are angry tend to rely more heavily on simple heuristic cues (sug- gestive of System 1 thinking) than those who are not angry (Bodenhausen, Sheppard, and Kramer 1994). Individuals are more likely to stereotype people (a form of System 1 thinking) when that stereotype is consistent with their desired impression of those people; conver- sely, when the stereotype is inconsistent with their desired impression, individuals tend to inhibit the use of this stereotype (Kunda and Sinclair 1999). Negative emotions (such as those induced by the receipt of infor- mation incongruent with a person’s prior beliefs) can improve the ability of a person to reason logically, thus enabling [them] to negate or discount that informa- tion (Goel and Vartanian 2011).

In the new information environment, exploitation of human cognitive architecture and capabilities – which are largely unchanged from what existed millennia ago – provides the 21st century information warrior with cyber- enabled capabilities that Hitler, Stalin, Goebbels, and McCarthy could have only imagined. By exploiting cogni- tive limitations, the perpetrators of cyber-enabled infor- mation warfare have learned to exacerbate prejudices, biases, and ideological differences; to add heat but no light to political discourse; and to spread widely believed “alternative facts” in advancing their political positions.

Russian interference in the 2016 US presidential elec- tion has dominated news headlines ever since. But interference by authoritarian countries in the elections of democratic states – as undesirable and threatening as it may be – is hardly the only negative consequence of cyber-enabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed par- ties on all sides share a basic understanding and knowl- edge of the relevant facts. Yes, they may have different values and different priorities, may act under different constraints, and be able to bring to bear different levels of resources to these problems.

But without shared, fact-based understandings of the blast, thermal, and radiation effects of nuclear explosions, what hope is there for national leaders to reach agreements to reduce the threat of nuclear holo- caust or to make good decisions about nuclear weap- ons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in cor- responding increases in global temperature and cli- matic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

### IL---Climate

#### Degradation of the information ecosystem locks in climate denialism. Cyber-enabled tactics exploit cognitive biases.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, ¶ indicates start of a new paragraph //chico

Climate change denialism

Climate change denialism can be fairly characterized as cyber-enabled information warfare against the reality of large-scale anthropogenically-induced climate change. In the responses of people resistant to taking action to miti- gate climate change, we see a number of psychological factors at work (Zaval and Cornwell 2016). For example, one key element of System 1 thinking is the availability heuristic, with which individuals tend to associate the like- lihood of an event with the ease with which they can remember similar events in the past. But the long-term consequences of climate change are unprecedented in recorded human history and obviously people have no personal memories of unprecedented events.

Moreover, climate change is a long-term process whose inexorable progression is easily masked by short-term fluc- tuations in local weather conditions. For example, public concerns about climate changes correlate with local weather conditions (Krosnick et al. 2006). Climate change deniers are also quick to flag for public attention days that are particularly cold as “evidence” that global warming is not occurring and thus, they claim, discrediting theories of climate change. This illustrates a bias known as attribute

substitution, as Kahneman and Frederick (2002) describe, through which individuals substitute salient information (such as the cold temperature today) for information that is more relevant but harder to understand (such as infor- mation about global climate change).

People are also subject to a loss-aversion bias, in which they place greater weight on losses than gains of equal value. In 1992, the United States committed itself to the United Nations Framework Convention on Climate Change, although President George HW Bush also stated that “the American way of life is not up for negotiation” – and in 2018, the United States withdrew from the Paris Agreement (which was based on the convention). The argument? That the United States would have to give up too much if it kept to the agreement.

To close this (merely illustrative) exploration of biases relevant to climate change denialism, the optimism bias suggests that people consider themselves exceptions when considering the likelihood of a negative event occurring. That is, bad things may happen to other peo- ple, but they won’t happen to me, even though I and those other people are similar in important and relevant ways. In a climate context, the bad things may involve sea level rise or heat waves – and the misperception that “others may suffer from such problems but I won’t” diminishes the power of personal concern as a driver for rational decision making.

Connecting the operation of these cognitive biases to the affordances of modern information technologies is not difficult. For example, Roxburgh et al. (2019) demonstrate how the characteristics of specific weather events (e.g. hurricanes or snowstorms) and “short-term socio-political context can play a critical role in deter- mining the lenses through which climate change is viewed.” Note especially the importance of “short-term socio-political context” – precisely the context that social media shapes.

Elsasser and Dunlap (2013) noted the influential role of a variety of newspaper columnists in advancing denialist arguments and thus amplifying these argu- ments to a broad segment of the American public. Fewer in number then, essentially all columnists today (of all political leanings) have a social media presence that they use to publicize their work, and in many instances their online presence is driven in significant part by social media and reach many more readers online than in print. Furthermore, subtleties and nuan- ces in their extended written pieces are likely to be lost when they are represented in social media.

Another important element of climate change denial- ism is the easy accessibility of seemingly-authoritative information that casts doubt on the well-established science of climate change. As reported by The Guardian, a variety of largely secret funding sources distributed $118 million to 102 denialist organizations (Goldenberg 2013). Oreskes and Conway (2011) provide the definitive work on deliberate information campaigns to obscure the scientific truth on a range of issues from smoking to climate change. These denialist organizations have gen- erated a variety of products for public and policy con- sumption (but – unsurprisingly – not many peer-reviewed scientific articles) that are easily accessible to the public, mainstream media outlets, and policy makers. Their pro- ducts are broadly disseminated through social media and easily found through customized search, and they are sought by reporters who seeking to cover “both sides” of a controversy that is intellectually equivalent to a “controversy” about whether the earth is round or flat

### IL---LIO

#### Cyber-enabled disinformation makes extinction inevitable. Fuels polarization that collapses LIO and fuels climate denialism.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, ¶ indicates start of a new paragraph //chico

¶ On the existential threat from cyber-enabled information warfare ¶ Corruption of the information ecosystem has become an existential threat to civilization as we know it because prosperity and advancement depend on a secure information infrastructure and environment that provides human beings with contextualized, reli- able, trustworthy information when and where it is needed. Information is as much a part of human ecol- ogy and the essence of being human as DNA (itself a form of information!) is a part of the evolutionary processes in biological systems. ¶ Today, chaos reigns in much of the information ecosys- tem on which societies depend. In many forums for poli- tical and societal discourse, national leaders shout about fake news, by which they mean information they do not like. These same leaders lie shamelessly, calling their lies truth, or perhaps “truthful hyperbole.” Acting across national boundaries, these leaders and their surrogates exacerbate existing divisions, creating rage and diminishing confidence in elections and democratic insti- tutions. Using unsupported anecdotes and sketchy rheto- ric, denialists undermine well-established science about climate change and other urgent issues. Established insti- tutions of the government, journalism, and education – institutions that have traditionally provided stability – are under attack precisely because they have provided stability.

### IL---Science

#### Cyber-enabled info-war collapses scientific decision-making. Causes extinction.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, //chico

Fearing the end of the enlightenment

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between state- ment A and statement B means that at least one of those statements is false. The truth of a statement about the world is tested by its correspondence to objective reality rather than by how many people believe it; that is, empiri- cal data are influential. Furthermore, statements known to be wrong or false do not affect conclusions or choices between alternative courses of action.

Cyber-enabled information warfare provides the tactics, tools, and procedures – in short, the means – to replace the pillars of logic, truth, and reality with fantasy, rage, and fear. In a world of ubiquitous cyber-enabled information war- fare, communication and information inflame passions rather than informing reason, play to the worst in people’s cognitive architectures rather than the best, and divide rather than unify. Deliberate corruption of the information ecosystem could be seen as an analog of poisoning water supplies that can be done remotely, inexpensively, and anonymously. All of this is just another way of saying that today it is possible to see glimmerings of an anti- Enlightenment that can possibly take root and that would indeed be the end of civilization as we know it.

Adversaries foreign and domestic that make use cyber-enabled information warfare turn our internal cognitive processes and our external institutional and legal processes against us. Under the cover of “fair play” rubrics and the First Amendment, they have turned us against ourselves. Desperately needed are ways of countering the insidious tactics of cyber-enabled infor- mation warfare for ourselves.

How might we proceed? We need action to develop better ways of identifying adversary cyber-enabled infor- mation warfare campaigns in progress; good counter- measures to help human beings resist the use of cyber- enabled information warfare operations targeted against them; and good measures to degrade, disrupt, or expose the adversary’s use of cyber-enabled information warfare operations. All of this is easier said than done, however, as cyber-enabled capabilities for information warfare increase while human cognitive limitations remain the same. Our work is cut out for us. If we fail, the world is at increasing risk of large-scale and long-term societal frac- ture, the end of the Enlightenment, and the start of an informational Dark Age.

### IL---Science Diplomacy

#### AND, disinformation spills over to collapse broader science diplomacy.

Dr. Marga Guai Soler et al 21, molecular biologist and the founder of SciDipGLOBAL, Dr. Mande Horford, associate professor in Chemistry at Hunter College and CUNY-Graduate Center, with scientific appointments at The American Museum of Natural History and Weill Cornell Medicine, Dr. Tolullah Oni is a public health physician and urban epidemiologist, principal of Oni et al. and the founder of UrbanBetter, “Twelve Months of COVID-19: Shaping the Next Era of Science Diplomacy,” AAAS Center for Science Diplomacy, 1/22/21, https://www.sciencediplomacy.org/editorial/2021/twelve-months-covid-19-shaping-next-era-science-diplomacy

COVID-19 is the first global crisis that affects virtually every person on the planet at the same time. The pandemic has been a stress test for the relationship between science and diplomacy,2 triggering a reckoning of how **transnational crises of planetary scale**—infectious diseases, the looming climate crisis, biodiversity collapse—interlink humanity’s destiny. **Despite** **the predictability** of an existential threat of this nature, most **countries were insufficiently prepared**. Their responses exposed a **profound disconnect** between the **scientific and foreign policy** domains and underscore the urgency of **bringing science** from the margins to the **center of global policy.**

While international research collaboration on SARS-CoV-2 thrived and achieved unprecedented breakthroughs at record speed, many **world leaders ignored** **scientific** recommendations and retreated from multilateral coordination, resulting in **fragmented measures** that often **contradicted** those of **neighboring nations**. These governmental **responses manifested the inadequacy** of current international science-policy interface structures **to address** the **challenges** facing humanity and the planet. With effective vaccines now available, the end of the pandemic is in sight, but **vaccine diplomacy** is being revealed as a battle **for international leadership and geopolitical influence**,**4 rather than** the global **cooperation and solidari**ty this moment calls for.

A crucial task before us, as we enter the next phase of the pandemic, is to capture the lessons from this extraordinary chapter in history to prevent crises of such magnitude in the future, and to rebuild adaptive and resilient systems that prevent the next health and environmental disasters. This special issue of Science & Diplomacy examines the science diplomacy dimensions of the pandemic from different regions, stakeholders, and sectors, as they relate to preparedness, management, and recovery. Articles exploring approaches in the Americas, Europe, South Asia, the Arab region, and Africa all coincide on the need to build, restore, or strengthen national, regional, and global science-policy structures. For example, Dalal Najib describes the immense challenges facing Arab countries in the post-COVID recovery and the need for a regional advisory body to better coordinate policy actions.5 Phyllis Kalele and Stanley Maphosa take stock of the COVID-19 response on the African continent, noting that only half of the 54 countries in Africa have national academies of science, and many of those lack the resources and recognition to adequately advise their governments.6

Many were surprised to watch countries with some of the most robust systems and structures of government science advice struggle to contain the virus. Lemay et al. argue that one of the reasons may be the disconnect between domestic and foreign science policy. As governments went into crisis mode, science attaché networks were underutilized.7 Science attachés were forced to pivot away from their regular duties to support repatriation efforts of stranded country nationals or advise colleagues on the import and export of COVID-19 medical technologies. The **logistical disruptions** and reorientation of work **interfered with communication among science attach**és from different countries in the same region, **a missed opportunity for** better **regional coordination** and **optimization** of resources.

Three pieces focus on the role of higher education institutions as engines of global collaboration for pandemic response and recovery. Alice Gast calls for universities to augment their nations’ foreign policy with a synergistic apolitical approach of their own, given their ability to transcend political barriers through academic collaborations that promote transboundary cooperation.8 Lyons et al. suggest creating new science diplomacy mechanisms to fill what they call the “orphan space” at the intersection of academia, government, science, and international engagement.9 Lee et al. show how it is in every high-income country’s national interest to invest in research and capacity development in low- and middle-income countries.10 Similarly, tackling global problems at the local level is how Schneider et al. propose to address the so-called “infodemic” of misinformation that has eroded trust in science and could jeopardize the rollout of the vaccines. By engaging with local communities, and not just disseminating information from centralized institutions, scientists can regain society’s trust.11

Authors note that in most countries, the scientific and diplomatic communities are largely siloed educationally and professionally, with different cultures, values, skill sets, and career paths.12 Here universities can play a key role by formally introducing science diplomacy in STEM and international relations curricula to build the necessary bridges between the two communities.13 A growing number of governments and diplomatic academies are also embedding scientific and technological expertise in the foreign service,14 but academic, legal, administrative, and cultural barriers still impede bidirectional engagement between the scientific and diplomatic spheres in many countries. Governments must foster the demand for science diplomacy by establishing mechanisms such as fellowship programs, pairing schemes, and secondments to immerse scientific experts in foreign ministries and multilateral bodies.

The piece by Sholts et al. on the history and future of the Smithsonian Institution highlights the often neglected colonialist and imperialist roots of historical scientific cooperation episodes driven by the Global North now being reframed as examples of science diplomacy.15 Robert Swap adds that effective science diplomacy is based not only on sharing knowledge, but cultivating cross-cultural and interpersonal skills that build trust over time and address the legacies and currently lived realities of racial, social, and environmental injustice in order to foster more equal international partnerships.16

One baseline challenge noted in several pieces is the unfamiliarity of many stakeholders with science diplomacy as a concept and as a tool. As there is neither a commonly agreed-upon definition nor a consensus on its objectives, actors, instruments, and activities, the term is neither universally embraced nor consistently used.17 Kerri-Ann Jones offers an explanation: science diplomacy is still evolving out of two very well-established fields and is struggling to establish its distinct identity.18 Furthermore, the narrative has come under intense academic scrutiny19 in recent years as a focus on its cooperative logic has led to the neglect of its competitive dimensions, which are increasingly important given that commercially-oriented scientific and technological breakthroughs can give particular nation-states an economic edge over others.

Indeed, rapid advancements in frontier research and innovation can help unify nations toward collective actions to achieve the United Nations’ 2030 agenda, but the convergence of some of these technologies--artificial intelligence, quantum computing, synthetic biology, gene editing or climate-altering technologies--with political and societal issues can generate enormous risks and challenges for democracy and multilateral governance. As these technologies become strategic sovereign assets and critical infrastructure for national security, they can also amplify social inequalities, perpetuate racial and gender biases, and deepen geopolitical divides.20 To remain relevant and fulfill its potential to address global challenges, the institutional architecture of science diplomacy will need to adapt to the scale and speed of the transformations ahead with a whole-of-society approach. Beyond the policy and academic communities, other actors including technological and pharmaceutical companies, international scientific societies, and philanthropic individuals and organizations,21 have played a pivotal role in addressing COVID-19 and will have an influential role in strengthening science diplomacy efforts moving forward.

While COVID-19 discoveries have been the top priority of the global scientific community, let us not forget how issues pertaining to biodiversity loss, climate change, land use, food security, ocean health, and energy have persisted, as noted by Muhammad Adeel and other authors.22 2020 tied for warmest year on record.23 A record-breaking Atlantic hurricane season and the fires ravaging Australia, California, and the Amazon were a reminder of the inextricable links between human and planetary health. As Lemery et al. put it, “the pandemic has served as a palpable admonishment of our custodianship of the commons.”24

We have a once-in-a-generation opportunity to change the trajectory of the interrelated global crises upon us. Several articles in this special issue touch upon the Overton window, a name for the idea that policy proposals that are unthinkable and intractable in one moment (such as universal basic income, emergency policies to house the homeless, and the provision of free internet to support remote learning) can swiftly become not only acceptable, but even inevitable.25 The historic mobilization of resources, public policy measures, and behavioral change during the pandemic can pave the way for more sustained engagement between the scientific and policy spheres for bigger crises, such as climate change. Preventing and responding to the next global crisis will require building creative coalitions among a broader range of actors and placing science, health, climate, and the environment at the heart of the multilateral system. Building (or repairing) the bridges between science and diplomacy will allow us to reframe our relationship with each other and with the planet, as the impact of transboundary threats to health and environment anywhere are felt everywhere. This point is exemplified by the recent legal ruling in France that overturned a deportation order against a man from Bangladesh with severe asthma, as the dangerous air pollution in his country of origin is a threat to his life should he return.26

Perhaps the most salient lesson from the analyses, reflections, and proposals presented in this collection is that science diplomacy starts at home: if nations do not build a strong foundation for science-informed policy, their science diplomacy strategy will not stand on solid ground. That said, given that the pandemic will not be over until outbreaks are under control in the “Majority World” and not just in the Global North, **addressing global challenges** will **require aligning national and global interests** **if we want to ensure** the **benefits** of science diplomacy do not end at home.

Throughout history, pandemics have forced a break with the past and a re-imagining of a new world.27 Opening such a portal to a more just society and sustainable planet needs synchronized unlocking by multiple key holders working in unison towards a common purpose. We hope this special issue inspires you to expand your view of what is possible and necessary to achieve the future we all want.

#### Disinformation erodes public trust in CDC, WHO, and medical and institutional authority writ large. That emboldens anti-science movements and the far-right

Gill and Goolsby 22, Ritu Gill has a PhD in psychology from Carleton university, Rebbeca Goolsby is the co-Lead of a NATO Research Technology Group on cyberdiplomacy and communications, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 7 //chico

Messages such as drink corona beer to get the corona virus, or to prevent it, were sometimes sent for fun. Disinformation in the form of conspiracy theories appear to be sent to recruit new believers, and to reinforce or extend the conspiracy story. Other disinformation appears orchestrated and is part of larger influence campaigns. In some of these cases there are likely to be behind the scene marketers making money by spreading disinformation as has happened in various elections around the world. False images about the size of the re-open protests, disinformation about anti-reopen public proponents, stories about empty hospitals and the like are types of disinfor- mation used to promote social behaviors such as protests, voting, and belief in public institutions. Disinformation about the CDC, WHO, and various medical authorities was used to reduce trust in these public institutions. Disinformation linking different vaccines, social distancing, and facemasks was used to build bridges between diverse groups in attempts to create or strengthen particular movements and political agendas. Such disinformation supported the anti-science movement and a far-right political agenda. Disinformation regarding the actions of governments, police, or leaders such as false descriptions of lock down procedures or their role in promoting a vaccine was used to discredit and so decrease trust in these actors or to bring them undue credit. Some disinformation was aimed at specific minority groups—sometimes to harm and sometimes to keep their voice out of the public debate.

### IL---Vaccines

#### Combatting adversaries solve COVID “truther” sentiments. Russia and China are uniquely responsibly for misinformation.

---Also doubles as combatting China and Russia key warrant

Kathleen Mary Carley 22, Professor of Computer Science, Institute for Software Research at Carnegie Mellon University, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” Advanced Sciences and Technologies for Security Applications, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 13-14 (found under, “Chapter 1: A Political Disinfodemic”) //chico

Although this is a small exploration, it does show a connection among conspiracy theories. It also shows an interesting link to China. In a further examination, we also found that the anti-vax community had more members who followed the state spon- sored media accounts from China and/or Russia. In other words, the anti-vax groups are getting fodder for their conspiracies in part from the disinformation coming from foreign states. We also found that there were more bots among the anti-vaccination community than among the pro-vaccination community. And, the bots on the anti- vaccination side often promoted stories about Bill Gates inventing the virus or 5G towers used to control people.

Prior studies have shown that Russian trolls were instrumental in transforming the pro/anti-vax divide into a partisan divide (Walter et al., 2020). They were also instru- mental in amplifying the debate (Broniatowski et al., 2018). Our results add to this by showing that the divide is not just due to trolls; but that bots, and regular users are also transforming the nature of the vaccine debate through the use of disinformation. Indeed we find that regular members of the anti-vax group brought in disinformation to the community to foster conspiracies about the effect of vaccinations and the need for them. Conspiracy stories were used to bind individuals into groups and promote vaccine hesitancy. Bots amplified and possibly increased the speed with which this was done by promoting the sane conspiratorial information. Further, we find that links to China, not just to Russia, played a role.

### IL---Grid

#### Information warfare manipulates the behavior of citizens—grid shut down and blackouts

Gururaghav **Raman et al. 2020**, PhD in Computer Engineering and Research Fellow at Future Resilient Systems Programme; Bedoor is an Assistant Professor of Computational Social Science at New York University Abu Dhabi, UAE. She received her PhD in Interdisciplinary Engineering in 2017 from Masdar Institute of Science and Technology, and her MSc in Computer Science from the University of Illinois at Urbana-Champaign; Marcin Waniek is a Post-Doctoral Associate at New York University Abu Dhabi; Talal Rahwan is an Associate Professor of Computer Science at New York University Abu Dhabi, UAE. He received his Ph.D. in Computer Science in 2007 from The University of Southampton, UK, where he received the Dean’s Award for Early Career Researcher; Jimmy Chih-Hsien Peng received the B.E. and Ph.D. degrees in electrical and computer engineering from The University of Auckland, Auckland, New Zealand, in 2008 and 2012, respectively. He is currently an Assistant Professor in electrical and computer engineering with the National University of Singapore, Singapore.; “How weaponizing disinformation can bring down a city's power grid”, Aug 2020//SK

Social media has dramatically altered the ways in which conflicts are fought. By allowing belligerents to command the public narrative, these technologies have created a paradigm wherein the most viral information can influence the outcome of wars [1]. This phenomenon has been exacerbated by social media algorithms that value virality over veracity [2,3]. Unsurprisingly, many notable skirmishes in recent years have used disinformation to manipulate peoples' behavior [1,4]. Such campaigns have become particularly effective due to the ever-increasing prevalence of big data and machine learning techniques that allow the behavioral patterns of the masses to be analyzed with unprecedented precision. Among the clearest manifestations of such campaigns are the alleged Russian interference into the 2016 US presidential election and the Brexit referendum [5,6]. These incidents suggest that the microtargeting capabilities provided by companies such as Cambridge Analytica [7] can be weaponized [8] to influence the long-term decisions of a society. While many studies have analyzed campaigns targeting long-term social behavior manipulation [2,9-12], little attention has been given to targeted attacks that use disinformation as a weapon to manipulate social behavior within a limited time span.

One particularly sensitive target that is vulnerable to behavioral manipulation is critical infrastructure, the attack of which may have drastic implications nationwide. For instance, despite high levels of security, human operators proved to be the weakest link during the Stuxnet attack on the Iranian nuclear program, unwittingly introducing malware into the facilities [13,14]. Another attack of this kind that drew concern from governments worldwide was the Ukrainian power grid cyberattack of 2015 [15,16]. In this incident, attackers deliberately cut off the power supply for 230,000 residents for several hours using operator credentials harvested through one particular form of disinformation, namely, spear-phishing [17].

In this study, we focus on the power grid-a choice motivated by the devastation caused by historical power outages including human casualties and massive financial losses [18-20]. Yet, while numerous blackout prevention and mitigation strategies have been proposed in the literature [21-32], the link between disinformation and blackouts has never been studied to date. Driven by this observation, we seek to answer the following question: can an adversary bring down a city's power grid using disinformation without any physical or cyber intrusions? The main contribution of this analysis is to assess whether an adversary could attack the power distribution system not by targeting its hardware or software infrastructure, but by focusing entirely on manipulating individual consumers' behavior.

The rest of the paper is organized as follows. We begin by describing the mechanism of a disinformation attack on the power grid, and then evaluate the impact of such an attack considering the distribution network of the Greater London area as a case study. Subsequently, to quantify the risk posed by disinformation attacks, we perform analyses to estimate what disinformation follow-through rates could be achieved by an adversary in reality. We conclude by highlighting the implications of our study.

Attack impact on the power grid

We consider an attack in which an adversary attempts to manipulate the behavior of citizens by sending fake discount notifications encouraging them to shift their energy consumption into the peak-demand period. Such a shift may result in the tripping of overloaded power lines, leading to blackouts (see Methods). An overview of this attack and the disinformation message are shown in Fig 1. Ultimately, the success of such an attack depends on the follow-through rate , i.e., the fraction of people who behave as intended by the attacker. We analyze the impact caused by such behavioral manipulation on the power grid. To this end, we modeled the power grid of Greater London (see S1 Note in S1 File) and simulated the behavior of residential energy consumers. Importantly, our model considers residential electric vehicle (EV) adoption since the owners of such EVs control a substantial amount of deferrable energy, and thus can cause greater harm when manipulated by an adversary. We vary the EV adoption level in the city, and model the capacity upgrades that are necessary for the grid to support the demand corresponding to each such level [33-35]; see Methods. Note that although the EV charging demand is only one component of the total deferrable demand, it nevertheless accounts for a significant part of the latter. Therefore, in the following analysis, we use increasing EV adop-tion level as a synecdoche for the increasing amount of deferrable demand in the grid.

Fig 1. An overview of a disinformation attack on the power system. Illustrating how the disinformation attack is launched from an attacker, thereby altering the energy consumption patterns of a portion of the population. Importantly, not every recipient follows-through on the notification. [see PDF for image]

We consider a scenario where the grid is heavily loaded and any distribution line can sustain at a maximum a 10% increase in the peak demand through it (see Methods). Fig 2a presents the percentage of consumers who experience a blackout given varying follow-through and EV adoption rates. As can be seen, increasing the EV adoption up to 20% increases the system vulnerability to the attack, whereas beyond 20% the system resilience increases, i.e., it requires a greater follow-through rate to achieve the same attack magnitude. This trend is caused by two opposing forces: (i) increased vulnerability due to the consumers controlling more deferrable energy, and (ii) increased resilience due to the grid's upgraded capacity to cope with the increased number of EVs. When the EV adoption is smaller than or equal to 20%, the former force outweighs the latter, and hence we see an increase in the system vulnerability. The opposite is true when the EV adoption exceeds 20%, leading to the observed increase in resilience. Next, to get a sense of the distribution of the blackout across the city, we depict the state of the system corresponding to two different cells in the heat map; see Fig 2b and 2c. As can be observed, the impact is dispersed throughout the city rather than being concentrated in very few massive pockets.

Fig 2. Impact of an attack on the power distribution network of Greater London. a: The percentage of consumers suffering from a blackout as a result of the attack given different follow-through rates and EV adoption rates. The figure also highlights the columns corresponding to projected EV adoption rates for the UK in the years 2020, 2030, 2040, and 2050. b: Visualization of the status of every power distribution line in the system for a follow-through and EV adoption rates of 0.17 and 0.20, respectively. Grey indicates active lines, whereas red indicates lines that have tripped as a result of overloading. c: The same as (b), but for follow-through and EV adoption rates of 0.12 and 0.20, respectively. [see PDF for image]

We then study how the grid's vulnerability depends on the peak overloading capacity of the distribution lines. Say the overloading capacity is increased from 10% to 15%. Simulating the system for follow-through and EV adoption rates of 0.17 and 0.20 respectively, we find that the attack results in only 5.9% of consumers being offline. This is in contrast to 35.4% of consumers that were affected by the blackout when the line capacity was 10% (see Fig 2b). Further increasing the overloading capacity to 20% reduces the size of the blackout to 1.4% of the consumers. The heat maps corresponding to these scenarios are presented in S2 Note in S1 File. To obtain more insight, we analyze the grid in terms of the line capacity upgrades that are necessary to support increasing EV adoption. The results shown thus far are for the case where, for any given EV adoption rate, the grid is assumed to be upgraded to support exactly that rate. However, if the grid is upgraded to support more than this rate, the impact of the attack will be substantially alleviated, and vice versa. Taking the year 2025 as an example, if by then the grid was not upgraded since 2020, then a mere 5% follow-through rate can bring the grid down completely. On the other hand, if the grid in 2025 was upgraded to support the projected EV adoption until 2030, then even a 100% follow-through rate would cause a blackout for less than 20% of the residents. These results highlight the need for future grid upgrades to not only be dictated by the technical aspects governed by physical laws, but also consider the behavioral aspects of the consumers who may act unpredictably and irrationally, especially when subjected to disinformation. However, since grid upgrades come at a high cost to the power utility [35], perhaps a more realistic solution would be to focus on increasing the awareness of the consumers and immunizing them against disinformation.

Estimating disinformation follow-through

Having assessed how the power grid is affected by the consumers who follow-through on the fake notification, we now estimate what follow-through rates could be achieved by an attacker in reality. Here, the social aspect could play an important role, since people may unknowingly amplify the attack by forwarding the disinformation notification to their friends; see Fig 3a for an illustration. (Note that the term "friend" is borrowed from the context of social media to refer to any "acquaintance".) In this context, Goel et al. [36] analyzed a billion diffusion events, and found that (dis)information is unlikely to become viral through social media, since the vast majority of the studied events terminated either right after the initial broadcast itself, or after a single step of propagation through social media. As such, assuming that the attack considered here has similar limitations, our analysis considers only a single step of propagation, whereby the initial recipients of the notification consider forwarding it to some of their friends.

### IL---Russia Key

#### No alt causes. Russia’s diverse array of tactics magnifies the internal link.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 //chico

At the same time, advances in information technology have a dark side. The same increases in the volume and velocity of information have created a louder and more chaotic information environment that stimulates fast, angry, reflexive, intuitive, and visceral thinking, reaction, and action in people and thus displaces more complex, reflective, and rational thought. In a chaotic environment of information overload, people are more likely to use mental shortcuts as a way to reduce the cognitive bur- den that such an environment places on their thinking.

In recent years, we have seen how the Internet, social media, and mobile devices (and other technologies) can be used by foreign adversaries to interfere in elections and to disrupt the democratic process. We have seen:

* Social media exploitation of cognitive biases to increase their impact and reach – short messages of 280 characters and emotionally evocative video/ audio clips are nearly ubiquitous and much more the norm than they ever were two decades ago.

Disintermediation of established information sources that reduces the role and influence of those pre- viously responsible for providing factual information and proliferates information sources. The US Supreme Court noted in Associated Press v. US (1945) that “the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public, that a free press is a condition of a free society.” Today, modern information technol- ogy has enabled the creation of a larger number of information sources than the 1945 US Supreme Court could possibly have imagined.

* Search engines that return highly visible results for queries based in large part on the popularity of those results and the inferred desires of the user for specific information rather than their actual importance to those queries. Such functionality also makes it easier than ever for people to find information online “by doing their own research,” thus indulging in their confirmation biases by selectively finding and attend- ing only to information that confirms one’s beliefs. Search engine optimization techniques enable gam- ing of search algorithms to promote the visibility of false, misleading, or worthless information.
* Many-to-many connectivity that enables the for- mation of echo chambers and media bubbles that reinforce pre-existing beliefs.
* Large-scale data mining that allows adversaries to sift huge amounts of personal data on individuals to identify and target those most susceptible to customized, inflammatory, false, malign, or mis- leading messages – and also to keep such mes- sages away from public view.
* Near-immediate data transfer, which enables pro- paganda and other malign information to spread far and wide quickly, while efforts to correct false information are more expensive, often fall short, and frequently fail altogether.
* Inauthentic voices that are largely indistinguishable from authentic ones. Macedonian entrepreneurs dis- covered ways to monetize an affinity of Trump voters for fake news (Subramanian 2017). Paid human employees of the Internet Research Agency created and spread false information on behalf of the Russian government prior to the 2016 U.S. election (MacFarquhar 2018). And automated “bots”–accounts purportedly associated with human users but in fact managed entirely or mostly by machines – add further chaos to the information environment.

Is this state of information affairs really new? Haven’t adversaries of all stripes always employed propaganda and lies – otherwise known as information warfare (or at least a big part of it) – to advance their interests?

Yes. Information warfare indeed has a long pedigree that reaches into the past for at least the three millen- nia since the Trojan Horse enabled Greek warriors to breach the walls around the city of Troy. Much more recently, the rise of the Nazi regime in Germany relied on propaganda. As Hitler (1925, 155–56) wrote:

[I]ts purpose must be ... to attract the attention of the masses and not by any means to dispense individual instructions to those who already have an educated opi- nion on things or who wish to form such an opinion on grounds of objective study – because that is not the pur- pose of propaganda, it must appeal to the feelings of the public rather than to their reasoning powers. . . . The art of propaganda consists precisely in being able to awaken the imagination of the public through an appeal to their feel- ings, in finding the appropriate psychological form that will arrest the attention and appeal to the hearts of the national masses. ... The receptive powers of the masses are very restricted, and their understanding is feeble.

But more so today than at any earlier point in human history, human beings are vulnerable to information war- fare. At the same time that new information technologies have led to an increase in the volume and velocity of information available on Earth by many orders of magni- tude in the past few decades, the cognitive architecture of the human mind is more or less unchanged on the time scale of centuries or even millennia.

## IL---Truth Decay

### IL---Truth Decay

#### NATO interconnectedness is the problem *and* the solution--- a system wide approach to combat disinformation is key to solving truth decay.

Kathleen J. McInnis 21, senior fellow with the Scowcroft Center for Strategy and Security's Transatlantic Security Initiative; Clementine G. Starling is the deputy director of Forward Defense and resident fellow of the Transatlantic Security Initiative at the Atlantic Council, “The Case for a Comprehensive Approach 2.0: How NATO Can Combat Chinese and Russian Political Warfare,” <https://www.atlanticcouncil.org/wp-content/uploads/2021/06/NATO-Comprehensive-Approach-Report-2021_final.pdf>, cy

Beyond these US, UK, and Finnish examples, comprehensive approaches to political warfare among NATO members and partners are less prominent. Perhaps in part owing to bureaucratic stovepiping and policymaking preferences, many capitals of NATO member states that are targets of these campaigns tend to view each of Moscow and Beijing’s actions discretely rather than as constituent parts of a holistic strategy. Failure to consider these activities and their implications holistically—and, therefore, failing to address their respective behaviors in a likewise holistic manner— risks the United States and its allies taking actions that achieve short-term successes at the expense of longer-term gains. Progress on areas like the EU-China Comprehensive Agreement on Investment (CAI), for example, which seeks to replace bilateral trade agreements between EU members and China with a common EU-wide investment framework, can present longer-term strategic risks to European states, including increased vulnerability to Chinese economic coercion and influence campaigns—not to mention heightened tensions in the transatlantic relationship due to increasingly divergent strategic approaches to China.47 In other words, a strategic-level approach between NATO, its member states and partners, the private sector, and like-minded multilateral organizations like the EU is needed, as is a framework to turn strategic consensus into concrete action. Fortunately, both by treaty and by recent operational practice, NATO is well positioned to serve as a bedrock for both. The Alliance can, therefore, usefully serve as a catalyst for developing a Comprehensive Approach to combat coercion and political warfare.

Article 2 and the Art of the Political: NATO’s Strategic Role in Countering Political Warfare

NATO stepping up to take on a larger role in countering political warfare has its trade-offs, and some might reasonably express concern about the knock-on effect that such an approach might have on the conduct of military affairs. Some concerns may include: first, if NATO is predominantly a military alliance, then it doesn’t have a significant role to play in countering political warfare, which is the realm of politicians, statesmen, home departments, departments of commerce, and so on. Second, to assign political warfare as a supporting task to militaries, and military institutions like NATO, would likely dilute their focus on their essential defense functions (which are hard enough to perform on the best of days). It might also lessen the pressure on NATO allies and partners to effectively share the costs of hard defense. In the minds of critics, adding political warfare to the growing list of NATO’s tasks means diminishing Alliance effectiveness.

These arguments—however well-intentioned—are unhelpfully divorced from both NATO’s history and current realities. NATO is, and always has been, a political-military alliance in large part because contemporary alliances are themselves an inherently political-military construct.48 To argue for the disaggregation of the military from the economic and political spheres is a conceit, arguably framed by present bureaucratic realities rather than institutional history. The post-World War II order, of which NATO is a part, was designed to be a proactive, forward-looking answer to the security dilemmas and distrust that had previously characterized alliance politics.49 “Despair, disorder, decay from within—these were the likely dangers, not a Soviet invasion.”50 As the USSR’s aggressive intentions became more clear, NATO itself became a solution to enabling European integration and economic revitalization rather than an end in and of itself.51

As NATO was established, reconstituting the economic and political health of its member states was seen as inextricably linked to military strength; military strength was one important pillar of a comprehensive strategy to counter Soviet influence and aggression. 52 NATO’s purpose, therefore, as established in the Washington Treaty, is not only to grapple with military and defense challenges, but also to foster and protect the values core to its mission and that distinguish NATO as an alliance of like-minded nations. This is why NATO not only convenes military leaders and defense ministers at regular defense ministerial meetings,53 but it also hosts foreign ministers at the same regularity54 and heads of state and government roughly once a year at summits or Leaders Meetings.55 Protecting the rights of its members as free and self-determining nations means, in essence, NATO allies have committed to upholding the integrity of the very institutions that are vulnerable to political warfare. This is why Article 2 of the Washington Treaty exists. It reads:

“The Parties will contribute toward the further development of peaceful and friendly international relations by strengthening their free institutions, by bringing about a better understanding of the principles upon which these institutions are founded, and by promoting conditions of stability and well-being. They will seek to eliminate conflict in their international economic policies and will encourage economic collaboration between any or all of them.”56

Article 2 of NATO’s founding charter is sometimes viewed as the “Canadian clause” or a throwaway paragraph in the Washington Treaty.57 Yet negotiators of NATO agreements know that they should never discount a good diplomatic “hook,” especially when it might be used to prompt positive action. Viewed in that light, Article 2 holds enormous utility in supporting and justifying much-needed NATO action on the political warfare challenges allies face on a routine basis. NATO has forgotten how to exercise its political arm to proactively contend with political and economic coercion as effectively as it does its military arm. Article 2 is critical to establishing an effective counter-political warfare response from NATO.

Specifically, in Article 2, allies have pledged to:

■ Shore up free institutions;

■ Establish public understanding of the principles undergirding institutions;

■ Promote stability and well-being; and

■ Eliminate conflict from international economic policies

and promote economic collaboration.

These Article 2 principles are the very areas at risk from Russian and Chinese political warfare today. NATO allies and partners have fallen behind in combatting the political and economic components of political warfare across the spectrum; as a result, NATO should rethink the mandate it already has and reinvigorate Article 2 to help empower and enable a more effective, comprehensive response to future political warfare campaigns.

This leads to the second concern articulated above, namely, that expanding the aperture of NATO’s activities will inherently dilute the Alliance and its military capabilities. This logic perhaps makes sense in the narrower context of burden sharing and defense planning. Yet the military is not an end in and of itself; rather, the object of the military is to be one means toward the promotion of national security and prosperity. Promotion of stability and security—and, therefore, (if indirectly) prosperity—has been interpreted in a variety of manners over the course of NATO’s history: from deterring Soviet aggression to responding to crises in the Balkans and the Middle East to overcoming Franco-German and Greco-Turkish differences. Further, identifying and countering political warfare is largely an intellectual endeavor; organized appropriately, the cost of building a NATO counter-political warfare capability would be miniscule in comparison to the cost of purchasing defense equipment and acquiring capabilities. Given that today the stability, security, and prosperity of NATO allies and partners are being directly challenged by both Russia and China, this marginal investment would likely yield enormous strategic dividends.

Economic and political coercion campaigns have important linkages to national security—linkages that are often difficult for agencies and institutions to fully appreciate on their own. Trade ministries have a different set of priorities than defense ministries, but they both work on matters that have a direct bearing on the security and well-being of their states. A greater cross-pollination of government efforts improves assessments of the threat and development of potential solutions.

Taking Stock: Assessing Existing Alliance and Partner Efforts to Counter Political Warfare

NATO might usefully seek to build shared understandings of, and approaches to, countering authoritarian coercion in two key areas: disinformation and election interference, and coercive diplomacy and economic subversion.58 What follows is an assessment of the current state of play and areas ripe for multi-stakeholder collaboration on these key issues. Current efforts underway by the Alliance and its members tend to focus on discrete areas of political warfare rather than the full gambit. Countering disinformation and cyber defense are the two most advanced areas of the transatlantic response to hybrid warfare, yet NATO allies and partners lack advanced strategies to mitigate coercive diplomacy and predatory economic practices.

Disinformation and Election Interference

Alliance-Wide Efforts

Disinformation is one of the most nefarious challenges NATO faces. False news and the spread of “alternative” facts and narratives creates confusion, foments distrust in democratic institutions and government itself, sharpens societal divisions, and creates negative psychological and emotional responses that can be used to manipulate people’s viewpoints and beliefs. Across Europe, nations come under near-daily attack from state-supported and rogue actor disinformation, from Russian-language campaigns, Chinese propaganda, social media swarms, and online bots. As Russia and China seek to shape the information environment in their favor,59 NATO allies have put various initiatives in place to help combat disinformation and build societal resilience. Allies have pursued different national initiatives and the Alliance has worked to share best practices. It is worth noting that NATO is further advanced in its understanding and response to Russian disinformation than it is of Chinese disinformation which is much less analyzed and understood in a transatlantic context.

#### Russian attacks erode public confidence in institutions.

Justin Pelletier 22, Director of the Cyber Range and Training Center in RIT's Global Cybersecurity Institute, “Russia could unleash disruptive cyberattacks against the US – but efforts to sow confusion and division are more likely,” <https://www-proquest-com.proxy.lib.umich.edu/docview/2623728130?pq-origsite=primo>, cy

As tensions mount between Russia and the West over Ukraine, the threat of Russian cyberattacks against the U.S. increases. The Department of Homeland Security issued an intelligence bulletin on Jan. 23, 2022, warning that Russia has the capability to carry out a range of attacks, from denial-of-service attacks on websites to disrupting critical infrastructure like power grids.

“We assess that Russia would consider initiating a cyber attack against the Homeland if it perceived a US or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security,” the DHS stated in the bulletin, which it sent to law enforcement agencies, state and local governments, and critical infrastructure operators.

Cybersecurity experts are concerned that in the wake of recent cyberattacks by hackers affiliated with Russia, the Russian government has the capability to carry out disruptive and destructive attacks against targets in the U.S. The SolarWinds attack, uncovered in December 2020, gave the perpetrators access to the computer systems of many U.S. government agencies and private businesses. The DHS and FBI accused Russian hackers in March 2018 of infiltrating U.S. energy and infrastructure networks.

Russian cyberattacks could include continued attempts to diminish Americans’ confidence in elections, undermine economic stability, damage the energy grid, and even disrupt health care systems.

While some components of these systems almost certainly remain vulnerable to Russian-aligned hackers, the Russian government is likely to think twice before unleashing highly disruptive attacks against the U.S., because the U.S. government could interpret such attacks, particularly those targeting critical infrastructure, as acts of war. The DHS bulletin stated that Russia has a high threshold for initiating disruptive attacks. As a researcher who studies cyberwarfare, I believe a more likely threat from Russian hackers is launching disinformation campaigns.

Distract, distort and divide

Americans can probably expect to see Russian-sponsored cyber activities working in tandem with propaganda campaigns. These activities are likely to be aimed at preventing a unified response to Russian aggression in Ukraine.

Russian military doctrine includes the well-evolved concept of information confrontation, which uses cyber means to create doubt about what is true. Russia’s information warfare strategy seeks to manipulate information and relationships.

The specific maneuvers aim to bolster narratives, people and groups that support Russian interests and undermine those that are counter to Russian interests. The maneuvers, which include dismissing and distorting information and undermining opinion leaders, are carried out in the press and on social media.

Russian intelligence operatives are skilled at using technology, including amplifying misinformation through fake accounts on popular social media platforms. In effect, Russia uses social and other online media like a military-grade fog machine that confuses the U.S. population and encourages mistrust in the strength and validity of the U.S. government.

Repressive governments like those in Russia and China have perfected the manipulation of online information as a way to control their own populations. Democracies are especially vulnerable to these techniques, given the open exchange of ideas and lack of centralized control over sources of information.

In addition, U.S. society is polarized, and that polarization is occurring at an increasing rate. A study by researchers at the University of Oxford examined Russia’s computational propaganda against the U.S. between 2013 and 2018 and found that it was designed to boost U.S. political polarization.

#### Information warfare will only get easier; management is key. Even if you don’t buy our specific scenarios cyber enabled disinformation erodes confidence in national security, elected officials broadly. Therefore, we access a bigger internal link to their DAs.

Herbert Lin 19, senior research scholar for cyber policy and security at the Center for International Security and Cooperation and Hank J. Holland Fellow in Cyber Policy and Security at the Hoover Institution, both at Stanford University, June 2019, “The existential threat from cyber-enabled information warfare,” Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196, modified language indicated in brackets, //chico

The coming information dystopia

Nuclear war and climate change are arguably the most important existential challenges today that are com- pounded by the corruption of the information ecosys- tem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impos- sible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyber-enabled information warfare could still can lead to an informa- tion dystopia. Here are some possible elements:

* Adversaries manufacture numerous graphic videos of American soldiers (complete with sound effects) committing battlefield atrocities, and spread them widely through the Internet. Once upon a time, high- quality video forgeries were difficult and expensive to make. AI-based technologies will bring this so- called deepfake capability to the masses, and anyone with imagination, a modicum of technical skill, and a personal computer will be able to distribute rea- sonably realistic forgeries. Denials will be issued but of course will also not be believed by large fractions of viewers. Even if proof of inauthenticity can be provided, such evidence will not affect the responses of many viewers.
* Political campaigns conduct similar efforts to dis- credit political opponents (e.g. “showing” an oppo- nent making controversial or disqualifying remarks before an election). But they also use the existence of deepfake technologies to deflect attention from authentic and real evidence of their own political and personal misdeeds. For example, a real video of a candidate punching an old lady who supports his opponent will be dismissed as “one of those deepfakes that anyone could have produced.”
* Financial markets are disrupted by falsified videos of CEOs making announcements regarding company prospects that are much more pessimistic than expected. Attempts to correct the record are drowned out in a subsequent flood of contradictory informa- tion, all of which appear at first glance to be authentic.
* Public safety is compromised by reports of local disasters (e.g. explosions of chemical plants that result in the release large amounts of toxic gases). These reports, along with “authentic” video of peo- ple choking amidst locally familiar locations (e.g. well-known fields or sport stadiums), cause sponta- neous mass evacuations. Contradictory directions for evacuation broadcast using social media result in chaos on the streets and highways.
* Public health is placed at risk when the safety and efficacy of medical treatments known to be safe and effective are publicly questioned through active disinformation campaigns conducted on the Internet and in bookstores. Attempts to pro- vide valid information are met with responses such as “that’s what the pharmaceutical companies and medical establishment want you to think, but just look at what’s happened to our children.”
* Children in schools are threatened by online cam- paigns to spread rumor, innuendo, and positive or negative information about various students. Conducting such campaigns for pay becomes the business model of entrepreneurs who advertise that they can guarantee admission to selective colleges, boost the social standing of the children of their cli- ents, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.
* Journalists, political leaders, and judges are com- promised by artfully forged emails and alterations to other documents that are mixed with entirely authentic leaked emails and documents and are indistinguishable from them.

A world with these elements – and many more comp- parable ones – will be the inevitable result if and when deployment and use of the tools of cyber-enabled infor- mation warfare become widespread. And even more trou- bling is the fact that not every bit of information needs to be corrupted for this dystopian outcome to occur – it will require only a fraction of it to be corrupted for people to lose faith entirely in “objective” and “trustworthy” sources of information, the result of which will be that people will fractionate into their own information realities.

## UQ---Democracy

### UQ---Democracy

#### LIO and NATO is backsliding now. Sino-Russo disinformation during the height of the pandemic put us on the brink.

Gill and Goolsby 22, Ritu Gill has a PhD in psychology from Carleton university, Rebbeca Goolsby is the co-Lead of a NATO Research Technology Group on cyberdiplomacy and communications, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. XXII, 213 (under “Foreword”) //chico

Information warfare involves several deceptive and manipulative tactics employed by adversaries to achieve desired goals (Gill et al., 2019). This includes the use of disinformation, which refers to a deceptive technique that is based on the dissemina- tion of untrue information with the intention to deceive, manipulate, create division and discord, and sow doubt and fear, versus misinformation in which the disseminator is unaware that the information is untrue and has no intention to deceive (Pamment et al., 2018). The goal of disinformation is to divide, foster confusion, and demotivate people. Disinformation is not new, it is part of an old playbook of active measures; however what is new is the development of the internet, more specifically social media platforms, creating a new medium to disseminate messages, expediting the ability to propagate disinformation (Gill et al., 2019). Weaponizing the internet and social media for disinformation purposes, adversaries have an extensive network of internet trolls, bots, and sock puppets to generate and spread disinformation, permeating all areas of the internet most likely to exert influence over people and their perceptions (Gill et al., 2019). Dominant disinformation narratives surrounding COVID-19 reveals that both Russia and China have capitalized on the confusion generated by the pandemic to spread disinformation and shape narratives consistent with their goals of undermining key Western and European Union nations and the North Atlantic Treaty Organization (NATO) (Duncan et al., 2020).

#### Russia and China threaten liberal democracy—US social media exploited for information warfare—US gov key

David L. **Sloss 2022**, He is a professor at Santa Clara University School of Law, received his JD from Stanford University, MPP from Harvard University Kennedy School of Government, and BA from Hampshire College. He worked as a litigation associate at Wilson, Sonsini, Goodrich & Rosati in Palo Alto and clerked for Senior Judge Joseph T. Sneed, U.S. Court of Appeals, Ninth Circuit, San Francisco. He also worked for the U.S. Arms Control and Disarmament Agency for nine years before he attended law school., “Tyrants on Twitter”, pg 3-5// SK

Similarly, in the modern era of social media, many techno- utopians mistakenly believe that any government regulation of social media is an unwarranted infringement of individual liberty. In fact, such regulation is necessary to protect our body politic from the threat posed by Russian and Chinese information warfare. Let us be clear: Liberal democracy is under attack, not just in the United States but around the world. As of 2019: “For the first time since 2001, there are more autocracies than democracies in the world.”2 To protect our cherished liberties, we need to protect democracies from Chinese and Russian cyber troops because democratic self- government is the foundation of individual liberty. The big technology companies are not up to the task. We need government regulation so that Facebook, Twitter, and other social media companies do not continue to function as Trojan horses, allowing the virus of information warfare to infect and ultimately subvert liberal democracy. In the current geopolitical and technological environment, proponents of liberal democracy and liberal internationalism— and I openly declare myself a proponent of both— confront a difficult choice. Advocates of liberal democracy are committed to freedom of expression, with minimal government controls. Advocates of liberal internationalism are committed to reducing barriers to transnational fl ows of people, goods, and information. Russia and China are working “to upend the Western liberal order by turning Western virtues of openness . . . into vulnerabilities to be exploited.”3 Unfortunately, their strategy is working because democratic governments have failed to regulate social media to protect democracy. If we want to preserve both liberal democracy and liberal internationalism, Western democracies must restrict the ability of Chinese and Russian cyber troops to exploit social media to conduct information warfare. Until now, democratic governments have given social media companies carte blanche to decide who is entitled to create and operate accounts on their platforms. The companies have adopted open- door policies, allowing almost all people from all countries to create social media accounts. Consequently, Chinese and Russian cyber troops have developed an active presence on U.S. social media platforms. Russia has taken advantage of U.S. social media platforms to interfere with democratic elections and to erode faith in democratic institutions.4 China has exploited U.S. social media platforms to disseminate foreign propaganda extolling the virtues of its authoritarian system and highlighting the flaws of liberal democracy.5 By granting Chinese and Russian agents unrestricted access to U.S. social media platforms, democratic governments are inadvertently making a significant, albeit indirect, contribution to the worldwide erosion of liberal democratic norms. For the foreseeable future, the world will be divided between democratic and authoritarian states. The United States will continue to be the most powerful country in the democratic camp. China and Russia will be the most powerful countries in the authoritarian camp. The United States and its allies will engage in geopolitical competition with China and Russia in both military and economic domains. However, the present era differs from the Cold War in several respects. Most importantly, for the purposes of this book, due to the spread of information technology, the domain of information operations has become a much more significant battleground in the broader geopolitical landscape. As one commentator noted: “The new great- power competition won’t necessarily take place on battlefields . . . it will happen on smartphones, computers, and other connected devices and on the digital infrastructure that supports them.”6 Currently, U.S. social media platforms— primarily Facebook, Twitter, YouTube, and Instagram— are critical battlefields in the ongoing competition between democratic and authoritarian states. Russian citizens use VK to communicate with each other via social media, but Russian agents exploit U.S. social media platforms to conduct information warfare in foreign countries. Chinese citizens use Sina Weibo and other platforms to communicate with each other, but Chinese cyber troops often use U.S. social media platforms to disseminate foreign propaganda. (Chinese agents also use WeChat, a Chinese platform, for this purpose.7 ) The power of democratic governments to regulate social media could potentially give liberal democracies a major strategic advantage in the information warfare domain. Until now, Western democracies have squandered that advantage by granting Chinese and Russian agents unrestricted access to U.S. social media platforms. Those platforms are some of the most powerful weapons available in the modern information warfare arsenal. Chinese and Russian cyber troops are deploying those weapons with great effect to undermine liberal democratic norms. U.S. technology companies are effectively subsidizing their information warfare activities by granting them access to U.S. social media platforms.

## IL---Democracy

### IL---Democracy---Russia

#### Russia disinformation campaigns destabilize institutions and damage democracy - they disseminate propaganda so fast that it is difficult for the West to keep up

Rani Gold 19, Master's Student at Georgetown University in German and European Political Studies, May 2019, "How Russia Uses Disinformation to Undermine Democracy Abroad, and What Can Be Done to Stop It," Democratic Erosion, https://www.democratic-erosion.com/2019/05/03/how-russia-uses-disinformation-to-undermine-democracy-abroad-and-what-can-be-done-to-stop-it/ //AShah

In the past, the word “authoritarian” brought to mind images of violent repression, censorship, and intensive surveillance, an image that. Today, however, autocrats have a new set of tools that allow them to be subtler in their methods of control, both at home and abroad. The internet and social media are key to autocrats’ strategies for domestic stability and have been used to great effect in damaging confidence in democracy worldwide. Though it is not the only country to use social media in this way, in the American consciousness Russia is the most controversial and sensational, and a perfect case study of the ways authoritarian governments use the internet and disinformation to increase control at home and destabilize the idea of liberal democracy.

How is disinformation used within Russia?

While Russia does engage in censorship and restrict criticism of the government, they also have a unique method of spreading propaganda, which Christopher Paul and Miriam Matthews of RAND call a “firehose of falsehood”. Disinformation is spread through every type of media, constantly, and at a high volume. Different narratives are completely drowned out by the amount of false information being disseminated, and the high volume of different sources both increase the number of recipients and render similar content more believable. Falsehoods are often founded in truth, and desirable interpretations of real events are attributed to experts with views opposite to what is presented.

These tactics make truth and reality difficult to grasp. With so much information being put out constantly, it is impossible to refute all of it. Moreover, it makes domestic political engagement difficult. Russian trolls invade popular discourse (Kurowska & Reshetnikov), and making it harder for citizens to know whether what they are receiving is real political dissent or manufactured content. For some, this might result in cynicism and disengagement, because of a perception that their voices will never be heard.

How is social media used to spread disinformation abroad?

Russia’s aggressive disinformation campaign in the US began in late 2014, with general attempts to sow chaos rather than to promote any specific narrative. The goals of the propaganda followed four general themes, including attempts to undermine confidence in democratic leaders and institutions, as well as finding and exploiting fault lines in society to increase social divisions. Even their attempts to influence the 2016 US presidential election were focused as much on creating distrust in elected officials. The “firehose of falsehood” was turned on the US, aiming to create a similar suspicion of media sources, and making reality hard to distinguish from lies.

All of these tactics were used to great effect in Ukraine in 2013-2014. Crimea’s ethnic Russian population was bombarded with disinformation from Russian state media, widely available and popular on the peninsula. The news being presented portrayed the Euromaidan protests against corruption as a threat to the safety of ethnic Russians in Crimea. This exploitation of social tensions ultimately led to the annexation of Crimea by Russia. The ethnic Russian populations of Donetsk and Luhansk were also targeted, contributing to the ongoing war in the Donbass region of Ukraine.

#### Information Warfare destabilizes democracy and kills military readiness---China and Russia are gunning for us now.

Brenna Cole 21, Air Force Institute of Technology, Department of Electrical & Computer Engineering and George Noel, Experienced Educator and Researcher in the field of Computer Science with a focus on Artificial Intelligence, “Nation-State Perspectives on Information Operations and the Impact on Relative Advantage”, <https://www.ornl.gov/event/iccws-2021-sixteenth-international-conference-cyber-warfare-and-security> //lenox

2. Russian information warfare

2.1 Russian perspective Russia perceives the United States and the North Atlantic Treaty Organization (NATO) as existential threats to Its existence (Zwack and Marie-Charlotte, 2019). It views western nations as actively trying to displace the regime and disarm its military capability (Costello and McReynolds, 2018). In response to this danger, real or perceived, Russia has exerted itself more aggressively across the globe (Zwack and Marie-Charlotte, 2019). Power projection and global influence are means for Russia to elevate itself to a world power and discourage threats to its survival.

Russia's quest to achieve global influence rests heavily on the use of information operations. This spans a wide set of options, ranging from strategic deception and information manipulation to hybrid warfare and offensive attacks (Krinstiina, 2016; Zwack and Marie-Charlotte, 2019).

One of the primary ways Russia uses cyber and information operations is to shape the geopolitical environment by manipulating public opinion, both across the globe and within its borders (Hans, 2018; ICA, 2017). Russia uses information campaigns to destabilize democracies and incite domestic chaos in the nations it views as opponents (Hans, 2018). Russia uses information shaping conducted in peacetime as a method to deter aggression and erode adversary readiness (Zwack and Marie-Charlotte, 2019). In addition to manipulating foreign perceptions, Russia uses information operations to influence its own populace by spreading anti-West sentiment across the nation (Kostyuk, Powell, and Skach 2018). The goal of this is to temper domestic unrest by uniting its citizens against a common enemy (Costello and McReynolds, 2018).

Another way Russia perceives cyber and information operations is as a way to conduct aggressive actions under a veil of deception and shadow (Hans, 2018). The concept of maskirovka, or military deception, is a fundamental part of Russian thinking (Zwack and Marie-Charlotte, 2019). Cyber operations are conducted with less visibility than kinetic operations, can be difficult to attribute, and are employed not only within the boundaries of a military engagement, but across all of society. This is because the battlefield is primarily logical and has unclear borders between military forces and civilians. Russia leverages these features of cyberspace to conduct actions within a "gray zone," where their actions fall short of inciting conflict yet still degrade adversary military capabilities (Bernstein and Ball, 2015; Zwack and Marie-Charlotte, 2019).

Thirdly, Russia views information warfare as a new and transformational method of waging war to prevail in conflict (Hans, 2018). Russia's political and military strategy will use hybrid warfare by emphasizing non-traditional weapons of power, such as cyber, information, and psychological effects (Krinstlina, 2016). Kinetic forces will still be employed, but not as the primary tool relied upon for success. Instead, they will be used alongside asymmetric warfare operations and to protect information security within the cyber domain (Hans, 2018; Kostyuk, Powell, and Skach 2018). Cyber operations will be used as a combination of indirectly shaping adversary decisions and directly delivering effects to destroy or degrade a target (Zwack and Marie-Charlotte, 2019)

2.2 Organization Russian information operations are executed by both government and non-government entities (Connell and Vogler, 2017). Within the government, major players are the Federal Security Service (FSB), the Foreign Intelligence Service (SVR), and the Ministry of Defense (MOD) (Connell and Vogler, 2017). Another information-related organization is the Federal Service for Supervision in the Sphere of Telecommunications, Information Technologies, and Mass Communications (Roskomnadzor), responsible for media regulation (Connell and Vogler, 2017). By regulating what ideas are presented in the media, this organization influences domestic opinion in favor of national goals.

An important element of Russian information warfare is that many activities are conducted by organizations not directly affiliated with the Russian government but believed to be sponsored by it (Zwack and Marie-Charlotte, 2019). Adding to the deception of cyber warfare, Russia denies the awareness or support of these groups. However, the actions conducted by them match Russian objectives well (Connell and Vogler, 2017). Russia is believed to work with criminal networks, such as the Russian Business Network (RBN), and commercial companies such as media outlets (Connell and Vogler, 2017; Krinstiina, 2016). Partnership with these companies allows the government to exert greater control over the narrative and ideas presented to its populace.

2.3 Examples Many examples could be used to demonstrate Russian use of cyber operations. Below are two selected to show how Russia uses information operations to shape the strategic environment and to assist in military conflict.

A well-publicized example of Russia using information operations to influence the geopolitical environment Is the Russian election meddling In the 2016 United States presidential election. In the unclassified report on these activities, the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) assessed "with high confidence that Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the U.S. presidential election, the consistent goals of which were to undermine public faith in the U.S. democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency" (ICA, 2017). Regardless of whether President Trump would have been elected without the Russian interference, this act demonstrated the disruptive effect that information operations can create. This is evidenced by the consistent media attention on the possibility of a Russian influence campaign and the public outcry of the invasion into the American democratic process. As stated earlier, one of the goals of using information operations to shape the strategic environment is to cause chaos and uncertainty, thereby weakening the united strength of a democracy (Hans, 2018). As President Lincoln famously stated, "A house divided against itself cannot stand. By generating domestic turmoil, Russia has at the least caused internal conflict within the U.S., which stole attention that could have been focused on international issues.

An example of Russian information operations employed during military conflict can be seen from the conflict in Ukraine. Russia has been in conflict with Ukraine since 2013, with particularly strained relations since Russia annexed Crimea in 2014 (Zwack and Marie-Charlotte, 2019; Connell and Vogler, 2017). Russia used information operations of various types throughout the entirety of this conflict. One way in which they used Information campaigns had similar intent as that in the U.S. election meddling—to destabilize public support by creating an air of confusion and mistrust (Krinstiina, 2016). For example, Russia used media in Ukraine and Russia to negatively portray Ukrainian soldiers and criticize the Ukrainian government (Krinstilna, 2016). However, In this case, the use of information operations did not stop at causing chaos. Escalating from creating an atmosphere of confusion, pro-Russian groups caused soldiers to mistrust their information systems and data via cyber attacks (Connell and Vogler, 2017). Escalating even further, a presumed Russian or Russian-sponsored group known as Sandworm conducted a cyber-attack directed at the Ukrainian power grid (Kostyuk, Powell, and Skach 2018; FireEye, 2016). The attack resulted in the western part of the country losing power for several hours (Kostyuk, Powell, and Skach 2018). These information operation activities provide a real-world example of how Russia will use cyber and Information effects In a declared conflict.

3. Chinese information warfare

3.1 Chinese perspective Globalization has forced China to confront a world order that challenges its traditional governance and regime (Waldron, 2019). China is a leader in the international system but did not become one until more than a century of lagging behind further developed nations (Kissinger, 2011). These years of "suffering" are a lesson and motivator for China to gain and maintain a position of strength (Kolton 2017; Kissinger, 2011). Once it entered the international arena, China emerged as a world power, primarily due to its economic influence (Waldron, 2019). Economic prowess alone, however, is not enough to preserve China's global standing. To protect its national sovereignty, regime stability, and regional dominance, China seeks to expand its influence to other areas. A primary way China has been doing this is by modernizing and expanding its military to gain strategic influence and be prepared for future conflict (Kania and Costello, 2018; Domingo, 2016).

China views "informationized" warfare as the key to military success and national security (Kolton, 2017). This emphasis on information warfare stems from the study of previous conflicts and factors that led to the victor's success (Clarke, 2019). The start of this realization was In 1991 with the Persian Gulf War, where China concluded that an advantage in Information technology could lead to overwhelming military advantage. Additionally, China observed that an opponent's dependency on information systems was a vulnerability that could be exploited (Costello and McReynolds, 2018). In this conflict and others since then, China has observed how technological strength contributes to military success. In addition to military support, China views information and technology as a way to maintain internal stability. It is perceived as a method to achieve and protect domestic and regional sovereignty. Based on these perceptions, China uses information superiority to project power, strengthen military capabilities, and maintain domestic control (Clarke, 2019).

#### Russia uses information war as their primary means---undermines the LIO and kills democracy

Tuukka Elonheimo 21, Finnish Air Force and Air War College Senior Developmental Education and Joint Professional Military Education Phase II, given at Maxwell Air Force. “Comprehensive Security Approach in Response to Russian Hybrid Warfare”, *STRATEGIC STUDIES QUARTERLY*, <https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-15_Issue-3/Elonheimo.pdf> //lenox

Information Warfare

Russia has a long history of demonstrating its mastery of information warfare, but the focus in Putin’s regime has shifted to manipulating foreign target audiences. Admittedly, propaganda and censorship have a strong position internally. Nevertheless, Russian information warfare increasingly undermines other states’ decision-making, deteriorates societal cohesion, and disputes foreign leaders’ authority and competence. Authoritarian Russia has solidified its role as a modern propaganda hegemony. Conversely, democracies have problems retaliating against this new soft and hard power mixture. Russia’s state-driven media, officials, proxies, trolls, and politicians promote ideas, rumors, and conspiracy theories favorable to Russia, unconfirmed truths via official digital channels, and biased social media accounts. Open information networks and technologies give Russian influencers a fast and cheap means to spread propaganda globally.35 As an authoritarian state, Russia effectively controls influencers, proxy actors, and agents to conceal the Kremlin’s fingerprints. Russia and China have spent millions of dollars increasing an asymmetric, aggressive, information warfare–based “sharp power.”36 Their sharp power creates a hostile environment, amplifying distrust and discord among people and state institutions by piercing and penetrating political and informational environments. Thus, the Kremlin has used sharp power, which is more harmful than traditional culture-based soft power, to meddle in other nations’ elections and corrupt information in recent years.37 Russia’s meddling in the 2016 US presidential election is the most visible example of comprehensive information warfare. Though foreign interference efforts have always played a role in policy making, handy, cheap new technologies made organized propaganda and disinformation campaigns more efficient and widespread than ever before.38 Strategic level information warfare undermined the US-led liberal world order and the populace’s belief in the democratic presidential election system, developing a clear advantage for Trump.39 Russian intelligence agencies illegally intruded and interfered with Hillary Clinton’s and the Democratic National Committee’s email accounts and leaked content on WikiLeaks, causing political and social discord in America.40 Russian intelligence agencies cunningly exploited all modern digital networks’ vulnerabilities. More importantly, the nonregulated human social media networks multiplied the effects of distortion, dispute, and distrust.41 According to the intelligence community’s assessments, President Putin ordered the multifaceted 2016 US presidential election meddling campaign—demonstrating how centralized hybrid warfare is in Russia.42 The all-encompassing information campaign consisted of cyber espionage and intrusions against political organizations and electoral boards, public disclosure of collected data, propaganda, Russian state-owned news agency (Russia Today, Sputnik) misinformation campaigns, and fake social media profiles controlled by professional trolls from the socalled Internet Research Agency in St. Petersburg.43 One worrisome phenomenon was that information warfare targeted partisan winners and losers differently; the campaign was not directed against the whole country like the examples of Pearl Harbor and 9/11.44 Social-engineered divisive information warfare increased partisanship in the US and was a detrimental sting against democracy.

### IL---Democracy---Russia---AT: Exaggerated

#### Experts conclude AFF. Information gets circulated AND it targets those susceptible.

Mathew Ingram 19, CJR’s chief digital writer. “Researchers say fears about ‘fake news’ are exaggerated,” Columbia Journalism Review (CJR), <https://www.cjr.org/the_media_today/researchers-fake-news-exaggerated.php> //chico

This might come as a surprise to Kathleen Hall Jamieson. She’s a veteran public policy researcher who published a book last year entitled Cyberwar: How Russian Hackers and Trolls Helped Elect a President. Jamieson, whose colleagues call her “the Drill Sergeant” for her no-nonsense attitude, has more 40 years of studying human behavior under her belt. In the book, she says the evidence suggests misinformation propagated by Russian trolls likely influenced the outcome of the election, in part because of the number of “swing” or undecided voters who were susceptible to those kinds of tactics. Jamieson also notes that the traditional news media played a key role in spreading this fake news and propaganda, by writing innumerable articles about Hillary Clinton’s emails. And she argues fake news wouldn’t have had to make much of an impact to influence the election, since a fairly small number of votes gave Trump the electoral college wins he needed.

### IL---Democracy---China

#### Chinese disinformation promotes global authoritarianism---only developing democratic resilience solves.

David Sloss 22, Professor of Law at the Santa Clara University, internationally renowned scholar who has published three books, 2022, “China’s Global Information Operations,” *Tyrants on Twitter: Protecting Democracies from Information Warfare*, Chapter Four, https://doi.org/10.1515/9781503631151, RMax, shoutout to sk for the book

CHINA AND THE GLOBAL SOUTH

China’s activities in the global South related to information and communications technology raise two distinct concerns that are relevant to the central themes of this book. First, Chinese companies are exporting surveillance technology to authoritarian governments around the world. Such exports facilitate the rise of authoritarianism in the global South. Second, Chinese companies and government entities are increasingly exerting control over the channels of communication in countries throughout the global South. By controlling the channels of communication, China can shape the overall information environment in a way that supports its broader effort to make the world safe for autocracy.

Exporting Surveillance Technologies

Digital authoritarianism can be defined as “the use of digital information technology by authoritarian regimes to surveil, repress, and manipulate domestic and foreign populations.”169 The technology includes “high- resolution cameras, facial recognition, spying malware, automated text analysis, and big- data processing,”170 all supported by sophisticated artificial intelligence (AI) to facilitate mass surveillance of ordinary citizens. “The Chinese Communist Party is forging a future of mass surveillance . . . and rapidly exporting those tools to other parts of the world.”171

As discussed previously (see pp. 84–86), private Chinese companies are exporting the technology of digital authoritarianism, but they are not alone. “Firms based in the United States, France, the United Kingdom, Germany, Spain, and Israel are also key suppliers.”172 The technologies that support digital authoritarianism are not inherently evil. With appropriate laws and regulations in place, democratic countries can ensure that governments employ the technology to enhance public welfare in a manner that is consistent with liberal, democratic ideals. Unfortunately, when Chinese companies export the technology to authoritarian countries, neither the exporting nor the importing country is likely to insist on regulations to promote liberal, democratic ideals. Absent such regulations, the tools of digital authoritarianism enable autocratic rulers to conduct mass surveillance and identify political opponents. All too often, identifcation of opponents leads to arbitrary arrest, torture, and/or extrajudicial killing. A 2019 Freedom House report stated “that 47 of the 65 countries assessed featured arrests of [social media] users for political, social, or religious speech— a record high.”173

The tools of digital authoritarianism strengthen autocratic rule. “Between 1946 and 2000— the year digital tools began to proliferate— the typical dictator ruled for around ten years. Since 2000, this number has more than doubled, to nearly 25 years.”174 Moreover, “those authoritarian regimes that rely more heavily on digital repression are among the most durable.”175 Hence, commentators legitimately fear “the emergence of an AI- powered authoritarian bloc led by China . . . [that] could prevent billions of people, across large swaths of the globe, from ever securing any measure of political freedom.”176 China doves contend that “material interests, not a universalist mission of promoting autocracy abroad, are the key drivers of China’s global strategy.”177 Assuming the doves are correct, their analysis should not be construed as an argument for complacency. Chinese companies driven by the profit motive will likely help autocratic rulers entrench their control unless there is countervailing pressure to regulate surveillance technologies. Notably, the Chinese government is not applying any such pressure.

It bears emphasis that U.S. social media platforms, in the hands of autocratic rulers, function as surveillance technologies. That is no accident. Facebook and Google earn most of their revenue through advertising. Companies and political candidates pay substantial amounts of money for microtargeted advertising because Facebook and Google have amassed a tremendous amount of information about us, the targets of the ads. Thus, private companies routinely engage in surveillance of social media users by collecting huge amounts of information from billions of internet users to support the delivery of microtargeted advertising. The information that social media companies collect from their users is the raw material of “surveillance capitalism.”178

In the United States and other liberal democracies, governments do not generally conduct surveillance on social media platforms because laws enacted by democratic legislatures restrict government surveillance. However, authoritarian governments are increasingly exploiting U.S. social media platforms for surveillance purposes. A 2019 Freedom House report stated: “At least 40 of the 65 countries covered by this report have instituted advanced social media monitoring programs.”179 Moreover, “of the 15 countries in Asia assessed by this report, 13 have social media surveillance programs under development or in use.”180 The report notes that “China is a leader in developing, employing, and exporting social media surveillance tools.”181

For example, a Chinese company called Semptian has developed the Aegis surveillance system. The Aegis system “is designed to be installed inside phone and internet networks, where it is used to secretly collect people’s email records, phone calls, text messages, cellphone locations, and web browsing histories.”182 The company’s equipment is helping the CCP “covertly monitor the internet and cellphone activity of up to 200 million people” in China. More recently, Semptian “has supplied the equipment to authoritarian governments in the Middle East and North Africa.” Although a company spokesman refused to identify those countries, an investigative journalist suggests that Semptian may have sold Aegis to “Saudi Arabia, Bahrain, Morocco, the United Arab Emirates, Oman, Sudan, and Egypt.”183

Knowlesys is a Chinese company described as “an award- winning surveillance industry veteran.”184 Knowlesys “sells social media and open source internet monitoring and analysis tools to . . . private sector giants from both the East and West.” The Knowlesys Intelligence System “is available in almost a dozen languages including Arabic, English, Chinese and Uighur.” Governments use it “to effectively monitor and analyze social media.”185 In August 2020, a group of hackers “obtained internal fi les from three Chinese social media monitoring companies,” including Knowlesys.186 The hackers offered journalists “a large dump of fi les” that allegedly exposed “social media monitoring and disinformation campaigns conducted by [Knowlesys and two other] companies at the behest of the Chinese government.”187

Thus, Chinese companies are strengthening autocratic rule in the global South by exporting surveillance technology to authoritarian governments, including technology that helps those governments exploit U.S. social media platforms to conduct surveillance of their own citizens.

Controlling Channels of Communication

Marshall McLuhan famously declared that “the medium is the message.” The CCP has built a global information strategy around this idea. According to Peter Mattis, a China expert at the Jamestown Foundation:

“Over the last ten years . . . the push has been less about messaging and more about the medium. This way they can crowd out other stories, they can have essentially a monopoly on the information environment— that makes it easier for their narratives to be received and accepted.”188 China’s effort to augment its control over communication channels in the global South includes both hardware and communications media.

With respect to hardware, a report by the Australian Strategic Policy Institute shows that twelve key Chinese technology companies, in the aggregate, are involved in “52 5G initiatives, across 34 countries . . . 56 undersea cables, 31 leased cables and 17 terrestrial cables; 202 data centres and 305 telecommunications & ICT projects spread across the world.”189 A 2018 Freedom House report notes that Chinese companies have “installed internet and mobile network equipment in at least 38 countries.”190 China can potentially use its control over information pipelines to engage in both surveillance and censorship. “As more of the world’s critical telecommunications infrastructure is built by China, global data may become more accessible to Chinese intelligence agencies.”191 Indeed, according to one source, “there is already evidence of Chinese companies using their control over dissemination channels . . . to suppress information deemed undesirable by Beijing. But even where this potential has not yet been activated, the foundations are being laid to facilitate future manipulation.”192

With respect to communications media, as discussed previously, Chinese state-run media operate hundreds of television and radio stations and dozens of newspapers in countries throughout the world. In addition, China has been engaged in an “opaque campaign of buying up broadcast space on foreign airwaves and inside newspapers. . . . Beijing has been able to infiltrate local media across the world by using overseas airwaves to disseminate its message.”193 For example, a “Reuters investigation revealed there were at least 33 radio stations across 14 countries that are part of a global radio web structured in a way that obscures its majority shareholder: state- run China Radio International (CRI).”194 Xinhua “has signed exchange agreements with local counterparts” in many countries, including Bangladesh, India, Nigeria, Egypt, Thailand, Vietnam, Belarus, and Laos.195 Xinhua concluded an agreement with the Thai News Network china’s global information operations 111 allowing Xinhua to broadcast its “China Report program in Thailand on a daily basis.” In South America, “TV Peru’s Channel 7 broadcast 12 documentaries about China . . . in 2016, nearly all of which were produced by CGTN and aired during prime time.”196

China’s attempt to control the information environment in the global South appears to be gaining substantial traction in Africa. StarTimes is a privately owned Chinese television distribution company with close ties to the Chinese government. “StarTimes has been a key player in the transition from analog to digital transmission [in Africa], accruing over 10 million subscribers in 30 countries.”197 The company determines “which stations those viewers are able to access.” It appears to prioritize channels operated by Chinese state media “at the expense of independent international news stations.”198 In early 2020, StarTimes launched a daily TV show with news about the coronavirus pandemic for an African audience.199 StarTimes also entered into a joint venture with the state broadcaster in Zambia. The deal allegedly “paves the way for a Chinese company to control Zambia’s national broadcasting service.”200

One analysis suggests that “audiences in the West may prove a challenge to win over— but there is concern that Africa is more vulnerable to China’s creeping media buy- ups. . . . With a less robust media environment and countless cash- strapped local networks, China has been more active in infi ltrating and controlling African media.”201 Public opinion polling data from the Pew Research Center suggest that China’s information operations in Africa are yielding positive results. Polling data “indicated an overall decrease in China’s global favorability rating— but African nations were among the most likely to express favorable attitudes towards Beijing.”202

The next chapter focuses on a single question: “If China and Russia are using information warfare to attack liberal democracies, why don’t we do the same to them?” The short answer is that the situation is not symmetrical. Russia and China are closed societies. The United States and other liberal democracies are open societies. Social media offers Russia and China a powerful tool to exploit our openness to undermine democratic governance. However, we cannot use social media to undermine authoritarian control in China and Russia because, in both countries, authoritarian governments control social media. Chapter 5 shows that the playing field is not level because social media and other digital technologies systematically tilt the fi eld in favor of authoritarian governance and against liberal democracy. The tilt in favor of authoritarianism is not an inherent feature of the technology. Rather, the uneven playing fi eld results from the interaction between technology and regulatory strategies.

### IL---Democracy---Canadian

#### Unrestricted Russian misinformation campaigns erode Canadian democracy.

Marcus Kolga 22, senior fellow at the Macdonald-Laurier Institute, “Russian propagandists are exploiting protests to destabilize our democracy,” <https://www.proquest.com/docview/2630527416?parentSessionId=s8zyVx8adrz1QzfffgyKSos0VJPK%2BhdjeHS0MQOAKKA%3D&pq-origsite=primo&accountid=14667>, cy

Despite repeated warnings about the threat of Russian and Chinese information warfare to Canadian democracy over the past years, policy-makers have done nothing to address it. We’re now seeing the consequences of our negligence, and we can no longer hesitate to defend ourselves against it.

From Chinese government interference in Canada’s last federal election to Russian disinformation targeting COVID vaccines, lockdowns and ethnic communities, foreign information warfare and influence operations are threatening to tear apart the core fabric of our democracy and society.

The warnings bells have grown to a deafening din, yet we’ve chosen to maintain a dangerously narrow focus on foreign interference in our elections. Over the past 24 months, hostile foreign governments, and those aligned with them, have intensified their attacks on our democracy, leveraging the fear, uncertainty and anger that the pandemic has caused to divide us.

This is nothing new. The Russian government used vaccine hesitancy to manipulate western societies since 2014, when it published amplified anti-vaccination narratives targeting left-leaning suburban families. Those campaigns were so effective that the WHO proclaimed vaccine hesitancy as the top global health threat in 2019, over a year before the COVID virus first appeared.

During the initial months of the COVID pandemic, the European Union and experts on information warfare warned the Russian government would exploit the crisis to intensify its effects and to “generate panic and sow distrust.” Indeed, Russian state media and their proxies have unleashed an unrelenting firehose of disinformation and COVID-related conspiracies that have provoked civil unrest from Berlin to Ottawa.

Ideologically agnostic, Putin’s only doctrine is power and the consolidation of it. He does not share any of our democratic values nor those of any of our mainstream political parties.

Over the past 22 years, he and the corrupt oligarchs who support him have robbed the Russian state and people blind. Russian incomes have not risen in over a decade and there is deep concern about corruption. Russia’s basic civil infrastructure hasn’t developed beyond the 1980s: in 2020 Russia’s chief auditor reported that one-in-three Russian hospitals lack running water.

To maintain the support of his people, Putin has created one crisis after another, from the 1999 apartment bombings to the new “genocide” in Eastern Ukraine. He manufactures enemies who conspire to suppress Russian power and the reconstitution of the Soviet Union. Russian propagandists vilify the LGBTQ community, NATO and Ukraine, even as Putin positions himself as a heroic leader who will save his people from the chaos of democracy.

Over the course of the pandemic, Russian state media and platforms aligned with it, including here in Canada, have aggressively published and amplified narratives that question the existence of COVID, the legitimacy of Canadian public health protocols and the safety of vaccines. These include wild conspiracy theories that claim “big pharma” is using the cover of COVID to inject citizens with poisonous substances masquerading as vaccines. The Russian embassy in Canada has directly published stories to promote hesitancy in western vaccines on its own website.

The trucker protests have been fuelled, in part, by this wave of disinformation. Riding on top of that wave are radical extremists who have injected themselves into the protests. Their caustic, anti-democratic messaging is now being legitimized and amplified by Russian state media.

In recent weeks, Russia state media coverage of the protests has provided an international platform for extremists, who have taken advantage of otherwise peaceful protests, calling for the removal of Canada’s government. This represents direct interference by a Russian government owned and controlled agency in Canada’s democracy. By legitimizing anti-democratic extremism, the Russian government is normalizing and promoting it. When Canadian elected officials promote Russian propaganda on social media and endorse it, they become direct participants in the Kremlin’s cognitive warfare against our democracy.

### IL---Democracy---AT: Alt-Causes

#### No alt causes---disinformation is the largest threat to democracy.

David Sloss 22, Professor of Law at the Santa Clara University, internationally renowned scholar who has published three books, 2022, “Policy Analysis: Weighing Costs and Benefits,” *Tyrants on Twitter: Protecting Democracies from Information Warfare*, Chapter Seven, https://doi.org/10.1515/9781503631151, RMax, shoutout to sk for the book

Accordingly, the argument in this chapter is directed toward a target audience who agree that democratic decay is a significant problem and that foreign threats to liberal democracy are significant causal factors contributing to that problem. If those two assumptions are correct, it follows almost inexorably that Chinese and Russian information warfare constitutes a significant threat to liberal democracy. Clearly the category of foreign threats to liberal democracy is broader than just information warfare (see figure 3 in chapter 1). Nevertheless, there is a broad consensus among relevant experts that Chinese and Russian information warfare is one of the most salient foreign threats— if not the most salient foreign threat— to liberal democracy. This chapter assumes that the expert consensus is correct. The analysis of costs and benefits proceeds from that premise.

## Impacts---Democracy

### Impact---Democracy---Kasparaov

#### Democracy solves extinction

Kasparov 17, Chairman of the Human Rights Foundation, 2/16/2017 Garry, “Democracy and Human Rights: The Case for U.S. Leadership” <http://www.foreign.senate.gov/imo/media/doc/021617_Kasparov_%20Testimony.pdf>

The Soviet Union was an existential threat, and this focused the attention of the world, and the American people. There existential threat today is not found on a map, but it is very real. The forces of the past are making steady progress against the modern world order. Terrorist movements in the Middle East, extremist parties across Europe, a paranoid tyrant in North Korea threatening nuclear blackmail, and, at the center of the web, an aggressive KGB dictator in Russia. They all want to turn the world back to a dark past because their survival is threatened by the values of the free world, epitomized by the United States. And they are thriving as the U.S. has retreated.The global freedom index has declined for ten consecutive years. No one like to talk about the United States as a global policeman, but this is what happens when there is no cop on the beat. American leadership begins at home, right here. America cannot lead the world on democracy and human rights if there is no unity on the meaning and importance of these things. Leadership is required to make that case clearly and powerfully. Right now, Americans are engaged in politics at a level not seen in decades. It is an opportunity for them to rediscover that making America great begins with believing America can be great. The Cold War was won on American values that were shared by both parties and nearly every American. Institutions that were created by a Democrat, Truman, were triumphant forty years later thanks to the courage of a Republican, Reagan. This bipartisan consistency created the decades of strategic stability that is the great strength of democracies. Strong institutions that outlast politicians allow for long-range planning. In contrast, dictators can operate only tactically, not strategically, because they are not constrained by the balance of powers, but cannot afford to think beyond their own survival. This is why a dictator like Putin has an advantage in chaos, the ability to move quickly. This can only be met by strategy, by long-term goals that are based on shared values, not on polls and cable news. The fear of making things worse has paralyzed the United States from trying to make things better. There will always be setbacks, but the United States cannot quit. The spread of democracy is the only proven remedy for nearly every crisis that plagues the world today. War, famine, poverty, terrorism–all are generated and exacerbated by authoritarian regimes. A policy of America First inevitably puts American security last.American leadership is required because there is no one else, and because it is good for America. There is no weapon or wall that is more powerful for security than America being envied, imitated, and admired around the world. Admired not for being perfect, but for having the exceptional courage to always try to be better. Thank you.

### Impact---Democracy---BioD

#### Democracy solves biodiversity - it provides political accountability, compliance with international treaties, and effective political lobbying

Oskar Ryden 19, a PhD Student in political science. My general research interest includes issues with equivalence in the measurement of social science concepts, Alexander Zizka is a postdoctoral researcher at the EA lab and synthesis group of the German Centre for Integrative Biodiversity Research (iDiv) in Leipzig, Germany, Sverker Carlsson Jagers is a Professor at University of Gothenburg and guest-professor at Luleå University of Technology, director of CeCAR (Centre for Collective Action Research), Staffan I. Lindberg holds a PhD (2005) from Lund University, Sweden. His dissertation won the American Political Science Association's Juan Linz Award for best dissertation 2005. He was assistant professor at Kent State University (2005-2006), assistant/associate professor at University of Florida (2006-2013), and has been with University of Gothenburg since 2010, full professor since 2013, Alexandre Antonelli is the Director of Science at the Royal Botanic Gardens, Kew, June 2019, "Linking democracy and biodiversity conservation: Empirical evidence and research gaps," The Royal Swedish Academy of Sciences, https://link.springer.com/content/pdf/10.1007/s13280-019-01210-0.pdf //AShah

Political institutions are relevant for biodiversity conservation since the national management of biodiversity can be understood as a case of decision-making in the political system. Thus, variation in the political institutions (i.e. being more or less democratic) that structure the selection of decision-makers, and the processes of decision-making, should be expected to impact the success of biodiversity conservation across countries. Specifically, there are three categories of hypothetical and non-directional arguments why democracy can be related to biodiversity conservation, all of them related to the opportunity structure that actors face (see e.g. Midlarsky 1998; Neumayer 2002; Li and Reuveny 2006 for a more detailed description of the links between democracy, biodiversity conservation, and environmental quality in general). First, the political rights, normally associated with democracy, including the freedom of association, the freedom of expression, and the freedom of press, together allow for a more productive involvement of citizens in politics, both through political parties and civil society organizations and to participate in or lobby decision-making. Political rights also allow for the media and other actors to address biodiversity issues through shaping the public opinion and affecting the policy agenda (Li and Reuveny 2006). Second, when the faith of political leaders are largely decided by citizens through repeated, free, and fair elections with universal suffrage, the expectation is that this vertical accountability electoral mechanism should promote the distribution of environmental public goods (Li and Reuveny 2006), including positive impacts on biodiversity conservation. Additionally, elections as the normal way of selecting leaders tend to reduce short-term uncertainty about political survival (i.e. fear of being removed from office) thus allowing actors to allocate more resources to long-term strategies (Wurster 2013). This can be expected to, for example, promote policies that are better aligned with future needs (i.e. conserving biodiversity for future generations) or allow political parties to compete for support with more or less ‘‘green’’ agendas. Third, through the political constraints that leaders face with increasing liberal democratic institutions, for example the rule of law, judicial constraints, and legislative constraints can foster compliance with legislation and international treaties (Li and Reuveny 2006). Constraining leaders also decreases their possibilities to act opportunistically, which should provide incentives for other actors to cooperate in the management of biodiversity as it introduces stronger mutual expectations of lawful behaviour (Sjo¨stedt 2013). This may well be expected to have a positive effect on biodiversity.

#### Biodiversity Loss causes Extinction.

Torres 16 Phil Torres 4-11-2016 “Biodiversity loss: An existential risk comparable to climate change” thebulletin.org/biodiversity-loss-existential-risk-comparable-climate-change9329 (founder of the X-Risks Institute, an affiliate scholar at the Institute for Ethics and Emerging Technologies)

The sixth extinction. The repercussions of biodiversity loss are potentially as severe as those anticipated from climate change, or even a nuclear conflict. For example, according to a 2015 study published in Science Advances, the best available evidence reveals “an exceptionally rapid loss of biodiversity over the last few centuries, indicating that a sixth mass extinction is already under way.” This conclusion holds, even on the most optimistic assumptions about the background rate of species losses and the current rate of vertebrate extinctions. The group classified as “vertebrates” includes mammals, birds, reptiles, fish, and all other creatures with a backbone. The article argues that, using its conservative figures, the average loss of vertebrate species was 100 times higher in the past century relative to the background rate of extinction. (Other scientists have suggested that the current extinction rate could be as much as 10,000 times higher than normal.) As the authors write, “The evidence is incontrovertible that recent extinction rates are unprecedented in human history and highly unusual in Earth’s history.” Perhaps the term “Big Six” should enter the popular lexicon—to add the current extinction to the previous “Big Five,” the last of which wiped out the dinosaurs 66 million years ago. But the concept of biodiversity encompasses more than just the total number of species on the planet. It also refers to the size of different populations of species. With respect to this phenomenon, multiple studies have confirmed that wild populations around the world are dwindling and disappearing at an alarming rate. For example, the 2010 Global Biodiversity Outlook report found that the population of wild vertebrates living in the tropics dropped by 59 percent between 1970 and 2006. The report also found that the population of farmland birds in Europe has dropped by 50 percent since 1980; bird populations in the grasslands of North America declined by almost 40 percent between 1968 and 2003; and the population of birds in North American arid lands has fallen by almost 30 percent since the 1960s. Similarly, 42 percent of all amphibian species (a type of vertebrate that is sometimes called an “ecological indicator”) are undergoing population declines, and 23 percent of all plant species “are estimated to be threatened with extinction.” Other studies have found that some 20 percent of all reptile species, 48 percent of the world’s primates, and 50 percent of freshwater turtles are threatened. Underwater, about 10 percent of all coral reefs are now dead, and another 60 percent are in danger of dying. Consistent with these data, the 2014 Living Planet Report shows that the global population of wild vertebrates dropped by 52 percent in only four decades—from 1970 to 2010. While biologists often avoid projecting historical trends into the future because of the complexity of ecological systems, it’s tempting to extrapolate this figure to, say, the year 2050, which is four decades from 2010. As it happens, a 2006 study published in Science does precisely this: It projects past trends of marine biodiversity loss into the 21st century, concluding that, unless significant changes are made to patterns of human activity, there will be virtually no more wild-caught seafood by 2048. 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.

## IL---Anti-Nuclear Movements

### IL---Anti-Nuclear Movements

#### Targeted misinformation campaigns erode NATO cohesion and distract from regulation of Russian nuclear stockpiling.

Lesley Kucharski 18, Counterproliferation Analyst at Lawrence Livermore National Laboratory, “Russian Multi-Domain Strategy against NATO: information confrontation and U.S. forward-deployed nuclear weapons in Europe,” <https://cgsr.llnl.gov/content/assets/docs/4Feb_IPb_against_NATO_nuclear_posture.pdf>, cy

Western philosophical and moral principles incline strategic thinkers in democratic societies to reject the notion that information can be used as a weapon or a domain of warfare instead of a tool of freedom and truth. International law suggests that the vast majority of societies and governments agree that freedom of information and truth are crucial to healthy societies. In practice, however, there are also governments that perceive them as both a form of strategic deception and as a vulnerability that can be exploited through information operations.

An increasingly common dimension of Russian strategy against the United States and its NATO allies and partners is information confrontation [informatsionnoe protivoborstvo], or IPb. Russia actively pursues a strategy of exploiting perceived vulnerabilities of these democratic societies by carrying out informational-technical (e.g., cyber) and informational-psychological operations below the threshold of open military conflict in order to exacerbate pre-existing societal, political, and military divisions, thereby degrading NATO cohesion. 1 The literature on IPb suggests that a key element of this strategy is an effort to create confusion and sow doubt in the existence of truth.2 Russia has also applied these operations alongside traditional military means of armed conflict in NATO partner states, Georgia and Ukraine, in order to slow down the decision-making processes in those countries as well as throughout the international community. In Georgia and Ukraine, Russia has employed both aspects of IPb to challenge the Westphalian international order and achieve a fait accompli with a limited use of military force.

The body of literature dedicated to understanding the role of IPb in Russian strategy has yet to explore its relationship to U.S. extended nuclear deterrence. This topic merits study for at least three reasons. First, Russian strategic thinkers and official strategic documents identify NATO as threat and assign an increased role for asymmetric, indirect, and non-military (including informational) measures in conflict resolution (see section 3). Second, Russia has historically used IPb against the Alliance with mixed success. In this regard, Soviet active measures [aktivnie meropriyatiya] operations targeting societal, political, and military divisions about NATO nuclear posture in the late 1970s and early 1980s are illuminating (see section 4). Finally, current Russian practice reflects an effort to propagate disinformation about U.S. forward-deployed nuclear weapons (see section 5)

This study seeks to contribute to the body of literature on IPb by analyzing the evolution of Russian strategic thought on and practice of IPb in relation to U.S. forward-deployed nuclear weapons in Europe. It explores the following questions: How and under which conditions does Russia employ IPb in an effort to achieve preferred strategic outcomes related to NATO nuclear force structure? What insights about contemporary Russian IPb efforts can be gained from studying Soviet active measures campaigns against NATO nuclear force posture? Analysis of trends in Russian strategic thinking, official Russian strategic documents, and two cold war case studies suggest that IPb operations targeting societal, political, and military divisions within NATO regarding the role of U.S. forward-deployed nuclear weapons in its defense and deterrence posture are an important feature of Russia’s multi-domain strategy against NATO. As the Soviet Union did, Russia pursues a two-tiered strategy “from above” and “from below” that exploits pre-existing divisions and perceived vulnerabilities of democracies.3 Rather than seeking to create confusion and sow doubt in the existence of truth in order to exacerbate existing divisions as the literature on IPb suggests, however, Russia promotes very specific, historically consistent, and simple political and security narratives about U.S. forward deployed nuclear weapons that resonate with the growing anti-nuclear weapons movement in democratic societies and deflect attention from its own large stockpile of non-strategic nuclear weapons.

Russian IPb strategy differs from Soviet strategy due to three structural factors: the characteristics of modern warfare, the contemporary information ecosystem and its associated information technologies, and the increased influence of non-governmental organizations (NGOs) on global politics. These three structural changes allow Russia to blur the distinction between its campaigns “from above” and “from below” in a way that the Soviet Union could not. For example, it has covertly planted disinformation about U.S. forward-deployed nuclear weapons into the information ecosystem using small independent internet news agencies and enjoyed the subsequent proliferation of its story and narrative across the world by other news agencies which picked up the story and through social media websites like Twitter. By leveraging this new information environment, Russia seeks to influence government officials as well as the general public rather than targeting one specific group. Furthermore, Russia leverages the contemporary information ecosystem to promote its narratives without needing to tie its hands to the anti-nuclear weapons movement through front organizations or foreign political parties as the Soviet Union did. It no longer needs to fund civil society organizations like the World Peace Council (WPC) in an effort to enhance the legitimacy of its narratives because NGOs that agree with Russian narratives about the dangers of NATO’s nuclear posture today are more numerous and have more political influence and larger endowments than similar organizations during the cold war period. The International Campaign to Abolish Nuclear Weapons (ICAN)—the NGO which was awarded the Nobel Peace Prize in 2017 for promoting nuclear disarmament and its leadership in advocating the Treaty on the Prohibition of Nuclear Weapons (TPNW)—and its 532 partner organizations in 103 countries is an example of this structural change. One significant consequence of these structural changes is that the pressure to pursue arms control arrangements is directed primarily at NATO instead of being distributed across NATO and Russia as it was distributed across NATO and the Soviet Union in the late 1970s and early 1980s.

# Solvency

## Advocates---Broad Cooperation

### Solvency Advocate---Best Practices/Broad Coop

#### Current NATO counter-disinformation tactics fail, BUT the plan’s approach centered around strengthening both national and international resilience by coordinating best practices and integrating effective tactics into NATO doctrine solves.

Linda Sanchez 21, Head of the U.S. Delegation to the North Atlantic Treaty Organization, United States House Representative from California’s 38th District, active competitor in the annual Congressional Baseball Game, October 2021, “Bolstering the Democratic Resilience of the Alliance Against Disinformation and Propaganda,” https://www.illiberalism.org/linda-sanchez-bolstering-the-democratic-resilience-of-the-alliance-against-disinformation-and-propaganda/, RMax

1. Increase NATO’s capacity to understand and respond to threats in the information space

66. Member states should expand NATO’s human, financial, and technological resources dedicated to fighting disinformation and propaganda to match both the level of the threat and the Alliance’s ambitions to counter it. Such resources would help strengthen NATO’s capacity to monitor the information environment in which it operates and respond to any hostile information activity.

67. NATO and its member countries should improve their understanding of the domestic vulnerabilities to disinformation and propaganda faced by the Allies. In particular, the Alliance should better account in its counter-disinformation efforts for the role of citizens within its borders in the spread of disinformation. Additionally, NATO should carry out regular in-depth assessments in all 30 member states to identify and monitor specific national vulnerabilities to disinformation and propaganda, similar to the surveys that it carries out every two years to assess the state of civil preparedness in Allied countries. These assessments could be carried out by peers or a group of experts. Based on the insight gained in such assessments, NATO should shift from a broad and one-size-fits-all communication strategy to a more tailored approach better targeting the groups most vulnerable to disinformation and propaganda in each Allied country. As such, these assessments would help NATO make the most of its limited resources and give member states a better understanding of the shortfall areas in which they could focus their efforts. In addition to this regular monitoring, member states should make more frequent use of the NATO Counter-Hybrid Support Teams to identify vulnerabilities to disinformation ahead of or during sensitive events, such as elections. Similarly, Allied countries should actively use the expertise of the relevant NATO centers of excellence, including the Strategic Communications Centre of Excellence.

68. NATO should step up its response to the disinformation and propaganda campaigns launched by authoritarian states, particularly Russia and China. As many of the false or misleading narratives promoted by these actors are predictable, NATO should increase its efforts to prebunk such messages at early stages before they spread widely, rather than debunk them once they have achieved broad circulation. At the same time, careful consideration must be given to which claims should be actively refuted and which should not. Indeed, disproving claims that have not yet been widely disseminated can be counterproductive as it may inadvertently give them increased visibility.

69. NATO and its member states should further bolster their efforts to increase public knowledge about the Alliance. Better educating Allied publics about the Alliance’s values, objectives, and benefits would indeed contribute to countering disinformation about NATO. To achieve this goal, however, NATO and individual member countries should shift the primary focus of their communications strategies from countering negative narratives to actively communicating positive narratives about the successes of the Alliance. They should continue promoting NATO’s achievements and solidarity, as they have successfully done in the context of the response to the pandemic.

70. NATO should further increase the coordination of counter-disinformation efforts between Allied countries and with partners. The wide-reaching nature of disinformation campaigns means that responses should be transatlantic in scope and inherently collaborative. NATO can play a more active role in coordinating national efforts and in sharing best practices amongst member states and partner countries for possible replication. To that end, NATO should develop a taxonomy of national measures adopted by NATO member states and partner countries, as well as countries that are not NATO partners but have experience in countering disinformation.

2. Create a framework that places democratic resilience and efforts to counter disinformation and propaganda at the center of NATO’s future

71. NATO and the Allies should ensure that countering disinformation and propaganda, and strengthening democratic resilience more broadly, are part and parcel of the ongoing discussions on NATO’s future, including the NATO 2030 process and the update of the Strategic Concept.

72. The Allies should reaffirm their shared commitment to democratic values and principles by establishing a Center for Democratic Resilience within NATO, as suggested by the NATO PA President Gerald Connolly and subsequently recommended by the NATO 2030 Group of experts (Connolly, 2019; Group of experts, 2020). Structurally similar to the Euro-Atlantic Disaster Response Coordination Centre, this Center would provide technical and research support to member states in strengthening democratic resilience, ensuring greater societal cohesion, resisting hostile interference, and responding to disinformation from external and internal actors. To do so, the Center would, first, monitor, identify, and highlight vulnerabilities in member states in the areas of democracy, human rights, and the rule of law. Second, the Center would assist member states, upon request, in the development of institutions, laws, and policies to tackle corruption, foster trust in elections, and respond to other governance challenges. Through these two strands of work, the Center would play a key role in supporting member states in recognizing and remedying democratic vulnerabilities that could otherwise be used by malevolent actors to spread disinformation and propaganda within the Alliance. Although institutionally part of NATO, the Center would harness the experience and knowledge of civil society experts and think tanks and could include an advisory group of external experts. The creation of the Center for Democratic Resilience, as a structure within NATO, would symbolize the enduring commitment of all Allies to uphold the founding democratic principles of the North Atlantic Treaty.

73. Member states should support the development of the Euro-Atlantic Centre for Resilience in Romania. This Centre, although not a NATO structure, constitutes a useful international resource for NATO, Allied countries and their partners to discuss threats to their resilience, including in the information space; to develop analytical tools and best practices to counter these threats; and to increase joint education and training activities in this area. The development of this Centre and the proposal to create a Center for Democratic Resilience within NATO should not, however, be opposed, as both institutions will play complementary roles. The Euro-Atlantic Centre for Resilience focuses on analysis, exchange, training and cooperation (including with partners outside the organization, notably neighboring countries and the EU), whereas the Center for Democratic Resilience will internally assist member states in operationally responding to threats to democratic values.

74. NATO should make the ongoing development of a counter-hostile information and disinformation toolbox for Allies a priority. In addition to outlining key definitions, approaches, and response options at the national level, it could be used as a basis to establish NATO-level standards for resilience to disinformation and propaganda. Member states could use such standards to set national targets and compare their progress to that of other Allies. This could include common standards in terms of the institutional structure designated to address disinformation threats, the financial and human resources allocated, and the legal framework.

75. NATO and Allied countries should reflect on options for a more offensive counter-disinformation approach. The Alliance should consider developing a strategy that would impose greater costs on malevolent actors aggressively disrupting the information space. NATO has recognized that a serious hybrid attack, such as a cyberattack, could trigger Article 5 of the Washington Treaty, where an attack against one Ally is treated as an attack against all (Stoltenberg, 2019). Attention should be paid to the conditions under which a disinformation or propaganda campaign could be considered a possible trigger. The Alliance cannot remain passive in the face of hostile information activity which threatens to undermine the foundations of our democratic institutions and societies.

#### NATO is key to implement a cognitive warfare monitoring and alert system - that allows member states to effectively track and respond to cognitive warfare campaigns

Alexander Cocron 21, Alexander Cocron is a Lecturer in the Whiting School of Engineering at Johns Hopkins University, where he teaches advanced innovation methods and strategy development, May 2021, "Countering cognitive warfare: awareness and resilience," NATO Review, https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html; //AShah

The need for awareness

The advantage in cognitive warfare goes to him who moves first and chooses the time, place, and means of the offensive. Cognitive warfare can be waged using a variety of vectors and media. The openness of social media platforms allows adversaries easily to target individuals, selected groups, and the public via social messaging, social media influencing, selective release of documents, video sharing, etc. Cyber capabilities permit the use of spearfishing, hacking, and tracking of individuals and social networks.

A proper defence requires at the very least an awareness that a cognitive warfare campaign is underway. It requires the ability to observe and orient before decision-makers can decide to act. Technology solutions can provide the means to answer some key questions: Is there a campaign going on? Where did it originate? Who is waging it? What might be its aims? Our research indicates that there are patterns of such campaigns that repeat and can be classified. They may even provide “signatures” unique to specific actors that can help to identify them.

A particularly useful technology solution may be a cognitive warfare monitoring and alert system. Such a system could help to identify cognitive warfare campaigns as they arise, and to track them as they progress. It could include a dashboard that integrates data from a wide range of social media, broadcast media, social messaging, and social networking sites. This would display geographic and social network maps that show the development of suspected campaigns over time.

By identifying the locations, both geographic and virtual, in which social media posts, messages, and news articles originate, the topics under discussion, sentiment and linguistic identifiers, pacing of releases, and other factors, a dashboard could reveal connections and repeating patterns. Links between social media accounts (for example, shares, comments, interactions) and their timing could be observed. The use of machine learning and pattern recognition algorithms could help quickly to identify and classify emerging campaigns without the need for human intervention.

Such a system would allow real-time monitoring and provide timely alerts to NATO and Alliance decision-makers, helping them to formulate appropriate responses to campaigns as they emerge and evolve.

Considerations on resilience

Since the early days of the Alliance, NATO has played an essential role in promoting and enhancing civil preparedness among its member states. Article 3 of the NATO founding treaty establishes the principle of resilience, which requires all Alliance member states to “maintain and develop their individual and collective capacity to resist armed attack.” This includes supporting the continuity of government, and the provision of essential services, including resilient civil communications systems.

Some key considerations for NATO at this time are how best to take the lead in defining cognitive attacks, how to help Alliance members maintain awareness, and how to support more robust civil communications infrastructures and public education frameworks in order to enhance the capacity to resist and to respond.

## Advocates---Innovation Center

### Solvency---Innovation Center

#### NATO action is key---only expanding Article V to hybrid warfare, promoting innovation centers, and supporting national governance prevents Russian hybrid tactics.

Dr. Chris Dolan 22, Professor of Political Science and Director of the Masters of Science Program in Intelligence and Security Studies at Lebanon Valley College, two-time Fulbright U.S. Scholar in international security in North Macedonia and Kosovo, Ph.D. in International Relations and National Security Studies from the University of South Carolina, 2/15/2022, "NATO Must Boost Hybrid Warfare Defenses," https://www.justsecurity.org/80176/nato-must-boost-hybrid-warfare-defenses/, RMax

Russia could launch a conventional military invasion of Ukraine at any moment, but it could also destabilize and undermine it without ever firing a shot. Russian military exercises and positioning are powerful tools of unpredictability that keep NATO and Ukraine off balance while Russian operatives and their proxies wage a hybrid war through covert operations, coordinated disinformation campaigns, and cyber attacks. To build resilience against hybrid warfare, NATO should collaborate with the private sector and devote more resources to technology literacy and innovation.

Russia’s Hybrid Warfare Strategy

Russia’s strategy is centered on promoting a narrative of grievances. Russia believes the United States is using Ukraine and promoting NATO expansion to contain Russian national security interests and encroach on its traditional spheres of influence. It also contends that Ukraine should return to the Minsk Agreements and end its attempt to win back Donbas. These are false narratives because sovereign and independent states have the freedom to determine their own path and seek membership in any alliance. And it would be madness for the Ukrainian government to retake Donbas given the Russian military presence there. The Russian rhetoric is a trojan horse created by the Kremlin to renegotiate the end of the Cold War and redraw European borders the same way Russia did when it illegally annexed Crimea in 2014.

The effectiveness of the Russian narrative depends on combining conventional military positioning with hybrid tactics or “active measures.” Hybrid actions taken in the so-called “gray-zone” typically consist of measures short of conventional warfare such as limited strikes, special operations forces, raids, cyber attacks, and covert influence operations. Hybrid warfare is a central element of Russia’s military strategy, in which operatives remain just below the radar and work with proxies to stage false flags to justify an invasion. To crush the Prague Spring in 1968, Soviet operatives in Czechoslovakia planted weapons in packages labeled “Made in the USA,” which were published in Soviet state-controlled outlets as signs of a U.S.-led plot. The KGB ran active measures during the Soviet war in Afghanistan in the 1980’s, often using “false bands” of Afghan units posing as CIA-backed guerillas to justify Soviet military operations.

Misinformation and disinformation are quickly and efficiently distributed through news channels and social media to influence public opinion. Russian state-owned outlets Russia Today (RT), Tass, and Sputnik have a strong presence on Facebook, Twitter, YouTube, and Telegram, echoing the Kremlin’s position and portraying NATO and the United States as aggressors. In 2013-2014, Russian state media framed the Maidan protests that toppled Ukrainian President Viktor Yanukovych as “fomented by the U.S. in cooperation with fascist Ukrainian nationalists” that were used as a pretext for Russia’s little green men to seize Crimea.

One Russian-backed channel on YouTube is НАШ or NASH TV, which has been promoting Russia’s narrative until it was banned in Ukraine. Founded by former pro-Russia Ukraine parliament member Yevheniy Murayev, NASH TV is a Kremlin mouth piece flooding viewers with anti-American and anti-NATO falsehoods. Last month, the United Kingdom accused Russia of attempting to overthrow Ukrainian President Volodymyr Zelensky and replace him with Murayev. This is the same approach used by Russia when it seized Crimea and installed Sergey Aksyonov as the so-called Prime Minister of Crimea.

Sustained Russian information operations reinforce specific elements in Moscow’s narrative of grievances. First, NATO’s eastward expansion since the end of the Cold War is the real threat, not Russia. Second, Ukraine and Georgia joining NATO would threaten the European security order. Third, the annexation of Crimea and support for separatists in Donbas are liberations of Russian-speaking communities.

Troll factories and bots spread large volumes of fake news stories, making it almost impossible to counter the steady deluge of disinformation. On January 31, it Western media reported that Russia planted fake stories about bomb threats against Ukrainian schools and shopping malls, forcing children to online learning and closing businesses. Just last week, U.S. officials uncovered a plot by Russian intelligence to fabricate a propaganda video portraying fake explosions, corpses, and grieving women designed to legitimate a Russian invasion to protect civilians in Ukraine.

Russia supplements information operations with cyber attacks. Russian hackers recently breached Ukrainian networks, replacing publicly facing websites with messages in Ukrainian and Polish designed to look like a Polish cyber operation. Russian cyber attacks targeted Georgian networks during the 2008 South Ossetia War and again in 2015 when Sandworm, a hacking group linked with Russian intelligence, took down Ukraine’s power grid.

Russian state-sponsored cyber attacks targeting Ukraine can devastate U.S. and NATO networks. The 2017 Notpetya and WannaCry attacks spread throughout the world soon after hitting their targets. In the 2020 Solar Winds hack, cyber criminals directed by Russian intelligence inserted malicious code into updates in Orion software that infected servers used by the U.S. Treasury, Energy, and Defense Departments, as well as Microsoft, Intel, and Cisco. The U.S. Cybersecurity and Infrastructure Security Agency recently warned U.S. networks are vulnerable to more Russian cyber attacks.

Russia also uses blended cyber operations, in which governments tolerate cyber criminals and ransomware groups operating in their countries. For example, the 2021 cyber attacks against Colonial Pipeline, which controls much of the fuel along the U.S. East Coast, were launched by criminal group Darkside operating in Russia. Darkside locked up Colonial Pipeline’s networks and held data hostage until it paid a ransom of $5 million.

Steps NATO Should Take

Information warfare and cyber attacks demonstrate that NATO must get serious about building resilience against hybrid war tactics. This means prioritizing counter-hybrid measures in NATO’s next Strategic Concept, which will be developed in June. NATO should take the following steps to counter Russian information operations:

1. NATO’s next Strategic Concept should update Article V of the North Atlantic Charter, which commits NATO members to defend one another, to include hybrid war tactics in addition to conventional military actions. While the range of gray-zone operations makes it difficult to know when and how to trigger the collective defense mechanism, NATO members should engage in deterrence in the contemporary battlespace.
2. NATO must establish a network of innovation centers to expand on its existing centers of excellence. NATO developed the Strategic Communications Centre of Excellence in Latvia to identify disinformation and the Cooperative Cyber Center of Excellence in Estonia to monitor cyber operations. NATO also approved the NATO-Industry Cyber Partnership to improve the alliance’s relationship with private firms and coordinate cyber defense efforts.
3. New NATO innovation centers could engage in cutting-edge research and development on artificial intelligence, quantum computing, autonomous machines, hypersonic technologies, and information and technology literacy. Innovation centers could be modeled on the European Union’s East Stratcom Task Force, which is staffed with experts specializing in Russian propaganda through its EUDisinfo site. Innovation centers funded through NATO’s Science for Peace and Security program could partner with NATO’s Joint Intelligence and Security Division (JISD).These centers could also develop public-private partnerships with commercial firms, academic institutions, and civil society groups to build resilience through training centers, research institutes, and information technology programming.
4. Governance and rule of law among alliance members must be improved as weak institutions provide maligned external actors avenues to interfere. For example, while an innovation center can improve North Macedonia’s ability to combat disinformation and cyberattacks, it must also improve domestic governance, combat corruption, strengthen judicial practices, and enhance economic opportunities. President Biden’s executive actions targeting corruption in the Western Balkans is a significant step to promote accountability.

The most effective way to defend against Russian hybrid tactics is for NATO to partner with the private sector and academia to lead research and development initiatives that can boost alliance-wide emerging and disruptive technologies policies. Since many security-related applications of emerging and disruptive technologies are derived from private firms, partnering with companies, start-ups, and universities and research institutes is essential to securing alliance members in the 21st Century. NATO should invest in strengthening capacity and innovation against hybrid attacks as much as it invests in conventional military hardware.

#### Cooperating with NATO via a central, coordinating counterinformation center successfully prevents Russia’s disinformation campaign.

Emilio Iasiello 17, expert cyber intelligence consultant for many private and public institutions, author of numerous peer-reviewed books and journal articles, M.S. in Strategic Intelligence from the American Military University, June 2017, "Russia's Improved Information Operations: From Georgia to Crimea," *Parameters*, Vol. 47, No. 2, https://doi.org/10.55540/0031-1723.2931, RMax

Recommendations

The United States needs to address hostile information activities from its adversaries more efectively. As observed in the recent hacking scandals surrounding the US presidential election in which Russia targeted and, according to the US intelligence community, used information to disrupt and ultimately help its candidate of choice to win, the soft power most effective in confounding the United States is information itself, and not necessarily any production or dissemination technology.65 Given the fact that Russia spends approximately $400–$500 million per year on foreign information efforts, while the US spends $20 million USD on Russian language services, it is easy to see that the United States is far behind.66 Some recommendations to address this shortcoming include:

National counterinformation strategy and center. The United States’ offensive cybercapability is generally considered among the most sophisticated and powerful on the planet; however, as observed in efforts against the Islamic State, America has been less adept in countering online messaging despite substantial resources.67

In late December 2016, President Barack Obama authorized $611 billion for the military in 2017 and to establish a Global Engagement Center to track foreign propaganda and disinformation efforts undermining US national security interests.68 Little information on the development of this entity is available to date, although a similarly named center focusing on Islamic State messaging is headquartered in the State Department. Such a center should serve as a central, coordinating entity as well as model the operations of the National Counterterrorism Center, which maintains cross-government civilian and military representation and directly advises the Director of National Intelligence. Furthermore, this center needs to collaborate with national security stakeholders to develop unique strategies for each state and nonstate actor.

Protect against fake news. The rampant proliferation of fake news, such as observed during the US elections and annexation of Crimea, undoubtedly plays a pivotal role in Russian information operations.69 One initiative to help reduce fake news involves leveraging cutting-edge technology to help identify the fabrications as soon as they emerge. Artificial intelligence and data analytics can be used to detect words or word patterns that might indicate deceitful stories. In addition, the US government via the Department of Homeland Security should implement a strategy for educating the public as well as identifying and reporting fake news outlets in much the same way cyberscams are reported to the Federal Bureau of Investigation.

International engagement. The global nature of the Internet provides many outlets for disseminating legitimate and illegitimate information. A myriad of social media platforms can also be used to promote slanted news stories and propaganda via Internet trolls. Increasing international collaboration among law enforcement and intelligence professionals who specifically focus on these outlets will help agencies identify and disable these sources.

Conclusions

Applying information warfare theories in today’s geopolitical climate remains a work in progress. An around-the-clock news cycle and the various ways of disseminating and consuming information worldwide make implementing information-based operations and tailoring messaging against competing narratives challenges. As observed in Georgia, smaller nations can competitively control information and influence target audiences to at least mitigate the efforts of, if not defeat, larger nations.

Even after learning from its missteps in Georgia, Russia, did not gain many Ukrainian regions. Russia lost opportunities in Luhansk and Donetsk when Russian troops were unable to penetrate the regions promptly. Russia, however, appears to be guided by Gerasimov’s principle of refining information confrontation strategies by continuing to engage in various forms of official and unofficial messaging as well as perfecting the art.

One scholar of Russian propaganda refers to it as less of an information war as much as a war on information. Given the value Russia places on manipulating information, perceptions of the information space as potentially dangerous and a successful agent for ousting governments and influencing public opinion and behavior are understandable. A former KGB general stated the overall goal of Soviet Union propaganda was not far from the “subversion” pursued by Russia’s modern Internet disinformation campaign: “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 in Europe, Asia, Africa, Latin America, and thus to prepare ground in case the war really occurs.”

While the media has focused on offensive cyberattacks and disruptive efforts to cripple critical infrastructures and to impede public access to financial institutions and emergency services, Russia understands the potential power associated with influencing via cyberspace. As such, Russia continues to refine its online information operations against regional and international targets, outpacing the United States in nonoffensive cybercapabilities and demonstrating not all threats in cyberspace are written in binary.

## Advocates---Office of Strategic Narratives

### Solvency---Office of Strategic Narratives

#### The United States federal government should, via Executive Order, create and establish an Office of Strategic Narratives

Luke Karl et al. 18 (Maj. Luke Karl is an active-duty officer in the Air Force and a graduate of the Joint and Combined Warfighting School in Washington, D.C., Maj. Joseph Lane is an active-duty officer in the Army and a graduate of the Joint and Combined Warfighting School in Washington, D.C., Cmdr. David Sanchez is an active-duty officer in the U.S. Navy and a graduate of the Joint and Combined Warfighting School in Washington, D.C, 7-26-2018, "How to Stop Losing the Information War," Defense One, https://www.defenseone.com/ideas/2018/07/how-stop-losing-information-war/150056/, DOA: 6-22-2022//Smarx Ahsan)

**--- has some possible arguments to the DoS counterplan in here, but im not sure how topical this is.**

Russia “is waging the most amazing information-warfare blitzkrieg in the history of information warfare,” Gen. Philip Breedlove told NATO leaders at their 2014 summit. There’s no evidence that Moscow’s efforts have since slackened—nor that the United States is institutionally equipped to develop an effective response.

This was not always the case. During and just after the Cold War, the U.S. more than held its own in the sphere of information operations. And though the internet — and particularly social media — have greatly increased the speed and scale (and decreased the cost) of such operations, the experience of those years suggests a way to build and run an IO organization to lead them successfully.

From 1953 until 1999, the deployment and use of the nation’s information-warfare “instruments of power” were led and coordinated by the United States Information Agency, or USIA. The agency was created by President Eisenhower, a military veteran who understood the power of information and alarmed by the activities of the “psychological strategists of Communism.” Among other areas, USIA was created to lead America’s efforts in the field of public diplomacy — the effort to influence foreign audiences through messaging and organizations such as Voice of America. (Its creation was advocated by Secretary of State John Foster Dulles, who wanted his own organization to concentrate on traditional diplomacy.) USIA’s strategic communication and counter-propaganda efforts helped shore up Western resolve while exploiting cracks between Warsaw Pact governments and their populations.

Even after the Berlin Wall fell, USIA ably equipped policy-makers with international public opinion atmospherics, aided in countering extensive Iraqi misinformation campaigns, and managed messaging to media outlets during 1990-91’s Desert Storm and Desert Shield. During the Clinton administration, USIA again played a key role in consolidating and pushing strategic messaging to foreign media outlets and audiences in reaction to a 1993 agreement between Israel and the Palestinian Liberation Organization, galvanizing world opinion in support of the U.S. government’s role as a peace broker and pushing for continued progress. And as the 1995 Dayton Peace Agreement began to send U.S. military forces into and around Bosnia, USIA’s public-opinion polls in the region helped U.S. government leaders and organizations make policy decisions.

But desires to streamline the post-Cold War government bureaucracy, coupled with State’s desire to engulf the agency and its budget, made USIA an easy target. In 1999, it was folded into the State Department. As its advocates feared, a clash of cultures and the weighted importance of traditional diplomacy pushed public diplomacy to the backseat.

Within just a few years, the consequences of an absent information arm made themselves apparent. The 2003 Iraq invasion became known for its IO missteps — among them “Mission Accomplished” and “coalition of the willing.” The problems were compounded by general U.S. policy-maker naiveté toward Middle Eastern and global public opinion on U.S. military actions. A year later, the 9/11 Commission Report highlighted the deterioration of the informational instruments of power, noting the monopoly enjoyed by al Qaeda in the domain of Middle Eastern public opinion.

Skip forward to 2015, when former Director of National Intelligence James Clapper is telling the Senate Armed Services Committee that the U.S. government needs “a much more robust capability from the standpoint of the resource commitment to counter-messaging.” His proposed solution? A “U.S. Information Agency (USIA) on steroids.“

Congress responded by establishing the Global Engagement Center, an interagency office housed at the Department of State “to coordinate and synchronize counter-propaganda efforts.” Lawmakers allocated the new center $120 million to start up in fiscal 2017, but the Trump administration spent none of it. The GEC was to receive $60 million in fiscal 2018, but as of March had neither the funds nor enough staff to do its job.

Other parts of the U.S. government still do messaging, spending about $730 million annually on a wide range of international media operations. That is “a small fraction of what our adversaries are spending,” according to the chairman of the Broadcasting Board of Governors, which supervises Voice of America, Radio Free Europe, and other government broadcasters. Writes one independent security researcher, “The State Department estimates that the Kremlin's sophisticated influence campaign effort includes a $1.4 billion-a-year internal and external propaganda apparatus, claiming to reach some six hundred million people in 130 countries and 30 languages.”

The USIA’s key contributions during an earlier period of competition underline the need for a concerted, interagency approach to strategic information operations. Among the requirements is a direct link between policy-makers and the informational instruments of power. Its funding problems aside, the GEC is simply too peripheral.

What is needed is a new organization — call it the Office of Strategic Narratives — and the right institutional placement. It should be located within the National Security Council, under the existing Deputy National Security Advisor for Strategic Communications. This will give it a direct line to the president and equal footing with the departments that run the various U.S. messaging programs. This new office should include representatives from across the government, and purview over the GEC and the BBG.

The OSN would have responsibility for developing narratives and counter-narratives on issues of national importance for U.S. communications, based on bottom-up interagency reporting from across the information environment and guidance from the president via the National Security Advisor. Its roles would include leading the informational instruments of power, gauging public opinions, countering mis/disinformation, monitoring and reporting on the effects of adversarial messaging, monitoring the IE as a whole, and disseminating presidential policies and messages. As part of all this, it would coordinate with the DOD’s PSYOP and Public Affairs service members nesting of messaging efforts under accepted national strategic narratives — not unlike how some Combatant Commands operate. As well, the new office might eventually work with NATO partner-equivalent offices to share the costs and burdens in identifying and countering Russian mis- and disinformation.

Importantly, the OSN should be established by executive order, which would head off efforts by more senior agencies to protect their parochial interests by not relinquishing control of assets and budgets.

The importance of the information environment has never been more greater — nor the need to move beyond today’s half-measures and establish a strong and central organization to coordinate America’s messaging, counter-messaging, and instruments of informational power. Establishing an Office of Strategic Narratives in the National Security Council offers the chance to duplicate, or even exceed, the effectiveness of the Cold War’s USIA.

## Advocates---Countermeasures

### Solvency---OCOs

#### Cyberattacks on foreign disinformation buildings solve.

Justin Ling 22, journalist for VICE News, has written in Medium, The Guardian, Business Insider, MSN Canada, The Independent, and Canadian Broadcasting Corporation, 5/13/2022, "NATO Should Elevate Its Cyber Game, and Quickly," Centre for International Governance Innovation, https://www.cigionline.org/articles/nato-should-elevate-its-cyber-game-and-quickly/

When Moscow attacked Ukraine in February, President Vladimir Putin expected a quick victory.

Not only did the Kremlin have military superiority, but it planned a concerted cyber and information campaign to disrupt the Ukrainian state, galvanize support among Russophones, weaken Western resolve and convince Ukrainians that resistance is futile.

Much like its resistance in the streets and on the battlefield, Ukraine has put up a remarkable defence against Moscow’s unconventional warfare.

“I believe that this war has been going on, not since February 24, but since the beginning of 2014, when Russia first attacked us,” Mykhailo Fedorov, Ukraine’s forward-looking vice prime minister and minister of digital transformation, the man behind President Volodymyr Zelenskyy’s 2019 win, told me in April from a location near Kyiv. “And as such, we have had eight years to reform.”

But while Federov may have helped prepare Ukraine for this moment, Russia’s relentless efforts to destroy his country — and its evident resolve — mean the country needs further defences. Kyiv requires help that Western allied governments, including Canada, are in a position to provide.

The Kremlin’s Global Disinformation Network

Russia’s propaganda and disinformation apparatus is extraordinarily complex. Some outlets are fully state-run, some are merely state-funded, and others are operated at arm’s length by Putin-linked oligarchs. The system churns out conspiracy theories and whataboutism to aid Moscow’s objectives.

From the start of the all-out invasion on February 24, Russian disinformation has thumped on a series of narratives: that the North Atlantic Treaty Organization (NATO) posed a security risk to the Russian Federation; that Ukraine was run by neo-Nazis; that Ukraine is responsible for slaughtering civilians on its own territory.

Those narratives have, unfortunately, been somewhat effective in discouraging a unified response from NATO. They’ve influenced millions of Westerners and found purchase with far-right and Russophilic politicians the world over.

The most visible Western response to date has been the collective taking offline of Russia Today, or RT, the state-run television network.

Yet trying to ban Russian media is a mug’s game. Any outlets forbidden by law or suspended by the social media giants would simply jump to the Russian-founded social media platform Telegram, which abhors regulation.

Rather than playing whack-a-mole outlet by outlet, Ukraine’s allies would be better off exposing how these disinformation networks work.

Many of these social media pages, self-styled think tanks, blogs and media outlets are designed to look fully independent and authentic. Efforts by Twitter, Alphabet and Meta to expose them as disinformation have been inconsistent.

Berlin-based, Moscow-run video aggregator Ruptly is “state-affiliated media,” according to Twitter, but “state-controlled media” per Facebook; its“transparency” feature notes that the outlet’s page administrators are in three EU countries, but doesn’t name them.

Some smaller but perhaps more effective outlets — such as the French-language Donbass Insider, which has used manipulative practices to spread Kremlin disinformation on its Facebook page — carry no disclaimer at all.

Plenty can be done to identify and expose who runs these propaganda outlets. Western intelligence can help shed light on how they interact and fit in with Russian intelligence efforts. But social media companies also need to deny their advertising services to these state-controlled outlets.

“What’s the currency of disinformation?” Marko Suprun, a Kyiv-based host and producer, asked me recently. “AdSense.”

Google’s advertising platform will hardly make any disinformation agent rich. But Suprun says it has created “a bit of a cottage industry — they make enough money to survive.”

If the companies drag their feet — in particular, those companies that have suspended operations in Russia but haven’t closed up shop entirely — moving to publicly shame them could be quite effective, as Kyiv has shown.

“What we’re trying to emphasize is that there are no grey areas here,” Fedorov told me. “This is basically as good-versus-evil as it gets. So, you either choose the path of good, and you stop operations in Russia and you help fight disinformation. Or you choose the path of evil and you stay in Russia and you pay taxes, which can, potentially, be used to fund the army that’s murdering civilians.”

Why Have a Cyber Command if You’re Not Going to Use It?

When the Islamic State used its al-Hayat Media Center to recruit Westerners to its cause, a US-based coalition bombed the group’s propaganda hubs and hacked its websites. Launching airstrikes in Moscow is obviously not an option. But that doesn’t mean NATO can’t take these stations offline. After all, Russian disinformation and hacking have targeted democratic systems and added fuel to extremist movements in the West.

Ukraine has already taken the fight to Russia’s doorstep. Aggressive distributed denial-of-service (DDoS) campaigns have knocked offline various elements of the Russian state. A well-trained “IT Army,” as Fedorov dubs it, has hacked major state companies and dumped the personal information of their employees and operations.

For years, NATO has been skittish about deploying its newly beefed-up cyber capacities, treating such powers as akin to missile strikes or active warfare. Ahead of NATO’s upcoming June summit, there are calls to come up with a more flexible policy on cyber operations. Giving member countries the freedom to target infrastructure used for malicious cyber or disinformation activity would be a great place to start.

In effect, NATO countries should have the flexibility to degrade Russia’s ability to launch information and cyber operations against Ukraine and the West. That doesn’t mean launching an operation that could be considered an act of war, such as knocking a power plant offline (something Russia has done both to the United States and Ukraine). It could mean, however, launching DDoS attacks on Russian websites, or attempting to spearphish access to a Telegram channel linked to the Wagner Group, a quasi-private military contractor. Those operations would be both proportionate and plausibly deniable.

The West also needs to help Kyiv continue its fight.“We, of course, need communications equipment, mostly satellite equipment — including, but not limited to, Starlink terminals,” Fedorov told me. “So that we can basically ensure connectivity whenever we can.” And, he says, although Ukraine has already been given a significant number of workstations, laptops and tablets, it needs still more.

Not all Kremlin support originates in Russia.

As a 2020 report from the US Department of State notes, an incredibly useful hub for Russian disinformation is the Canada-based “Centre for Research on Globalization.” The website, the report notes, boasts a “large roster of fringe authors and conspiracy theorists [that] serves as a talent pool for Russian and Chinese websites.”

Conspiracy theories that pop up on sites like these — such as the notion that Moscow is striking Ukraine to destroy US-funded biolabs similar to the equally fictional ones that other conspiracists claim gave us COVID-19 — have been adopted wholesale by Moscow.

Western intelligence agencies are aware, or should be aware, of the level of involvement these hubs have with the Russian state. That State Department report is a great first step toward declassifying far more intelligence than is currently done. Washington and London have started along that path, but all NATO members should engage — in both countering falsehoods and explaining to the world how Moscow creates, supports and amplifies them.

### Solvency---Countermeasures

#### The plan’s countermeasures based on the “Four Lines of Defense” acts as a test case for further cooperation.

Jakub Kalenský 22, Senior Fellow at the Atlantic Council's Digital Forensic Research Lab, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 172-188 (under ch. titled, “Chapter 7: How to Defend Against Covid Related Disinformation,”) //chico

7.5 Four Lines of Defense

Currently, there appear to be four basic “lines of defense” when countering hostile information operations.

1. Documenting the threat, in order to collect more data on the threat and gain a stronger understanding of the threat in the information environment.

2. Raising awareness about the threat to broaden the audiences that are aware of it and, thus, are inoculated against it. In contrast to the first line, which seeks to obtain more information about the threat, the second line attempts to ensure that more people have at least basic information about the threat.

3. Repairing, mitigating, and preventing weaknesses found within the information system, in order to decrease the ease of exploitation for attackers and to make their target smaller and harder to hit. This line of defense should mitigate effect of the threat on the target.

4. Limiting, challenging, constraining, punishing and deterring information aggressors. This line of defense, unlike those prior, is not directed at the victims of information aggression, but aims to decrease the aggressors’ desire to be aggressive instead.

Within each of these lines of defense contain various tactical countermeasures that can be undertaken. To underline the caveat above, none of these measures will solve one hundred per cent of the problem. However, this does not mean that the given measure is necessarily useless—it merely means that we need to be applying more such measures, which constantly adapt and evolve with the changing infor- mation environment and aggressors. It is critical to act and adapt to disinformation, providing space to develop lessons learned from efforts to counter disinformation versus searching for ideal counter measures which can be unattainable. The subse- quent section will discuss the tactical countermeasures relevant to each line of defense one by one.

#### Documentation is an imperative otherwise we’re fighting in a fog.

Jakub Kalenský 22, Senior Fellow at the Atlantic Council's Digital Forensic Research Lab, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 173-177 (under ch. titled, “Chapter 7: How to Defend Against Covid Related Disinformation,”) //chico

7.5.1 Line 1: Documenting the Threat

Documentation is the imperative first step without which almost nothing else is possible; and at the same time, still a measure that is gravely underestimated. It is necessary to document: the channels involved in spreading disinformation, the disinformation narratives themselves and how they change with time, how such information travels from one medium (e.g., language, platform, “filter bubble”, etc.) to another, the actors involved in proliferating them (both knowingly or not), and the effect that such disinformation has on given audiences. While this task may sound relatively straightforward, unfortunately, to date, this task has not, and is currently not, being dealt with properly. There are still many questions that we do not have answers to, which means that we are fighting in a fog, not knowing what we are standing up against.

The pioneer of systematic, day-to-day documentation of disinformation in the twenty-first century is the Ukrainian project StopFake.7 This project started right after the Anschluss of Crimea by the Russian Armed Forces, and centers on exposing and refuting Russian disinformation campaigns abroad. The project’s focus is specifically on disinformation campaigns targeting Ukraine, but StopFake has also debunked disinformation surrounding other countries or individuals.

The process of debunking may sometimes be quickly dismissed as too laborious, or as a “whack-a-mole” approach. There is also an incorrect, though unfortunately relatively popular, myth that debunking strengthens, rather than weakens, disinfor- mation efforts (Global Engagement Center, 2020c; Swire-Thompson et al., 2020). However, in order to be able to label a piece of information as disinformation, it is necessary to fact-check the given story and to identify whether and where, if at all, the piece distorts reality, i.e., refute the disinformation piece, debunk it. There is no other way to identify disinformation. Without the process of debunking, it is not even possible to have a conversation about disinformation, let alone to appro- priately document instances of disinformation. Without the documentation of cases of disinformation, there are no facts on which a decision or future learning may be based.

Documenting disinformation, no matter how underestimated or dismissed, is the imperative first step towards countering disinformation, without which nothing else could be done in an informed and verifiable manner. It is no coincidence that much of the misunderstanding and underestimation of disinformation campaigns and how to counter them comes from individuals and organizations who have never undergone this critical first step. It is also not unusual that those experienced with the vast disin- formation ecosystem often have to point out that their respective societies continue to underestimate the scope of Kremlin disinformation and propaganda.8

StopFake’s approach to countering disinformation has been emulated around the world. After the Kremlin’s Anschluss of Crimea and the renewed Russian information aggression that followed, NATO has created a factsheet called “Setting the Record Straight” (NATO, 2020), which debunks some of the most notorious disinformation narratives spread by the Kremlin and its disinformation ecosystem. Since 2015, the EU’s counter-disinformation unit, the East StratCom Task Force (EEAS, 2021), has been publishing its “Disinformation Review”, a project that documents pro- Kremlin disinformation,9 and has since evolved into the EUvsDisinfo campaign. As of April 2021, the Task Force collected over 11,000 cases of disinformation, which are presented within a searchable database10—so far, the only such database of its kind in the world.

However, the work of EUvsDisinfo also indirectly shows us how much we are missing. As of spring 2021, Brussels has not replicated this model beyond addressing pro-Kremlin disinformation campaigns. There is no such project, for example, that documents disinformation originating in China.11 Rather, the coverage of Chinese Communist Party disseminated disinformation seems to be based on the work of non- EU researchers and journalists, as opposed to the EU’s own data set (EUvsDisinfo, 2020b). Similarly, hard data about disinformation campaigns such as that of ISIS, or other so-called domestic actors, are not provided by the EU.

The refuting and documenting of disinformation is also done by think tanks, NGOs and civic activists. The Atlantic Council’s Digital Forensic Research Lab focuses on “identifying, exposing and explaining disinformation using open source research”12 and in 2021, the team presented a report on COVID-related disinfor- mation (DFRLab, 2021). The Prague-based European Values Center for Security Policy (European Values) exposes “Russian influence and disinformation operations focused against Western democracies.”13 The Lithuanian “Elves”14 kick-started their counter-trolling efforts following the Russian invasion of Ukraine. Through their cooperation with established media and information technology and artificial intel- ligence (AI) experts, a unique system dubbed Debunk.eu has been built (Global Engagement Center, 2020a). Debunk.eu combines an algorithm which identifies potential disinformation stories with robust manpower to verify the information pinpointed by the algorithm, i.e., fact-checking and setting the record straight (Delfi, 2020). The Czech company Semantic Visions also uses AI to monitor the spread of disinformation stories (Semantic Visions, 2020).

The Czech version of the “Elves”15 are documenting what is happening across disinformation-oriented outlets, and also across non-public channels that spread disinformation, including chain emails (which are still popular among the elderly population in the region; EUvsDisinfo, 2017a). Researchers in Ukraine have docu- mented the rise of pro-Kremlin disinformation that has penetrated some of the country’s most popular Telegram channels (Velychko, 2020). Infiltrating such groups that use closed channels of information is probably best done by actors within civil society, rather than by formal institutions (governments and other such organizations would be susceptible to accusations of “Big Brother”-like espionage). Apart from the work undergone by the public sphere, there are also institution- and government- level efforts underway (Pogrund, 2020). This work, though sometimes very high in quality, may be limited in impact if the work remains non-public.

Even though there are already a few initiatives working on documenting and refuting disinformation, there are still many crucial questions that remain unanswered. For example:

• How many disinformation channels are there? Is their number increasing or decreasing? How many new channels have appeared in the last week/month/year?

• How many messages do these channels spread on a daily/weekly/monthly basis?

• How many people do these messages target and reach?16

• How many people believe the messages of each given disinformation campaign?

(because, hypothetically, the decreasing numbers of the disinformation narratives or channels does not necessarily mean that the campaign would be less successful, it can just mean it is evolving into a more effective stage, doing the same job with less resources)

Without answers to these questions, we remain fighting in a fog. We are in a situation akin to a country that has been attacked by an outside aggressor but does not have even the remotest of ideas about how many soldiers, tanks, jets or missiles the enemy has in their arsenal, or even how many people per day they succeed in killing.

In addition to this, without having the answers to these questions, we cannot address other crucial questions. Following every major incident that the Kremlin has lied about, many researchers and civil servants receive the same question: Has there been an increase in disinformation? The issue here is that, if we are not properly measuring the extent to which disinformation is present during the uneventful, or “calm”, periods, we cannot begin to address a potential increase, or lack thereof, following major events, or “hot” periods. We do not know what the baseline is and, therefore, we cannot talk about deviations from the baseline, empirically speaking at least. We cannot answer questions about the potential success, or lack thereof, of various disinformation campaigns, either, if we do not have empirically certain data about them. Essentially, there is an unknown, but powerful, force influencing our audiences, and we cannot say how big or how dangerous it actually is.

We are in a situation in which we see but the proverbial tip of the iceberg, without having a clue as to whether we are aware of ten or only one per cent of the problem. We need to be designing various solutions to address one hundred per cent of the problem. Finding any missing information as soon as possible should be the imper- ative. Governments should be taking the lead or, at the very least, be providing the necessary funding for relevant third-party actors, as many civil society organizations do not have sufficient resources for adequate monitoring.

Aside from trying to document disinformation campaigns as exhaustively as possible, we also need to document the success, or lack thereof, of each given campaign, while answering the following question: “How many people believe each disinformation message?” Unfortunately, the work that is being done to address this question is quite sporadic and less systematic than required.

The question surrounding the impact of disinformation campaigns is one of the most difficult in the field. Disinformation expert Ben Nimmo, the head of Global Threat Intelligence Strategy at Facebook, has developed a model based on whether information remains on one platform, or travels across multiple, and whether this information similarly remains in one community, or spreads across many (Nimmo, 2020). Other researchers have measured the engagement rate of specific disinfor- mation narratives on social media, often concluding that disinformation frequently beats true information in this respect (Dizikes, 2018; RFE/RL, 2020a).

Another option is to measure how many people believe a particular disinforma- tion campaign via opinion polls—because it is highly probable that the information aggressors are more interested in turning peoples’ hearts and minds, rather than in engagement numbers on social media. This method is more precise in the cases where we know that a particular message would never be in the information space if it had not been introduced by various information aggressors, such as the pro-Kremlin disinformation campaign surrounding the crash of flight MH17, or the poisonings of Litvinenko, Skripal and Navalny. In instances where a particular disinformation campaign builds upon pre-existing conditions, such as low trust in authorities or fear of various socio-economic groups, it is hard to distinguish between the impact, or lack thereof, of the campaign itself, as opposed to other factors. That being said, this can still provide valuable data to consider for policy makers or opinion leaders dealing with the information space.17

A cause for concern is the tendency for significant numbers of the population in several European countries to fall for disinformation narratives (Shutov, 2020). For example, even in a country like Ukraine, where the level of awareness about the Kremlin’s disinformation campaigns is very high, there remains a significant part of the population that believes disinformation narratives that would not appear within the information space if not for the pro-Kremlin disinformation ecosystem (EUvsDisinfo, 2017b). Unfortunately, at present, there are no individual actors or organizations, public or private that are conducting regular opinion polls on the subject.18

As of yet, we do not have consistent, reliable, and replicable information about the potential successes of these disinformation campaigns. Not only does this mean that we are uncertain as to how big the threat is that we face, we also cannot reliably measure whether our countermeasures work (i.e., whether the number of people believing various disinformation narratives have decreased).

Documenting the threat of disinformation may seem like a measure that is critical only after a given event or campaign has occurred but, in fact, this measure can be of use even during an ongoing disinformation campaign. Following the poisonings of Sergei and Yulia Skripal by Russian secret service agents, the British govern- ment documented and exposed the various conflicting, constantly changing narra- tives spread by the Kremlin as they appeared (Dettmer, 2018). In so doing, the British government was swift and consistent in its response to the disinformation, and the conflicting messages and lies spread by the pro-Kremlin disinformation ecosystem were exposed (EUvsDisinfo, 2018b). A simple timeline of the various messages spread by Kremlin’s propaganda bullhorns made it obvious as to the deception at play.19

#### Raising awareness is paramount. Civilian awareness substantially hinders misinformation campaigns effectiveness.

Jakub Kalenský 22, Senior Fellow at the Atlantic Council's Digital Forensic Research Lab, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 172-188 (under ch. titled, “Chapter 7: How to Defend Against Covid Related Disinformation,”) //chico

7.5.2 Line 2: Raising Awareness About the Threat

Documenting the threat is the first step to countering systematic disinformation campaigns, and the raising of awareness afterwards, by making use of the data collected, is the natural continuation of this first step. Projects such as the DFRLab (Atlantic Council), EUvsDisinfo (EU), and Kremlin Watch (European Values) are not only documenting cases of disinformation, but are also publishing relevant arti- cles and reports, as well as providing training and briefings for governments, media, and the academic community. However, there is a limit to these organizations’ reach. Irrespective of whether the actor is governmental or non-governmental, neither can reach nor persuade an audience in full—they each have a limited target audience. It is necessary not only to collect more data about disinformation campaigns and to educate one’s own audience about the threat, but also to constantly broaden the audience that receives that message.

In addition to the organizations mentioned above, the Swedish Civil Contingencies Agency (MSB) created a handbook for civil service communicators intended to help them counter information influence activities (MSB, 2019). A similar effort was initiated by the UK government (UK Government, 2019). The MSB and the Security Service Säpo have also been briefing politicians and media in Sweden (EUvsDisinfo, 2018c). The Czech Center for Countering Terrorism and Hybrid Threats is also focusing on educating the country’s civil service about hybrid threats, including disinformation (Ministerstvo vnitra Cˇ R, 2016). In some countries, it is the secret services that provide excellent information on the threat, and their materials are highly valued by the expert community and the media—see e.g., the annual reports of the Estonian KAPO,20 or the Lithuanian National Threat Assessment.21

The NATO StratCom Centre of Excellence (CoE) in Riga publishes reports on the topic of disinformation and strategic communication.22 They also organize confer- ences targeted at civil servants and experts dealing with the topic. The CoE also provides briefings and training for governments in NATO’s member countries. The joint EU-NATO Hybrid CoE in Helsinki is working in a similar manner.23

Ideally, increasing awareness on a given disinformation campaign or narrative may help to mitigate or dispel a false story before it has time to spread. A compar- ison between the infamous “Lisa case” in Germany with its Lithuanian counterpart demonstrates the difference between how a disinformation campaign plays out in a country aware of the threat, versus in a country where this awareness is not very high. The Lisa case took place in Germany in January 2016 (Meister, 2016). A 13- year-old girl from a Russian-speaking family, upon not making it home in time for her curfew, told her parents that she had been raped as an excuse. While she later admitted that the story was false, and the German authorities confirmed this, pro- Kremlin media and activists in Germany ignored this and continued to spread only the original falsehood. This resulted in demonstrations and a public denunciation by Russian Foreign Minister Sergei Lavrov of the German authorities, accusing them of a cover-up (McGuiness, 2016).

By contrast, a year later, a similar fake story in which an underage girl was allegedly raped appeared in Lithuania, failed completely (Schultz, 2017). This was in large part due to the Lithuanian Armed Forces’ StratCom team’s preparation of the country’s civil servants and local authorities for such attacks, which had been anticipated prior to the NATO Enhanced Forward Presence exercise in the country. Local authorities, once having registered the falsity of the planted story, alerted the StratCom team, which quickly debunked it and alerted all relevant stakeholders. The first Lithuanian media coverage on the subject was not “a little girl allegedly raped”, as with the German counterpart, but rather “another information attack against Lithuania”. An extremely high awareness of disinformation campaigns in the country, as well as a timely exposure of the false story (which by definition had to involve the often-dismissed debunking of the story), resulted in one of the most instructive success stories in the entirety of the EU thus far.

However, given the fact that audiences today are more fragmented than ever before, it is necessary to move beyond the small circle of government officials and experts focused on the topic, and try to raise the awareness among broader audi- ences as well. One proven way to attract wider audiences is through humor. In fact, the ridiculous nature of some of the falsehoods spread by disinformers may provide a lot of ammunition for jokes and ridicule. The tweet by the Canadian Permanent Representation to NATO, which ridiculed Russia’s repeated “mistakes” regarding geography, has already become well-known (@CanadaNATO, 2014; Burtch, 2018). The official account of the Ukrainian presidential office mocked the Kremlin’s propa- gandistic appropriation of Ukraine’s history as being a part of Russian history with a GIF from The Simpsons (Thomsen, 2017). The EUvsDisinfo project has a rubric for lighter, sarcastic pieces that make fun of recent propaganda.24 Taiwan’s Prime Minister has also used funny memes directed towards COVID-related disinformation (Yang, 2020).

Interestingly, research shows that act of ridiculing can work well with general audiences, although it is not advised when appealing to conspiracy theorists (Lewandowsky & Cook, 2020). In spring 2021, EUvsDisinfo published a specialized guide to communicating with those who believe the COVID-related conspiracy theo- ries (EUvsDisinfo, 2021a). The US State Department’s Global Engagement Center (GEC) details the use of a “counter-brand approach”, in which those countering disinformation should not refute every single false claim, but rather point out the untrustworthiness of the source spreading disinformation, thus reaching broader, mainstream audiences (GEC, 2020b).

Notably, professional influencers are likely the most effective at broadening their audiences and reaching beyond the typical filter bubbles of civil servants and NGO activists. One such success story once again takes place in Lithuania; a local TV journalist, Andrius Tapinas, launched a show named “Hang in There” (Schearf, 2017), in reference to the ridiculed response of then Russian Prime Minister Dmitry Medvedev to a Crimean pensioner who confronted him about the low pensions in Russia (RFE/RL, 2016). As Tapinas himself describes, the aim of the show is to make fun of the Russian government and politics. In the Czech Republic, the Youtuber known as Kovy has filmed a series of videos aimed at increasing media literacy among the country’s younger generation, as well warning about the dangers of manipulated information (Jeden sveˇt na školách, 2019). Kovy’s primary audience are Czech youth—an audience primarily untouched by both government, NGO and CSO initiatives on the project.

It must be acknowledged that some methods of communication may work effec- tively for only a part of a given audience and may be ineffective for another—but this is not a justification to stop implementing these various methods. As journalist Anne Applebaum documented prior to the onset of COVID-19 in Italy regarding the anti- vaccination disinformation campaign, different approaches to raising awareness of a threat will reach and impact different people, but this does not make one approach better or worse than another (Applebaum, 2019). Efforts towards finding new opinion leaders to reach new audiences should never stop—there is always a means to make a given message resonate.

## Advocates---AI

### Solvency---AI Controls

#### AI is a two-edged sword---it both magnifies next generation disinformation and is key to combat it. The plan’s coordination of efforts between the government and the private sector ensures it’s effect is mitigated.

Katarina Kertysova 18, George F. Kennan Fellow at the Kennan Institute of the Woodrow Wilson Center, policy fellow with the European Leadership Network, 2018, “Artificial Intelligence and Disinformation How AI Changes the Way Disinformation is Produced, Disseminated, and Can Be Countered,” *Security and Human Rights*, 29, pp. 55-81, <https://doi.org/10.1163/18750230-02901005>, RMax

5 Conclusions

As the volume of online content continues to grow, automated fact-checking holds great potential as a speedier and cost-efficient complement to, or even replacement of, human oversight – by blocking or removing false content before it is uploaded online. It might take another five to ten years for AI to make nuanced distinctions and proactively identify harmful content embedded in linguistic, cultural, and political contexts with minimal to no human input.116 For as long as AI does not grasp context and grey areas, human supervision remains critical. As regards their accuracy, detection algorithms need to be further developed to reach the efficiency level of e-mail spam filters.

As this paper demonstrates, the development of AI systems is a two-edged sword for democratic societies. On the one hand, AI systems will improve human processes and tasks in the online environment, such as detection of disinformation, bots, altered text and images, and manipulated audio and video material. On the other hand, when the same technologies are adopted by adversaries, they will enable them to magnify the effectiveness and scale of information operations. As ideological and geopolitical tensions between democratic and authoritarian states continue to grow, AI and computational propaganda are likely to become tools of political warfare used against democratic societies.

There needs to be a greater global effort to work on ways to detect and respond to AI-generated content. Policies aiming to combat false and harmful content should already be focusing on the next generation of disinformation which, fuelled by advances in AI and decentralised computing, promises to spread faster, to be more sophisticated, and harder to detect.

New technologies evolve far quicker than government policies and often undermine existing legal and policy frameworks. In order to ensure responsible use of AI, as well as to develop the right responses for its potential misuses early on, stronger connections, partnerships, and open conversations need to be established between policymakers, engineers, and researchers.117 Acknowledging that technology companies, including social media platforms, can provide powerful solutions, governments and other stakeholders should strive to cooperate with them in order to develop better filters to prevent the spread of disinformation. Broader ex-ante consultation with online platforms, users, and other stakeholders would help prevent pitfalls such as unrealistic legislative proposals, a lack of balance in the distribution of responsibilities, and regulation or infringement of freedom of expression. Enhancing dialogue between relevant stakeholders will generate more realistic and agile policies.

## Security Cooperation/DOD Key

### DOD/Military Key

#### Military resilience is key---info warfare shuts down readiness and deterrence.

Alicia Wanless 18, director of the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace, Ph.D. researcher at King’s College London; and Michael Berk, Visiting Research Fellow with the Centre for Cyber Security and International Relations at the University of Florence, 3/27/2018, "For Every Action There is an Information Reaction: How Exercises Need to Adapt in a Digital Age," https://thestrategybridge.org/the-bridge/2018/3/27/for-every-action-there-is-an-information-reaction-how-exercises-need-to-adapt-in-a-digital-age, cy + RMax

The internet, social media, artificial intelligence, and other digital technologies are enabling the manipulation of the information environment for strategic purposes. Global hyper-connectivity and increasing competitiveness have propelled information warfare as a viable means of achieving strategic objectives—but what its theory and practice means can vary from military to military and expert to expert. Indeed, a lack of universal definitions, combined with a desire by military thinkers to carve things up into military domains and focus on hardware and technology, has left the role of information in the context of 21st century warfare insufficiently examined. This article, building on a previous one entitled "The Strategic Communication Ricochet," considers why information is more than a domain, and how military exercises must be adapted accordingly to foster increased resilience to information warfare.

The idea that information can be used in conflict is not new—great military strategists such as Sun Tzu, Machiavelli, and Clausewitz all emphasized using information to outmaneuver an enemy.[1-3] Despite an historic awareness of information in warfare, finding an internationally accepted definition of information warfare has been a challenge. Part of the problem is the word information itself—which can encompass many things. For example, one meaning as provided by the Oxford Dictionary is “data as processed, stored, or transmitted by a computer”—this could entail everything from code to content.[4] This understanding has been reflected in some military materials, such as the U.S. handbook on Inform and Influence Activities, which breaks the information environment out into three dimensions:  the physical (e.g., infrastructure), informational (e.g., data) and cognitive (e.g., values, beliefs).[5] Such scope, however, means that information is actually integrated into nearly everything a military does—from command and control functions to public affairs. Yet, information activities are often treated as something stand alone, or unrelated to more traditional military domains. Moreover, when it comes to the cognitive dimension of information in particular, there is an emphasis on outgoing communication with little attention to how such content will be twisted and used by adversaries against the sender to negatively affect leadership and decision-making.

What is lacking at the moment, both conceptually and from a strategic perspective, is an understanding for what information has become, and how every action, from those of the top general at headquarters to those of a private in theatre, carries with it challenges and opportunities for friendly strategic communication as well as adversarial exploitation. The ways information can be shaped demands that each activity during mission planning and corresponding exercises be reimagined for its cascading exploitative potential—which means looking far beyond the basics of public affairs or social media messaging in training scenarios.

Despite the changing information environment, most military doctrine focuses only on outgoing communications, and practitioners conduct military exercises as Ian Kippen notes in a recent Small Wars Journal article, in a linear fashion putting greater emphasis on later phases of operational preparedness (such as defend, restore, and transition).[6] Such an approach leaves the most critical first phase (deter) aiming to avoid conflict entirely, or create a more favorable starting position for later fighting, less practiced. However, this is precisely the phase where manipulation of the information environment by an adversary would occur, enabling them to mislead friendly leadership and deny time and opportunities for preparation and coordination of activities. As it stands, most operational exercises fail to integrate information activities in a meaningful manner into all phases of training, particularly the early planning stages. As a result, while information and strategic communication activities are continuously generated in support of other operations, there is no fostering of the necessary understanding for the role of information in modern warfare at all levels of military or relevant supporting agencies within and outside of government.

NATO notes on its website that “exercises are important tools through which the Alliance tests and validates its concepts, procedures, systems and tactics. More broadly, they enable militaries and civilian organizations deployed in theatres of operation to test capabilities and practice working together efficiently in a demanding crisis situation.”[7] Arguably, in a digital age, militaries and their partners must also do all of this within a complex information environment, and as such, training must adapt to develop appropriate skills beyond specialist units. Ultimately, these findings should bring about several key changes in how the military structures their training exercises.

#### Military susceptibility to disinformation risks compromising US and allies deterrence capabilities

Dr. Ritu Gill 22, Ph.D. in Social Psychology from Carleton University, section head at the Defence Research and Development Canada Centre for Operational Research and Analysis; Dr. Meghan Fitzpatrick, strategic analyst with Defence Research and Development Canada Centre for Operational Research and Analysis; and Jennifer Giles, communication and operations officer in the US Marine Corps, instructor at the Marine Air-Ground Task Force Staff Training Program, 2022, “Information Warfare: Lessons in Inoculation to Disinformation,” *Parameters*, Vol. 52, No. 1, pp. 105-118, https://doi.org/10.55540/0031-1723.3132, RMax

Armed Forces and Disinformation

Like the nation it protects, the US military is increasingly diverse. Women made up 16 percent of the active-duty force in 2017, and ethnic minorities currently comprise 42 percent of military personnel.20 This diversity can leave the military, like the country at large, vulnerable to disinformation campaigns. These campaigns represent a serious challenge to operational security and the overall cohesion of the armed forces, their allies, and the wider defense community.

For example, adversaries have consistently targeted the forces making up NATO’s Enhanced Forward Presence in Estonia, Latvia, Lithuania, and Poland. In 2020, Russian-sponsored actors released a forged letter online where Polish Brigadier General Ryszard Parafianowicz appeared to criticize openly the American presence in his country during the US-led exercise DefenderEurope 20. During the same exercise, Russian sources also claimed the US military had ignored COVID-19–related travel restrictions, even though US officials had reduced the size and scope of Defender-Europe 20 due to public health considerations.21 The threat of influence no longer exists only during deployment but also in garrison because of “the collapsed nature of communication . . . and . . . porous boundaries between war and everyday life,” which means geography is no longer enough to act as a defense.22

Hostile actors consistently target members of the US armed forces and veteran communities online. Beginning in 2017, Vietnam Veterans of America, a congressionally chartered nonprofit organization, began a two-year investigative study and discovered, “persistent, pervasive, and coordinated online targeting of American servicemembers, veterans, and their families by foreign entities.”23 The report demonstrated servicemembers and their social networks are vulnerable to disinformation. Foreign entities see members of the military community, who often have access to confidential and classified materials, as an attractive target. What is more, active members and veterans are a significant influence demographic in US political life. A team of Vietnam Veterans of America researchers inspected hundreds of Facebook pages and social media accounts and found American servicemembers, veterans, and other social media followers of several veterans organizations were specifically targeted by foreign entities.24 They also found individuals from over 30 countries administered the sites they reviewed, and that administrators of these imposter Facebook pages infiltrated other public and private groups.

Imposter pages and accounts built a following by impersonating legitimate military and veterans groups, like the Vietnam Veterans of America, and used camaraderie and community as a way to attract new members. This activity was so prolific Facebook shut down a third of the reviewed accounts for inauthentic behavior or “misleading actions to deceive others about who an individual/group is or what the individual or group is doing.”25 Before the shut down, the pages drew over 32 million users. Foreign administrators had used the platforms to “try to drive wedges between groups along varying racial or ethnic identities or prejudices, often pitting law enforcement against minorities.”26 This action frequently involved posting divisive content designed to polarize group members, from sharing pictures of NFL quarterback Colin Kaepernick to spreading false information about controversial public figures like Congresswoman Alexandria Ocasio-Cortez and posting xenophobic statements like “VETS BEFORE ILLEGALS” to play on sensitive topics like immigration.27 Disinformation targets fault lines within a society, and military personnel are not immune to these tactics.

Adversary disinformation campaigns undermine servicemembers’ ability to discern fact from fiction. These campaigns penetrate their social networks and make them susceptible to conspiracy theories and extremist groups, which degrades unit cohesion and presents a real force protection threat. Although there are no indications an adversary was directly responsible for the US Capitol attack of 2021, years of influence operations culminated in a distorted cognitive environment—an alternate reality—for many who participated in the riots, and implanted a lasting social and political division that could continue for years.28 Using the attack as an example, adversaries will continue active disinformation campaigns and employ all information domain tools to exacerbate discord and strengthen their position.29 Russia has used digital media to fan the flames following the Capitol attack, and China’s media has taken the opportunity to create false equivalencies to justify its behaviors and undermine faith in democratic processes and US legitimacy as a global leader.30

These effects offer clear evidence online conspiracy theories and disinformation do not remain online only but can and do culminate in violence. While disinformation is insidious and creates long-lasting effects at the national, strategic, and tactical levels, it can be mitigated through awareness and education.

#### The Defense Department needs to take action on information warfare --- Russia Proves

Tonya Riley 21 (Tonya, Technology and cybersecurity policy researcher, 4-30-2021, "Analysis," Washington Post, https://www.washingtonpost.com/politics/2021/04/30/cybersecurity-202-defense-department-isnt-armed-combat-growing-threat-information-warfare-experts-warn/, DOA: 6-22-2022//Smarx Ahsan)

National security experts will warn Congress today that the U.S. government isn't doing enough to fight back against the growing national security threat of information warfare aimed at sowing distrust in the U.S. government at home and abroad.

“Cyber-enabled disinformation, whether domestically or foreign generated, is a national security problem, corroding our democracy and governmental institutions, and threatening our public health and, potentially, public safety,” former NSA general counsel Glenn Gerstell will testify in front of the House Armed Services subcommittee on cyber, innovative technologies and information systems.

Other witnesses include Nina Jankowicz, a disinformation fellow at the Wilson Center; Herb Lin, senior research scholar at the center for international security and cooperation at Stanford University; as well as Joseph Kirschbaum, director of the defense capabilities and management team at the Government Accountability Office.

The hearing underscores how the United States has struggled to combat the emerging cyberthreat of information warfare.

The rise of social media and other emerging technologies has enabled foreign adversaries to escalate their offenses in recent years. Russia and other adversaries relied on social media, bots and data leaks to stir up trouble in both the 2016 and 2020 elections. In 2019, the FBI became aware that Trump campaign advisor Rudolph W. Giuliani was the target of a Russian influence campaign, as Ellen Nakashima, Shane Harris and Tom Hamburger scooped yesterday. The warning reflects a broader concern by U.S. intelligence about Russia's influence operations during the election, they wrote.

The U.S. intelligence community warned that “Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities,” in its annual worldwide threats report earlier this year. Other adversaries, such as China and Iran, are also stepping up their information warfare, the report warns.

Engagement in information operations also isn't limited to election cycles: China and Russia launched disinformation campaigns around the coronavirus. Experts say that kind of interference will only get worse.

But so far the United States has failed to respond to those escalations with an integrated government approach, Jankowicz says in her written testimony.

“Rather than organizing crosscutting, proactive, whole-of-government responses, we have mostly stood up ad hoc capabilities only when necessary, such as election war rooms before events like the 2018 and 2020 elections,” she writes.

#### Military cooperation with NATO is key---resources and expertise.

Glenn Alexander Crowther 17, Senior Fellow with the Transatlantic Defense and Security Program at the Center for European Policy Analysis, “The Cyber Domain,” *The Cyber Defense Review*, Vol. 2, No. 3, <https://www.jstor.org/stable/pdf/26267386.pdf>, cy

In addition to the Three Warfares, China has made advances in conceptualizing “strategic information war”. This concept “refers to the use of information and information technology in the political, economic, (science & technology), diplomatic, cultural, and military arenas to secure information advantage. In this broad sense, information war spans military and civilian spheres, peacetime and wartime, and has a global nature.” [35]  Although there are a variety of names for the Russian approach, the most accurate appears to be “new generation warfare” which “is manifested in five component elements: political subversion, proxy sanctuary, intervention, coercive deterrence and negotiated manipulation.” [36] Together these two approaches provide a significant threat to the United States, NATO Allies and like-minded partners around the world. This means that we all need to be competing in the information space. Information competition is so important that the Chairman of the Joint Chiefs of Staff recently designated “information” to be a joint function, co-equal with the existing joint functions of command and control, intelligence, fires, movement and maneuver, protection, and sustainment. [37]

The military has five functions that partially exist in the information environment and seven that exist entirely within the environment: Information Operations (IO), Military Deception, Psychological Operations (PSYOPs, also known as Military Information Support Operations or MISO), Public Affairs, and Strategic Communications are entirely within the environment. Communications & Signals, Cyber, Electronic Warfare (EW), Intelligence, Space operations and Operations Security (OPSEC) exist partially within. Physical operations also have an information effect, as when a US Army unit goes to a firing range in eastern Poland. All of these functions are legitimate military operations within cyberspace.

Conventional information operations are the age-old arts of persuasion. They are sometimes called propaganda (if your opponents are performing the operations), educational material (if your side is doing it) or even advertising via printed text, radio waves or television. Since tribes formed before history was captured, human beings have shaped the cognition of other human beings, both in the ‘in group’ and the ‘out group.’ Even though operations in the information environment have been central to civilization from the beginning, these operations expanded dramatically with the communications revolution inherent in the advent of the telegraph in the 1800s and accelerated with the further evolutionary additions of radio and television.

A new category of operations in the information environment is cyber-enabled information operations, which began with the arrival of the Internet. This takes the form of a traditional operation which uses cyber to magnify the Impact of the operation or to enable the operation itself. The hack of the Democratic National Committee would be an example of a cyber-enabled information operation. The information was obtained through cyber operations (the enabling function) but released via Wikileaks and thence to mainstream media outlets, a more traditional method of disseminating information.

Cyber information operations are a relatively new set of information operations that takes place entirely in cyberspace. An example would include Daesh recruiting videos. Videos are smoothly produced in a variety of languages and are aimed at global youth. As their target audience are digital natives, Daesh builds their products to be consumed as they do other digital materials. [38]

Countering these types of operations requires that the same techniques be used. As the Carter Center says, “The implementation of preventative community-based policies will equip trusted Islamic scholars and religious leaders with the necessary analysis and digital tools” [39] meaning that people hoping to counter them must use digital techniques to compete. This makes operations in the information environment a key cyber mission for militaries.

Military Operations and Cyberspace

Military operations can also be cyber-enabled or executed purely in cyberspace. This analytic framework discusses two types of military operations: conventional and special operations.

[figure 5 omitted]

Cyber can either enable an operation or can be the operation itself. As such, there are cyber-enabled conventional operations, cyber-enabled special operations, conventional cyber operations and special cyber operations. Cyber-enabled conventional operations happen on a daily basis while almost all special operations (due to the availability of resources) are cyber-enabled. It is probably safe to assume that cyber conventional operations happen frequently and regularly. Cyber special operations, like their kinetic namesake, probably do not occur often.

An example of a conventional or normal military operation would be the invasion of Iraq. An example of a special operation would be the raid to eliminate Osama bin Laden. Although these operations occurred with a minimum of cyber enabling, as time goes on and cyber capabilities suffuse militaries, more and more of these operations will become cyber-enabled. Eventually, all conventional and special operations will become cyberenabled unless specific counter-cyber operations negate that advantage.

An example of a cyber-enabled conventional military operation would be Russian operations in Georgia in 2008. Although Russia previously conducted purely cyber operations against Estonia in 2007, Georgia was different in that Russia conducted cyber operations against targets in Georgia to affect Georgian command and control in support of conventional military operations on the ground and air. [40]

An example of a cyber-enabled special operation would be the Mumbai attacks of 2008. Planners used a Go-Pro camera and walked the route so everyone could see videos of their routes during their preparation for the operation. Planners used Google Earth during their planning process. The command and control element monitored Indian social media

and traditional media (such as radio and television) to track the response by Indian security forces and steered the attacking force away from reacting Indian forces, enabling the operation to continue much longer than expected. [41]

As mentioned, cyber military operations also come in two flavors: conventional and special operations. A conventional cyber operation would be like “dropping cyber bombs on Daesh”. Secretary of Defense Ash Carter explained at an event at US Northern Command that “We’re using these tools to deny the ability of ISIL leadership to command and finance their forces and control their populations; to identify and locate ISIL cyber actors; and to undermine the ability of ISIL recruiters to inspire or direct Homegrown Violent Extremists,” [42] Although the operations may be classified, mere classification would not be sufficient to label this a special operation. This is a conventional operation in that it does not require special techniques or unique modes of employment, and does not require a covert approach to the operation.

According to Joint Publication 3-05, Special Operations, these operations require: … unique modes of employment, tactics, techniques, procedures, and equipment. They are often conducted in hostile, denied, or politically and/or diplomatically sensitive environments, and are characterized by one or more of the following: time-sensitivity, clandestine or covert nature, low visibility, work with or through indigenous forces, greater requirements for regional orientation and cultural expertise, and a higher degree of risk…Special operations may differ from conventional operations in degree of strategic, physical, and political and/or diplomatic risk; operational techniques; modes of employment; and dependence on intelligence and indigenous assets. [43]

A cyber special operation would be the Stuxtnet attacks on Iran. It meets many of the criteria for a special operation as defined above. It required unique modes of employment, tactics, techniques, procedures, and equipment. It was conducted in a hostile, denied, or politically and/or diplomatically sensitive environments. It was a low visibility operation characterized by a clandestine or covert nature, as manifested by the fact that no one has yet proved who conducted the operation.

As militaries routinely conduct conventional and special operations, these types of operations involving cyberspace are appropriate for militaries to conduct. All operations will eventually be cyber-enabled while there will be more and distinct cyber operations.

CONCLUSION

Because cyberspace is so large, and so much cyber activity occurs in the private sector, militaries do not have any business operating in most of cyberspace. Although militaries should be able to range anywhere throughout cyberspace to complete appropriate missions, most cyber activity should not involve the military at all.

There are pressures for the military to become more involved in cyberspace. DoD leaders have thus far managed to avoid being dragged into additional areas, mainly by sticking to DoD’s three cyber missions: Defend DoD networks, systems, and information; Defend the U.S. homeland and U.S. national interests against cyberattacks of significant consequence; and Provide cyber support to military operational and contingency plans. These are legitimate cyber missions for any military. These have been clearly articulated by the U.S. military; however, other militaries probably have not thought this through as they are busy building their cyber forces.

As manifestations of these legitimate cyber missions, there are four areas in cyberspace that are appropriate for the military to operate in crime, intelligence, information operations and military operations. This article has provided examples of how the military would be involved in all four of these areas. Although military forces are involved in these areas, they are not involved in all operations in these areas (for instance, the Department of Justice handles most cybercrime) but are involved in these areas. This, then, is the circumscribed area that should be called the military cyber domain. Militaries and Alliances like NATO around the world would do well to conceptualize these missions as appropriate for military cyber forces, understand why they should not be performing cyber missions outside of these areas, and inform their political masters that expanding cyber operations away from those four missions risks frittering away cyber combat, which would put at risk the overall mission of the military, the defense of the nation.

#### The AFF solves-- Only a properly funded, strategic communication effort can counter Russia’s attack on Western media

Henry **RIdgewell** **2016**, Henry Ridgwell reports for VOA from London, September 2016, “NATO Warns West Is 'Losing Information War' Against Russia, IS”, Voice of America News /sk

LONDON - The West must step up its efforts to combat and counter the information war being waged by its opponents, according to NATO officials. They warn that countries like Russia are exploiting the freedom of the press in Western media to spread disinformation. The term "hybrid warfare" is frequently used to describe the tactics used by the Kremlin in its forceful takeover of Crimea in 2014, when unmarked, heavily armed gunmen now widely known as the 'little green men' began storming Ukrainian military bases in the region. Moscow initially denied they were Russian military, yet weeks later similar unidentified armed units appeared in eastern Ukraine. That conflict between Russia-backed rebels and the Ukrainian military is still continuing. The West is under attack Speaking at this month's United Nations General Assembly, Ukraine's President Petro Poroshenko said hybrid warfare is being waged against the whole Western world. "Political pressure, blatant propaganda, interference with the electoral process, economic coercion, secret subversive and military operations, cyberattacks, misuse of diplomatic measures, these are modern and congenial methods of the undeclared war," Poroshenko said. At a recent conference on Information Warfare at the London-based Royal United Services Institute, the Director of the NATO StratCom Center of Excellence Janis Sarts said the West is playing catch-up. West not focused on this type of warfare "The technology is ours. The marketing powerhouses are in our countries. Yet we're having this discussion against the feeling of being pushed. Against the feeling of being pushed by different actors: Russia, Daesh... also China in more subtle ways," said Sarts, using and Arabic term for the Islamic State. The conference focused on the growing reach of Russian state media such as the 24-hour news channel Russia Today or RT, often accused of being a propaganda outlet for the Kremlin. Senior editor at The Economist Edward Lucas argued channels like RT should not be considered as journalism. "Russia has really grasped the post-truth environment. And they will lie about things absolutely brazenly. They understand the weaknesses of our media in the post-Cold War environment: that we prioritize fairness over truth." Russia investing big money Lucas added the West should do more about what he termed "social media hygiene." "There's a real problem with comment fields, and with fake social media accounts, particularly on Twitter. The Russians are putting lots and lots of money into creating tens of thousands of trolls." Mark Laity, the chief of Strategic Communications at NATO's Supreme Headquarters Allied Powers Europe or SHAPE, noted that Russia includes information strategy as a key pillar of its conflict planning, but in the West the communications are often handed off to separate public relations teams. "We are still fighting on the margins," he said, "when actually a properly funded, strategic communication effort is incredibly cheap compared to other costs." Laity warned Russia was deploying disinformation and hybrid warfare in its intervention in Syria - most recently in the disputed bombing of an aid convoy outside Aleppo earlier this month. He added the West must learn how to fight back.

### DOD Key---Internal Disinfo

#### Military cooperation is key to countering disinfo in the force

Raphael Cohen 21, Director of the Strategy and Doctrine Program of RAND Project AIR FORCE; Nathan Mustafaga, associate policy researcher at the RAND Corporation, Joe Cheravitch; Defense analyst at the RAND corporation; Alyssa Demus, associate international/defense researcher at the RAND Corporation; Scott Harold, political scientist and Associate Director of the RAND Center for Asia Pacific Policy; Jeffrey Hornung, senior political scientist at the RAND Corporation; Jenny Jun, Ph.D. student in the Department of Political Science at Columbia; Mike Schwille, senior policy analyst at RAND; Elina Treyger, political scientist at the RAND Corporation; Nathan Vest, adjunct research assistant at RAND, “Combating Foreign Disinformation on Social Media,” <https://www.rand.org/pubs/research_reports/RR4373z1.html>, cy

Train for Disinformation, Focus on Key Demographics, and Minimize Widespread Bans on Smart Phone and Social Media Use

The joint force has made significant strides toward incorporating counter-disinformation efforts on social media into their regimen. One way has been to simulate the social media environment through such programs as ION. Another has been to make real-world information environment monitoring a part of regular training exercises, such as Trident Juncture. There are pros and cons to both approaches, but detecting and responding to disinformation needs to be built into training programs—from the unit level down to the individual service member level—particularly as disinformation on social media becomes a staple of great-power competition.

This expansion of disinformation training will push the joint force to reach new audiences, possibly in uncomfortable ways. U.S. adversaries do not target all service members equally; they might not even narrow their focus to just service members. China tends to base its disinformation campaigns on ethnic lines, placing Chinese- and Taiwanese Americans at greater risk of attack.7 Russia targets military family members. In 2015 and 2016, several military spouses—many of whom led military family support groups or wrote about military family matters— received death threats on Facebook and Twitter from a group claiming to be “Cyber Caliphate” but actually tied to Russian intelligence, possibly in a bid to deflect attention from Russia’s actions in Ukraine and encourage support for Russia’s action to fight the Islamic states in the Syrian conflict.8 Both Russia and China could launch disinformation campaigns that do not target U.S. audiences at all but still hamper the joint force’s ability to operate by targeting local communities where the joint force bases overseas. Properly training for disinformation campaigns requires reaching out to new audiences (such as family members and base communities) and tailoring modules for specific at-risk groups.

Training all service members and family members to recognize disinformation campaigns is a herculean task. A simpler solution would be to ban the use of smartphones and social media during periods of conflict. However, such a policy could prove impractical. As Ukraine’s experience during the height of the conflict in the Donbass demonstrated, smartphone bans, even for front-line soldiers, proved difficult to enforce because bored soldiers found ways to smuggle phones to the front. 9 Theoretically, the joint force could pursue limited technological solutions (e.g., jamming reception or blocking access to certain sites) or selectively enforce bans for certain key units for limited periods of time, but improving force resiliency against disinformation will still depend mostly on training.

### DOD Key---Training

#### DoD training is key

Meghan Fitzpatrick 22, strategic analyst with Defence Research and Development Canada; Ritu Gill, section head with DRDC; Jennifer Giles, communication strategy and operations officer for the Marine Corps, “Information Warfare: Lessons in Inoculation to Disinformation,” *The US Army War College Quarterly: Parameters,* Vol 52, No. 1, cy

In addition to the computer-based training, the service components should also implement focused in-person media literacy training at the company level. Sessions should be held in small classrooms or town halls and led by DoD facilitators, from public affairs or communication strategy and operations, who have been trained by leading public-sector practitioners. The training should address trouble areas flagged by the annual computer-based class and facilitate practical application exercises that test the students’ ability to recognize and counter disinformation using personal devices. The practical application exercises would model leading public-sector courses but would focus on DoD equities. The in-person class would also offer an opportunity for servicemembers to discuss ongoing adversarial cyberattacks, media influence, military actions, challenges faced by partners and allies, and foreign interference in domestic events.

In addition, family predeployment briefs should integrate media literacy training to increase awareness before a servicemembers’ deployment. Although the Department of Defense cannot mandate family members take online media literacy training, many are concerned about the threat of false information and welcome opportunities to understand and protect themselves from these threats.43 Family readiness officers and key spouse leaders are also conduits to promote and share online media literacy education opportunities and encourage awareness.

Servicemembers and their families must learn and practice media literacy skills so they can protect themselves and counter adversary initiatives.44 Awareness programs would help them realize the disinformation threat and encourage them to defend themselves.45 A DoD-mandated, standardized, and multifaceted media literacy program that combines public-sector best practices and DoD equities can produce a comprehensive computer-based course and an in-person course that provides servicemembers and families the skills they need to confront adversary disinformation threats successfully.

Conclusion

The pace of technological acceleration and the division inherent in recent politics shows no signs of abating. As a result, the world will continue to face a proliferation of disinformation in online spaces, enhanced by sophisticated technology like deepfake videos.46 These advancements make it difficult to determine attribution or debunk disinformation and create a serious threat to democratic institutions, which are increasingly diverse in composition.47

While decisionmakers have considered a variety of solutions, none are likely to have the lasting impact of thorough media literacy education.48 In 2017, former “Chairman of the Joint Chiefs of Staff, General Joseph Dunford Jr. . . . designat[ed] information as the seventh joint warfare function.”49 For troops to be effective warriors, they must possess the skills needed to navigate a deceptive environment and recognize when and how they are being manipulated online. In “Deepfakes and the New Disinformation War,” Robert Chesney and Danielle Citron argue, “democracies will have to accept an uncomfortable truth: in order to survive the threat . . . they are going to have to learn how to live with lies.”50 If democratic societies are to function effectively, everyone will have to learn to survive and thrive in a complicated digital landscape.

### DOD Key---Intel Sharing

#### Intel sharing checks Russian hybrid warfare – Fusion Cells prove

Underwood et al. 22 (Major Andrew Underwood, USA, is Executive Assistant to the Deputy Director for Strategy, Plans, and Policy (J5), Europe, NATO, Russia. Colonel Andrew Emery, USAF, is the Space and Missile Defense Planner in the U.S. Military Delegation to the NATO Military Committee (JCS) at NATO Headquarters, Brussels, Belgium. Lieutenant Colonel Paul Haynsworth, USA, is currently serving in the Commander’s Action Group in the NATO Special Operations Headquarters at Supreme Headquarters Allied Powers Europe, Mons, Belgium. Commander Jennifer Barnes, USN, most recently served in the Commander’s Action Group at U.S. Africa Command Headquarters in Stuttgart, Germany., 4-14-2022, "All Quiet on the Eastern Front: NATO Civil-Military Deterrence of Russian Hybrid Warfare," National Defense University Press, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999367/all-quiet-on-the-eastern-front-nato-civil-military-deterrence-of-russian-hybrid/, DOA: 6-17-2022//Smarx Ahsan)

\*\*IO=Information Operation

Information Operations. Another critical aspect of imposing costs and limiting options available through Russia’s hybrid warfare approach is effective IO attribution and response. IO is substantive enough a factor in Russian hybrid warfare to be considered beyond comprehensive defense. Staying abreast of Russian hybrid objectives, methods, and tools prevents Allies and partners from being caught flat-footed. It also enables a better understanding of Russian intent and options for hybrid activity, both in traditional spheres and within the gaps and seams of 21st-century technology as an information platform. This analysis focuses on the intelligence- and information-gathering and strategic communication aspects of IO. Intelligence- and information-gathering are critical to identify Russia’s hybrid options and intent and to mobilize NATO member states toward the activity. Conversely, strategic communication is a proactive, comprehensive defense measure to specifically limit Russian hybrid options and to broadcast the costs Russia would incur if it moved forward with them.

For intelligence-gathering to be effective in today’s operating environment, countries must be willing to break down stovepipes and widely share information within their own government structures as well as with Allies and partners. The coordinated actions of hybrid warfare allow Russia to exploit regional, national, and international seams. Building intelligence-sharing apparatuses both within and without ministries among and across countries helps to close those seams. Effective intelligence-sharing could occur at levels ranging from joint/multinational collection teams to finished intelligence analysis at ministerial or national levels. In other words, information-sharing does not always have to be top-down driven; sometimes bottom-up is effective.

One goal of shared intelligence is to reduce the time required for NATO to consult and respond in part or as a whole. This effort could be facilitated by a common intelligence picture shared by all parties. Partial, inconsistent, or stovepiped intelligence might slow NATO’s response process by creating doubt or failing to correctly attribute malign activity to the Russian government. In addition, whether internal to a state or between allied states, stovepiping challenges coordinated action against hybrid warfare. Better intelligence-sharing would allow states to deny Russia the benefit of using IO techniques in hybrid warfare to isolate specific states or populations. A common intelligence picture also makes it more likely, for example, that a Russian intelligence operative or team preparing to assassinate a dissident would be identified and detained, and have the network and messaging compromised. An example of intelligence-sharing success within NATO nations against hybrid activity is the Baltic Special Operations Forces Intelligence Fusion Cell, a budding Estonian, Latvian, Lithuanian, and Polish initiative that operates with assistance from the United States. If implemented properly, such intelligence fusion cells might provide key indications and warnings of Russian hybrid warfare operations across the spectrum of IO, denying Russia the benefit of being able to claim noninvolvement/noninterference and could serve as a template for future initiatives among other Allies and partners. Furthermore, such fusion cells provide a path for connecting information across the Alliance’s multiple stovepipes, that is, the intra- and inter-bureaucratic inertia and the multilingual nature of the information environment. This enables a common intelligence picture and, consequently, the ability of the Allies to collectively deny Russian IO to access seams unfettered and without attribution.

Once Russian hybrid warfare IO activity is recognized and NATO agrees a response is appropriate, strategic communication would likely be employed as the principal countermeasure and vanguard to prevent Russian activity. The situational awareness derived from the shared information and intelligence discussed in the previous section would be critical to crafting targeted messages. Strategic communication would likely be split between two audiences: external actors and an audience internal to the conflict (that is, the targeted population). Internal strategic communication efforts should focus on countering the information aspect of hybrid warfare. Prior to a campaign, successful strategic communication might limit the vulnerability to target audiences, such as the Russian-speaking minorities of the Baltic states, or a Russian hybrid campaign. This is achieved by negating Russia’s plausible deniability concerning the sponsorship of the conflict’s version of “little green men” (or whatever the aggressor looks like in that campaign). Internal strategic messaging campaigns must be swiftly organized and executed because they are most effective if they prevent Russia from gaining a tactical advantage during the initial “fog of war” period. Once a hybrid warfare campaign has begun, the focus of external strategic communication should be to expose Russian activities to NATO (and the rest of the world). This might undermine Russian public support for such activities, would inform decisionmakers during NATO deliberations, and should unite the international community against the malign actor.

## NATO Key

### NATO Key---Broad

#### NATO adoption of a holistic interoperable approach to combatting disinformation is key. Prevents a litany of x-risks---Russia war, nuke terror, prolif, EDTs, warming, and LIO collapse vis-á-vis China rise.

Gill and Goolsby 22, Ritu Gill has a PhD in psychology from Carleton university, Rebbeca Goolsby is the co-Lead of a NATO Research Technology Group on cyberdiplomacy and communications, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. XXII, 213 (under “Foreword”) //chico

Our unity and our ability to adapt is even more critical as we face a more unpre- dictable, complex, and rapidly changing sphere of geopolitical conflict. We face more sophisticated cyber-attacks and disinformation, a more assertive Russian, brutal terrorism, nuclear proliferation, disruptive technologies ever. The security impact of climate change, so crucial for own public opinions, and where NATO is embarking energetically in that direction. And, of course, the most critical game-changer in global affairs in many, many decades, or probably centuries, is the shift in the worldwide balance of power with the rise of China.

Such hostile activities seek to undermine our democracies, our institutions, our shared values on which our Alliances is founded. But perhaps more fundamentally, it seeks to undermine the trust of our citizens in the very institutions of democ- racy because this competition, global competition that never ends, historically, is today also a competition of fundamental ideas. And the most crucial part is what we do, not only to describe this intimidation as worrisome and concerning but to take concrete actions to face this phenomenon. We must continue to invest in our strategic communications capabilities and build an evidence-based understanding of the (dis)information environment to contest a highly contested communications space.

In the last past 18 months only, COVID-19 has shown us how disinformation and propaganda can be used to sow distrust, undermine science, and threaten lives and our security. We have seen dangerous disinformation campaigns about the origins of the Coronavirus, cyber-attacks on hospitals, the nature of Alliance activities, and online espionage on medical research centers working on vaccines and treatments.

Our information environment assessment capability must have well-trained staff, supported by the right technology, with the right scientifically informed under- standing to navigate this extraordinarily complex field. It will be essential to develop objective-driven, proactive communications strategies, responding rapidly to the increasing volume of information attacks on our institutions, our people, and our values.

NATO has shown that we remain ready and able to defend our nations, that allies and partners are supporting each other, and that investing in our Armed Forces is an investment in the strength and resilience of our societies. This readiness was demonstrated in no uncertain terms by our Alliance’s vital role in fighting this deadly pandemic. This capacity stretches across the maritime, land, air, cyber, and space domains, as well as the information or cognitive sphere.

Taken together, this will help us build the resilience of our societies, and building resilience in our communities requires a whole-of-society approach. Everyone has a role to play; the media, the private sector, academia, civil society, of course, the whole-of-government. But it also includes all the relevant groups in our communities to ensure that our institutions and citizens are equipped for today’s digital realities. Beyond the nations that make up the Alliance, we must work in concert with our partners to strengthen our collective ability to prevent crisis and address challenges. It is clear that no nation alone, no continent alone, can cope with the magnitude of the challenges we are now facing as democratic societies.

#### NATO action now is key---the Strategic Concept provides perfect timing for renewed counterinformation tactics.

Tomasz Chłoń 22, Director of NATO Information Office in Moscow, postgraduates diplomas in international relations and European integration from the Polish Institute of International Relations, the University of Maastricht, and the University of Warsaw, co-author of the book “Counter-Disinformation Education and Research Platform – Building Social Resilience,” May 2022, “NATO and Countering Disinformation The Need for a More Proactive Approach from the Member States,” https://www.globsec.org/wp-content/uploads/2022/05/NATO-and-Countering-Disinformation-ver1-spreads.pdf, RMax

Towards a Consistent Response to 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 Plan4 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)6 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.7 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.8

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 20229 . 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.

Strategic Context

The Alliance’s new Strategic Concept could therefore reflect more comprehensively the key tenets of an enhanced approach to disinformation, encompassing public diplomacy, strategic communication and social resilience. Such an approach could also consider new and innovative tools to combat disinformation, given that these can fit into a broader strategic context of NATO’s work.

In 2019, the Alliance approved not only the first secret military strategy in over 50 years but also a strategy for developing the necessary military and technological potential in connection with the changing nature of conflicts (NATO Warfighting Capstone Concept). With its stronger deterrence and defence approach to security, NATO began implementing a policy that enabled the coordinated development of breakthrough technologies, recognising that technology development will be a priority in seven areas: (i) artificial intelligence, (ii) advanced big data analysis, (iii) autonomous technologies, (iv) quantum computing technologies, (v) biotechnology, (vi) hypersonic capabilities and (vii) space technologies. In February 2021, the Allies approved the Coherent Implementation Strategy on Emerging and Disruptive Technologies. Eight months later, in October, the first NATO strategy on artificial intelligence was approved. From the perspective of disinformation activities, the future of artificial intelligence can be seen as a dual-purpose tool. Depending on human decisions, it can become a sword in the hands of opponents of freedom or a shield that protects societies and individuals against the consequences of their actions.

NATO Strategic Concept and Recommendations

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 practices10.

#### NATO key to a unified response to Russian Information Warfare attacks

Molly McKew 17, a writer, and expert on information warfare; she currently serves as narrative architect at New Media Frontier, a social media intelligence company. As an analyst and author; her articles have appeared in Politico Magazine, the Washington Post, and other publications, September 2017, "The Scourge of Russian Disinformation," Congressional Hearing, https://www.govinfo.gov/content/pkg/CHRG-115jhrg26880/html/CHRG-115jhrg26880.htm //AShah

Third, irregular warfare, including information warfare, will be fought within our borders. This means we need to rethink authorities. Our most experienced assets shouldn't be boxed out of defending the American people. We need sanctioned irregulars to build defensive and retaliatory capacity in information operations, and a good place to start would be a combination of U.S. Special Forces--who are, by mission, trained to fight unconventional wars--with counterintelligence and independent actors. We must also work with our trusted allies on the geographic front lines of NATO using--as you noted, Senator Gardner--the 10th Special Forces Group, our Europe-aligned group, which brings a range of knowledge and experience in countering Russia to the table.

#### Fact-based approaches fail. Cooperation is key to innovating effective counter-strategies to disinformation.

D. F. Reding & B. Wells 22, Dale F. Reding and Bryan Wells are both Chief Scientists at NATO, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” *Advanced Science and Technology for Security Applications*, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 25-43 (under the ch. titled, “Cognitive Warfare: NATO, COVID-19 and the Impact of Emerging and Disruptive Technologies,”) //chico

Disinformation campaigns are hardly new and have long been a staple of geopolit- ical conflict. Nevertheless, the precision, breadth, volume, automation and audacity of such attacks are unprecedented. Exploiting the situation, some states, social groups and individuals with malice and forethought sought to conduct cognitive warfare on entire populations, using the opportunities presented by COVID-19 to seek political or social advantage. These have had, and will continue to have, severe consequences for Alliance nations and the health of its citizens. Ultimately, as we have discussed in this chapter, the NATO alliance has faced these issues through the active use of S&T and a focus on facts, concrete actions, and trust-building. Nevertheless, it is a well understood psychological phenomenon that facts do not always win an argument. While arguably a successful strategy, the lingering effects of these attacks suggest that the struggle is far from over. In the end, whether it is at the strategic or tactical level, conflict is a decidedly human activity. The most effective way to overcome an opponent is to impact their thoughts and beliefs, thereby turning them against themselves. Continued research into disinformation and its impact on societies will help develop new battle plans to counter these attacks. Further, the success and increasing development of more sophisticated attacks suggest that cognitive warfare will become even more important for the Alliance as potentially the sixth operational domain for NATO.

### NATO Key---Private Sector

#### NATO has unique private sector ties which shore up cognitive warfare defenses.

John Fuisz 22, CEO/Founder at Veriphix, “Veriphix Announced as Winner of NATO Innovation Challenge - Fall 2021 Iteration: Veriphix to implement Beacon, the industry's first belief tracking dashboard, for NATO Countering Cognitive Warfare Efforts,” <https://www.proquest.com/docview/2632243011?parentSessionId=qNodNc0hWc6t9e5hIzdORwZhnN%2FE85JeZ9KaFpouKvU%3D&pq-origsite=primo&accountid=14667>, cy

WASHINGTON, Feb. 24, 2022 /PRNewswire-PRWeb/ -- Co-organized by NATO's Innovation Hub and the Canadian Ministry of Defence, the 2021 iteration of the NATO Innovation Challenge ended on 30 November 2021 with the victory of Veriphix, a US company that has developed a belief dynamics platform to track and measure a population's beliefs about any topic, empowering brands to move customers towards ideas, products and services.

This challenge, co-organized with the Canadian Special Operations Forces Command, with Innovation for Defence Excellence and Security (funding program of the Canadian Ministry of Defence for innovation) and Old Dominion University, dealt with Cognitive Warfare and brought together more than 130 solutions from 13 nations. High-level authorities such as Mrs. Jody Thomas, Deputy Minister of National Defence of Canada and General Philippe Lavigne, NATO Supreme Allied Commander Transformation, showed their support by opening the event.

The Fall 2021 Innovation Challenge iteration focused on innovative solutions that pertained to countering cognitive warfare. During the virtual final pitch event, the remaining 10 finalists delivered their proposals and answered questions from the jury.

The Innovation Challenge was open to entrepreneurs, designers, inventors, engineers, scientists, coders, innovators and others. The best entries in this edition of the NATO Innovation Challenge could help inform and support the development of future NATO military doctrine, standards and requirements, and the development of new capabilities.

"Influence operations have been around since ancient times." said John Fuisz, Veriphix Founder and CEO. "Advancements in the modern era from the cognitive sciences have made them more systematic and effective. We are pleased to offer our solution to help NATO strengthen its defensive cognitive warfare capabilities."

About Veriphix

Veriphix is a behavioral science-based data analytics startup that tracks and measures belief, and provides the nudges that impact belief, to improve business outcomes across marketing, strategy, and product design.

About the NATO Innovation Hub

Since 2017, The NATO Innovation Hub from Headquarters Supreme Allied Command Transformation has organized innovation challenges twice a year. Each challenge is co-organized with a NATO Nation, which host the final event: the pitch day of the finalists. The challenge is open to anyone (individuals, entrepreneurs, start-ups, industry, academia, etc.) located in NATO Nations. The Innovation Challenge aims to give NATO new, creative and efficient ways to respond to security challenges.

By organizing these important competitive innovation challenges around real-world issues, Allied Command Transformation continues to be at the forefront of NATO efforts as it relates to the importance of transformation and development as continuous and essential drivers of change.

## U.S. Key

### U.S. Key---CYBERCOM

#### Reorienting US CYBERCOM toward incorporating counter disinformation in their cyber defense capabilities is necessary to prevent disinformation---only the US can ensure

Dr. Martin Libicki 17, Keyser Chair of cybersecurity studies at the U.S. Naval Academy, Ph.D. from U.C. Berkeley, Spring 2017, “The converge of Information Warfare,” *Strategic Studies Quarterly*, Vol. 11, Issue 1, pp. 49-65, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11\_Issue-1/Libicki.pdf, RMax, IW = Information Warfare

The Future of US Information Warfare

Given the trends and convergence of information warfare, how might the United States exploit these trends? On the face of it, no country is better positioned to carry out information war. US skills at cyberwar have no equal. US institutions lead the world in the commercialized arts of persuasion, and the collection and analysis of personal information for commercial and political purposes have proceeded farther in the United States than anywhere else. No country is more advanced in digitizing and networking things. US expertise in systems integration is unchallenged. But figuring out how to effectively harass another country's citizens one at a time does not seem like an urgent or important, much less permissible, US national security problem to solve.

Nevertheless, because other countries are interested in figuring out how to combine these elements of information warfare into a unified whole, the United States ought to understand how to do so itself. First, there may be useful techniques learned even if the larger idea is unacceptable. Second, even though the prospect of operating a harassment campaign based on IW is unpalatable, one cannot rule out occasions in which the only way to stop others from doing so (short of armed conflict) may be a credible offensive capability. Third, just as the Defense Advanced Research Projects Agency was established shortly after Sputnik launched for the purposes of preventing surprise- -and then went ahead to develop technology that surprised others- dabbling in the arts of IW could help prevent external developments from surprising the United States.

If the United States were to embed cyber operations within a broader context of IW, then the mission and organization of US Cyber Command would have to change. Today it boggles the mind to ask an organization (deservedly) wrapped in great secrecy to take the lead for influence operations, which are ineluctably public. But in time, the choice to overlook the psychological effects of cyber operations or the potential synergy between psychological operations and cyber operations would make just as little sense.25 Serious thought may be needed on how to build an information warfare authority, whether housed under one organization or achieved through intense coordination among the various communities: cyber warriors, cyber intelligence collectors, electronic warriors, psychological operators, and, in some cases, special operators.

Perceptions of cyberwar might also need rethinking. One could debate the plausibility of a determined cyber attack campaign unaccompanied by violence. However, it is harder to imagine a cyber attack campaign unaccompanied by other elements of information warfare, in large part because almost all situations where cyber attacks are useful are also those which offer no good reason not to use other elements of IW. For instance, if another country is trying to exhaust US will by conducting cyber attacks on information systems that underlie US commerce, they would not necessarily try to blow up trucks. Rather, cyber attacks that compromise trucks, to reduce confidence in their safe operation, are more plausible, if achievable. It is also quite likely that in a systematic campaign, attackers would try to jam GPS or override satellite uplinks, using cyber espionage to create the impression that they are watching Americans and are prepared to dox particular individuals, or letting a thousand trolls bloom to create a news environment that would pit Americans against each other. The latter activities have attributes of nonlethality, unpredictability, ambiguity, and persistence that allow them to fit the strategic niche occupied by cyber attacks. Preparations to retain resilience and accelerate recovery after a cyber attack campaign would also do well to address the complications that could arise if other elements of IW were used in conjunction with cyber attacks.

### U.S. Key---Agreement

#### US lead is key to ensure agreement.

David Shedd 20, professor at the Patrick Henry College, former acting director of the Defense Intelligence Agency; and Ivana Stradner, Visiting Research Fellow at the American Enterprise Institute, J.S.D. from the University of California, Berkeley,8/11/2020, "Countering Russia’s Influence Operations in the Balkans," https://www.heritage.org/europe/commentary/countering-russias-influence-operations-the-balkans, RMax

Even the pandemic has the potential for fomenting political unrest.

In recent days, thousands of Serbs have taken to the streets to protest Serbian President Aleksandar Vucic’s announced strict curfew in response to a surge in Covid-19 cases. Many have pointed a finger at pro-Russia ultra-right groups and foreign intelligence services for fueling the violent riots.

Moscow denies any “Russian trace” in the unrest. Whether Russia is behind the violent protests in Belgrade remains to be seen. One thing is for certain. The Kremlin’s efforts to sow mayhem in the Balkans would not be new; this would merely be the latest attempt by a resurgent Russia to threaten Euro-Atlantic security and challenge the United States’ ability to defend its interests in Europe.

Russia is promoting its interests in the Western Balkans through the widespread use of disinformation and cyberwarfare. The U.S., however, isn’t helpless. It has an opportunity to obtain insights into these efforts and counter Russia's influence campaigns. It is time to confront Russia's strongman Vladimir Putin's cyber games before American interests are permanently damaged in the Balkans.

The U.S. and the E.U. have long been ambivalent about defining their interests in the Western Balkans. Russia has capitalized on these years of neglect and leveraged a power vacuum in the former Yugoslavia to gain economic and political influence. The region is now at the forefront of Russia's use of low-cost strategies to expand its global influence and undermine western interests.

Russian disinformation, aided by repeated cyberattacks on government institutions, was instrumental in the 2016 Moscow-sponsored coup attempt in Montenegro. In North Macedonia, Russia spread disinformation prior to the name-change referendum that finally enabled North Macedonia to join NATO. It also established hundreds of North Macedonia-based “troll factories," from which Russia pedaled fake news against the 2016 U.S. elections. Facebook recently banned troll farms from North Macedonia that pushed COVID-19 disinformation.

Moscow has also been investing in critical sectors in Croatia. With its strategy of fomenting political divisions, the Kremlin has been exploiting internal conflicts in Albania. In Bosnia and Herzegovina, disinformation campaigns have sown ethnic and religious discord, while promoting the secession of ethnic Serb regions from Bosnia. In response, the U.S. should encourage the transatlantic integration for Bosnia and Herzegovina, the Western Balkans’ most fragile country.

Russia has used state-sponsored media to promote nationalist and anti-Western narratives in Serbia, including the opening of a Sputnik office in Belgrade. Also,  Russian-run “Humanitarian Center” in Serbia is very close to the main NATO based in Kosovo (Camp Bondsteel). Some European and American officials fear that it serves as a base for the Kremlin intelligence-gathering activities to eavesdrop on U.S. interests in the Balkans.

Russia’s preeminent goals in the Balkans have been to refine their disinformation tactics and erode Western influence in the region, including in Croatia, Montenegro, North Macedonia and Albania, which are all NATO members. The West needs to aggressively respond to this Russian posture, including using a cyber-focused campaign to counter Russia's provocations.

For crafting such a strategy, the West should look to Estonia. After the 2007 Russian cyberattack on Estonian government institutions, Estonia became a global leader in cybersecurity and home to the NATO Cooperative Cyber Defense Centre of Excellence, which is a cyber-defense hub that supports member nations with cyber-defense expertise. A similar approach by the West would benefit the Western Balkans, where information and communication technology sector is the most promising and the fastest growing economic sector in the region. In Serbia alone, the I.T. sector generates more than 10% of GDP with a similar trend in other countries in the region, which have some of the highest numbers of outsourced I.T. workers per capita in Europe.

An American-led strategy should focus on creating a regional cyber-security infrastructure in the Western Balkans, modeled on Estonia's example. Given that countries in the Western Balkans share the same cyber-security threats from Russia and, more recently, from China, a regional hub for cybersecurity would allow states to cooperate among each other in cyber deterrence, attribution of attacks and collective countermeasures.

Several countries in the Western Balkans have joined NATO, but alliances are notoriously unreliable, especially among the smaller states. Countries in the Western Balkans need strong NATO and E.U. ties to withstand Russian influence. Cyber-security is one of the areas where they can strengthen their positions in allegiance with the western democracies.

The timing is excellent for the U.S. to establish a regional cyber-security hub in the Western Balkans. Immediate steps need to be taken to halt malign Russian influence. With elections approaching this year in the U.S., North Macedonia, Croatia and Montenegro, countries should continue cooperating to counter malicious Russian cyber activities.

The U.S. can learn more about Russian cyber tactics at the same time. One way to send a strong message would be to deploy a cyber-team to strengthen NATO’s countries’ cyber-capabilities in an effort to thwart future Russian network intrusions such as the one that was undertaken by Russian intelligence operators in Bulgaria in 2017.

Serbia, a key ally to Moscow in the region, remains the biggest obstacle to countering Russian influence. Serbia just had parliamentary elections boycotted by the opposition that resulted in Vucic's Serbian Progressive party winning a landslide victory and further strengthening his power. The close Russia-Serbian relationship can make it difficult to detect Russia's subversive activities.

Of all the Western Balkans countries, Serbia had the highest military expenditure in 2019, and President Vucic thanked Russia for making Serbia’s military 10 times stronger since NATO intervention in 1999. After Russia employed an S-400 missile system in Serbia for a military drill, the Pantsir S1 air-defense systems were delivered this past February, despite a looming U.S. sanctions threat.

Should Serbia continue obtaining Russian weapons, Washington should impose sanctions. Serbia must understand that its strategy of neutrality is unacceptable to the U.S., as are its claims to balance their interests among Russia, China and the West. The U.S. should remain solidly committed, leading efforts to solve the Kosovo dispute and wrest control of that narrative from Russia.

While variances in the national interests may complicate cooperation among the Western Balkan countries, they share similar vital objectives that make cooperation possible and even attractive under U.S. leadership. Among these are the historical fear of Russian domination and a desire for E.U. and NATO membership. A U.S.-led strategy with NATO country participation to enhance their cyber-capabilities will improve their security in countering nefarious Russian influence while enhancing cooperation between Balkan nations.

Moscow is determined to expand its influence in the Western Balkans, using cyber-warfare at the expense of U.S. and western interests. To prevent it, the U.S. should design a new strategy for the Western Balkans that demonstrates that the U.S. is committed to countering Russia's disruptive activities in the Western Balkans and beyond. The time for that response is now.

## Say Yes

### Say Yes---2AC

#### Status quo efforts to counter Russian disinformation campaigns prove that they are popular within international institutions like NATO but absent the aff they fail

Adam Kowalski 22, Adam is research assistant with the Russia and Eurasia Program at Chatham House. He worked as a project officer at the European Bank for Reconstruction and Development (EBRD), June 2022, "Disinformation fight goes beyond Ukraine and its allies," Chatham House - International Affairs Think Tank, https://www.chathamhouse.org/2022/06/disinformation-fight-goes-beyond-ukraine-and-its-allies //AShah

Reactive response to new information realities

As the Kremlin tightened its grip over the media space in Russia and increased spending on information dissemination, the international response was fast and unified with many tech companies and social media platforms increasing efforts to highlight and remove malicious information actors.

Fact-checking and debunking organizations ramped up their operations and the UK and Australia explicitly asked social networks to block Russia state-linked services and content providers. The European Union (EU) and the UK banned both Sputnik and RT, and Canada announced increased funding for the G7’s Rapid Response Mechanism, which was created to respond to threats from foreign actors ‘seeking to undermine democratic societies and institutions’.

International responses to Russia’s malign information tactics are based on decades of experience and are now supported by growing funding and a heightened awareness of the nature of the problem. During the war in Ukraine, they have demonstrated how quickly they can react to new information realities – changing narratives, target audiences, or methods of spreading information.

But if these approaches to the growing disinformation threat cannot be extended to the Kremlin’s other targets, including those [closer to home](https://balkaninsight.com/2022/05/09/russia-targets-bosnia-with-disinformation-about-ukrainian-war/), pressure from beyond national borders will grow to [make concessions which are advantageous](https://www.chathamhouse.org/2022/03/cost-ceding-advantage-russia-far-reaching) to Russia’s longer term aims.

# Add-Ons

## DOD Innovation

### Add-On---DoD Innovation---2AC

#### Countering adversaries’ disinformation solves DoD innovation.

Sydney Litterer 22, Research Assistant at the RAND Corporation; and Krista Romita Grocholski, physical scientist at the RAND Corporation, 4/22/2022, "Effective Use of Nonlethal Weapons Could Require Combating Disinformation," No Publication, https://www.rand.org/blog/2022/04/effective-use-of-nonlethal-weapons-could-require-combating.html, RMax

In an era of strategic competition, nonlethal weapons can potentially bolster U.S. Department of Defense (DoD) capabilities. The temporary and reversible effects of these weapons can provide DoD with an appropriate response to provocations that don't merit the use of lethal force, reducing the potential for collateral damage while mitigating the risk of inadvertent escalation in peacetime and gray-zone situations.

Public perceptions can have powerful effects on how these systems are employed and the impact of their use. Understanding these factors, and particularly the potential for negative narratives emerging from the use of novel technologies could be vital for DoD as it develops innovative nonlethal weapons because the technologies they rely on may be poorly understood by the general public.

The Joint Intermediate Force Capabilities Office, which oversees nonlethal weapons for DoD, is already conducting proactive public outreach to ensure that the new and useful nonlethal weapons it develops don't become the object of public misperceptions. However, these efforts may need to be bolstered to effectively counter the spread of disinformation when nonlethal weapons are employed in contentious situations. DoD might consider whether pre-emptive, large-scale public-information efforts or focused counterdisinformation campaigns could effectively address the risk of controversies stemming from inaccurate information regarding nonlethal weapons. After all, if a weapon is too controversial to use, its technical capabilities are irrelevant.

This issue is far from hypothetical. For example, DoD has a nonlethal, directed-energy weapon—the Active Denial System (ADS)—that uses a beam of millimeter waves to create an intense heating sensation that goes away as soon as a person leaves the beam. Millimeter waves are incapable of penetrating beyond the outermost layer of skin, so their effects are superficial and do not cause long-term damage. Nevertheless, ADS has been the subject of a great deal of controversy. Because most people outside of DoD are unfamiliar with millimeter waves, perceptions that DoD has developed a “heat ray” meant to microwave people have gained traction. ADS is also sometimes brought up in discussions of “Havana syndrome,” a type of brain damage potentially caused by microwave attacks, even though its effects are temporary and entirely different. This controversy may inhibit the deployment of ADS, despite its proven safety record and impressive efficacy.

Expanding public-information efforts to address controversies surrounding novel technologies like ADS could be important as the United States engages with near-peer competitors like Russia and China, who both recognize the power of narratives in shaping competition and conflict. In particular, Russia's recent use of disinformation to justify its invasion of Ukraine is but one facet of its extensive engagement in information operations. RAND research describes these efforts as a “firehose of falsehood,” in which Russia uses traditional and social media channels to flood foreign audiences with unreliable information that exploits existing societal tensions to increase feelings of alienation among Russian-speaking populations in neighboring countries and introduce social and political instability more broadly. Portraying U.S. and NATO actions as aggressive and escalatory contributes to both aims—and has been a key component of Russian rhetoric in recent days. In future gray zone conflicts, where other nations can take advantage of ambiguity and misdirection while using purported civilians as proxies (and the United States may face significant incentives to avoid escalation), use of new nonlethal weapons may provide fertile ground for disinformation by U.S. rivals.

All of this is already possible for nations skilled in information operations, and, as the COVID-19 pandemic has made abundantly clear, disinformation spreads like wildfire. Acknowledging that DoD may not be the only arbiter of how these weapons are perceived could be critical. Furthermore, what's unknown is easily demonized, and what's demonized may never be used and thus remains unknown.

If DoD wants to introduce novel capabilities that commanders feel comfortable using, it could work to ensure that its current public outreach efforts aren't undone by the unopposed spread of disinformation during a crisis. Taking this risk seriously could mean exploring how large-scale, pre-emptive public-information efforts or responsive counterdisinformation campaigns could prevent adversaries from turning U.S. forces' use of nonlethal weapons against them in the realm of public opinion. Addressing the problem could enable U.S. forces to use nonlethal weapons confidently and successfully to reduce casualties and achieve narrative dominance.

#### DoD innovation solves extinction.

Bowman Heiden 20, professor at the University of California, Berkeley, co-director of the Center for Intellectual Property; Jeanne Suchodolski, attorney with the United States Navy Office, 2020, “Innovation Warfare,” *North Carolina Journal of Law & Technology*, Vol. 22, Issue 2, <https://scholarship.law.unc.edu/ncjolt/vol22/iss2/4>, RMax

VIII. CONCLUSION

Innovation Warfare is a competitive strategy prosecuted by nation states against the innovation infrastructure of the U.S. Innovation Warfare is a means to a geopolitical end and does not constitute economic competition as usual. Countries engaging in Innovation Warfare pose both a national security and economic risk to the United States because those countries threaten the innovation ecosystem at the root of economic power and prosperity, and at the root of military technological superiority.

China is currently prosecuting an Innovation Warfare competitive strategy against the United States. As documented and described herein, there currently exists a comprehensive, coordinated effort by China to acquire U.S. technology and to co-opt the U.S. innovation base for its own purposes. A future in which China prevails in the Innovation Warfare “fight” is one in which the United States cedes the technological future to another, and one in which its geopolitical power and the prosperity of its citizens is at risk. The danger presented by China’s Innovation Warfare tactics is also an existential one.

A technological future dictated by Chinese interests is unlikely to incorporate western values of privacy and personal liberties into that technology. Innovation Warfare thus constitutes a threat against which the United States must defend itself. Development and execution of an Innovation Warfare counterstrategy are therefore critical to protecting the national security and economic interests of the United States and negating the type of economic and geopolitical aggression that previously led to two World Wars. Executing a counterstrategy not only preserves the peace but ensures that peace is one in which American welfare and liberties remain intact. There are four things the United States must do to execute an effective counterstrategy. These four things are:

1. Future-Oriented Technology Intelligence – Develop machine learning tools to identify the possible technological futures and drive towards the preferred future(s);
2. Strategic Technology Development – Optimize and scope federal R&D spending to seed the innovations necessary to attain the preferred future(s);
3. Secure Technology Control Positions – Identify and secure control positions along the preferred future technology implementation path, including deploying and protecting intellectual property as an armament in the Innovation Warfare battlespace; and
4. Organize to Win – Develop the cross-functional capabilities and inter-organizational coordination both within the government and across the public-private interface.

Innovation Warfare distilled down to its most basic truth is a footrace to control the technological future. FTA capabilities are thus vital not just to winning, but also to defining the mileposts along the racecourse. Future investments in FTA capabilities will be critical to overtake the lead others have built in this field. One cannot influence the attainment of a future one cannot see, or which others can see well in advance. In a world where others have advanced FTA capabilities, it will be difficult to optimize research into new technologies with equivalent speed and insightfulness absent those investments.

The capabilities necessary to implement the remaining elements of the Innovation Warfare counterstrategy already exist but must be marshalled and aligned with strategic goals. In particular, the government, and specifically the Department of Defense, should work to expand its intellectual property portfolios and align them with Innovation Warfare objectives. Intellectual property constitutes a crucial armament in the Innovation Warfare battlespace. Intellectual property establishes control positions along the racecourse to the technological future(s). According to the principles of strategic openness, these control positions can be gated open to encourage technology adoption, or gated closed to prevent it. Deft use of advanced licensing techniques employs these principles to manage the established control positions and ensures that the technological future arrived at is the one preferred.

Each of these enumerated counterstrategy elements stands not alone but works in concert with the others. Leadership must organize nationally and at the agency levels to synchronize these efforts. Agencies with strong research portfolios, such as the Department of Defense and Department of Energy, will require a designated leader or function to coordinate the intellectual property and control position aspects of the counterstrategy across various internal stakeholders. This functionality can be achieved by appointing a CIPO or by expanding the responsibilities of existing personnel. Within the Department of Defense, it may additionally be possible to designate one department, for example, the Navy, as the lead executive agency with overall responsibility for implementing the counterstrategy. Sufficient statutory authority exists to execute the Innovation Warfare counterstrategy and organizational design, without the need for additional legislation or rulemaking.

Innovation Warfare may exist in the gray area between peace and war, but it nonetheless is a conflict the United States must win.

# Topicality

## Security Cooperation

### T- SC---Includes Nonmilitary Security Agencies

#### Includes non-military.

Still says DoD tho

CRS 16, Congressional Research Service, 8/23/2016, “DOD Security Cooperation: An Overview of Authorities and Issues,” https://www.everycrsreport.com/reports/R44602.html, RMax

DOD defines “security cooperation” as a broad set of activities undertaken by DOD to encourage and enable international partners to work with the United States to achieve strategic objectives. Included in the definition are DOD interactions with both foreign defense and foreign nonmilitary security establishments. Security cooperation includes all DOD-administered security assistance programs that (1) build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; (2) develop allied and friendly military capabilities for self-defense and multinational operations; and (3) provide U.S. forces with peacetime and contingency access to host nations.4 According to DOD, security assistance is a subset of DOD's security cooperation portfolio.

## Cybersecurity

### 2AC---AT: T Cyberattacks

#### The US CSC (Cyberspace Solarium Commission) votes aff.

CSC 21, The United States Cyberspace Solarium Commission, December 2021, "Cyberspace Solarium Commission," No Publication, <https://www.solarium.gov/public-communications/disinformation-white-paper>

INTRODUCTION – WHY DISINFORMATION IS A CYBERSPACE ISSUE

The United States Cyberspace Solarium Commission (CSC) was created by Congress in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy? While disinformation is considered by some an issue largely separate from cybersecurity or network security,1 the Commission addressed disinformation in the very narrow context of elections in its final report in March 2020. As the COVID-19 pandemic swept across the globe, the Commission revisited the issue, this time in the context of disinformation about the pandemic itself, noting, “Our adversaries’ disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts with which Americans are best acquainted.”2

Over the course of the intervening months, the Commission received demand signals from constituents within Congress and the executive branch to treat the topic of disinformation and potential policy recommendations more extensively. The Commission has previously been reluctant to delve deeply into the topic of disinformation for two reasons.

First, disinformation as a policy issue, unlike many aspects of cybersecurity policy, has been marked by a strong partisan divide. Researchers have identified an association between strong partisanship and vulnerability to misinformation;3 more than two-thirds of U.S. citizens believe that Republicans and Democrats disagree about basic facts;4 and while U.S. citizens in both major parties agree that disinformation is a problem, they disagree about who is responsible for it and what ways to tackle the threat are appropriate.5 Although this partisan divide persists today, it is the sense of the members of the Commission that there is room to reach some agreement on core issues.

Second, as noted above, disinformation is seen by many as an issue largely separate from cybersecurity and cyber policy in the United States. While the Commission understands this view, continuing to bifurcate these issues has become untenable. From a strategic perspective, the United States and its policymakers do themselves a disservice by continuing to differentiate between the two when our adversaries do not.6

In order to craft a comprehensive strategy to defend the United States from cyberattacks of significant consequence, policy-makers must account for the entire arsenal employed by adversaries to cause harm in cyberspace, including information. It is also important to take a more operational or risk management perspective: disinformation campaigns waged against the United States by foreign actors are often carried out by many of the same threat actors as are active in cyberspace and are often the consequence of cyberattacks.

For these reasons, members of the Commission believe that elements of the topic of disinformation are within our mandate. This white paper is the result of deep research, interviews with experts, and deliberations by the Commission. It seeks to explain how the Commission’s proposed strategy of layered cyber deterrence applies to combating disinformation and contributes a set of policy recommendations to better position the United States to prevent, counter, and withstand the consequences of disinformation launched against it.

#### Countering disinformation is cybersecurity---terrain, tactics, targets, and temptations prove. The EU votes aff.

DisinfoLab 21 – The EU DisinfoLab, 5/24/2021, "Why Disinformation is a Cybersecurity Threat," EU DisinfoLab, <https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/>, RMax

Context: Why Disinformation is a Cybersecurity Issue

Drawing on our research into coordinated disinformation campaigns and our own experience as an NGO in the field, we wish to highlight four areas of convergence between disinformation and cybersecurity of relevance to EU policymakers: the “terrain” on which disinformation is distributed (the social web and the internet stack, networking infrastructure, routing services), the “tactics” that increasingly combine disinformation as part of the cyberattack delivery package, the “targets” leading to victims of cyberattacks simultaneously being victim of disinformation, and what we could call the “temptation”, ie. the lucrative possibility of both disinformation campaigns and cyberattacks.

Terrain: While there is much focus on disinformation across major social media platforms, disinformation is an inherently distributed phenomenon. Disinformation campaigns continue to make use of networking infrastructure and routing services, leveraging different levels of the internet stack. As EU DisinfoLab’s  recent investigations have demonstrated, social media platforms often serve as gateways and amplifiers of disinformation websites. In this way, disinformation and cybersecurity implicate many of the same members of the private sector and the internet technical community.

Tactics: There is significant overlap between disinformation and cybersecurity regarding the tools and methods of attack. Disinformation is increasingly part of the cyberattack delivery package, used to deliver malware by manipulating people’s fears and heightened emotions (for instance the deployment of “fearware”, a subset of phishing lures that rose in prominence during the pandemic and rely on anxieties and informational deficits). The continuous proliferation of hack and leak operations as well as the coordination between hybrid tactics (illustrated in the Sandworm case) demonstrates this convergence. There is also significant convergence between disinformation campaigns and the  tactics used in cybercrime, for example, via illegal dark web transactions, illegally obtained documents, and various kinds of fraud.

Targets: Disinformation campaigns and cyberattacks can cause similar harms and are sometimes combined to reach the same targets. While a data breach can compromise information security, so can the manipulation of data. We saw an example of this related to Covid-19 vaccines early this year, when hackers stole confidential documents from the European Medicines Agency (EMA) a European Union regulatory body to  seow mistrust in the Pfizer-BioNTech vaccine. Meanwhile, so-called “anti-democracy attacks” and “cyber influencing attacks” like media manipulation and astroturfing in the context of elections illustrate the hybrid nature of interference in democratic processes.

Temptations: Hacking, cybercrime and influence operations are lucrative endeavors, often outsourced to skilled professionals. While individuals and businesses may have increased their readiness for ransomware attacks, disinformation strategies like defamation and extortion are now being used to cause reputational damage and seek profit. These activities all have strong financial incentives and as yet insufficient consequences, due in part to the challenges of attribution but also to the lack of dissuasive/restrictive measures.

#### Counter Interpretation: Cybersecurity means protecting info and communication systems from modification or exploitation

Sean S. Costigan, Director of ITL Security and Professor at the George C. Marshall European Center for Security Studies, and Michael A. Hennessy 16, scholar of Canadian foreign, defense and naval history, British Columbia graduate, “Cybersecurity: A Generic Reference Curiculum,” July 2016, https://www.nato.int/nato\_static\_fl2014/assets/pdf/pdf\_2016\_10/1610-cybersecurity-curriculum.pdf

For **definitional clarity**, we have relied on the **U.S. National Institute of Standards and Technology** (NIST**) definition** of cyberspace, the interdependent network of information technology infrastructures, which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers….” **Cybersecurity** has been defined as “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation.” That basic definition shapes what we have included throughout this document.

### 2AC---T---Includes Disinfo

#### Russian infowar is specifically a cybersecurity issue---prefer ev specific to the aff and from the US Department of Justice---their ev is outdated and doesn’t assume the unique threat of Russian disinformation

Paul Cobaugh et al 18, Vice President of Narrative Strategies, a coalition of scholars and military professionals, Anastasios Arazamptis, and Justin Sherman, “An Assessment of Information War as a Cybersecurity Issue,” Real Clear Defense, 3/2/18, https://www.realcleardefense.com/articles/2018/06/18/an\_assessment\_of\_information\_warfare\_as\_a\_cybersecurity\_issue\_113541.html

Summary: **Information warfare is not new, but the evolution of cheap, accessible, and scalable cyber technologies enables it greatly**. The **U.S. Department of Justice’s** February 2018 indictment of the Internet Research Agency – one of the Russian groups behind disinformation in the 2016 American election – **establishes that information warfare is** **not just a global problem** **from** the **national security** and fact-checking perspectives**; but** **a cybersecurity issue** as well.

Text: On February 16, 2018, U.S. Department of Justice Special Counsel Robert Mueller indicted 13 Russians for interfering in the 2016 United States presidential election [1]. Beyond the important legal and political ramifications of this event, this indictment should make one thing clear: information warfare is a cybersecurity issue.

It shouldn’t be surprising that Russia created fake social media profiles to spread disinformation on sites like Facebook. This tactic had been demonstrated for some time, and the Russians have done this in numerous other countries as well[2]. Instead, what’s noteworthy about the investigation’s findings, is that Russian hackers also stole the identities of real American citizens to spread disinformation[3]. Whether the Russian hackers compromised accounts through technical hacking, social engineering, or other means, this technique proved remarkably effective; masquerading as American citizens lent significantly greater credibility to trolls (who purposely sow discord on the Internet) and bots (automated information-spreaders) that pushed Russian narratives.

Information warfare has traditionally been viewed as an issue of fact-checking or information filtering, which it certainly still is today. Nonetheless, traditional information warfare was conducted before the advent of modern cyber technologies, which have greatly changed the ways in which information campaigns are executed. Whereas historical campaigns took time to spread information and did so through in-person speeches or printed news articles, social media enables instantaneous, low-cost, and scalable access to the world’s populations, as does the simplicity of online blogging and information forgery (e.g., using software to manufacture false images). Those looking to wage information warfare can do so with relative ease in today’s digital world.

The effectiveness of modern information warfare, then, is heavily dependent upon the security of these technologies and platforms – or, in many cases, the total lack thereof. In this situation, the success of the Russian hackers was propelled by the average U.S. citizen’s ignorance of basic cyber “hygiene” rules, such as strong password creation. If cybersecurity mechanisms hadn’t failed to keep these hackers out, Russian “agents of influence” would have gained access to far fewer legitimate social media profiles – making their overall campaign significantly less effective.

To be clear, this is not to blame the campaign’s effectiveness on specific end users; with over 100,000 Facebook accounts hacked every single day we can imagine it wouldn’t be difficult for any other country to use this same technique[4]. However, it’s important to understand the relevance of cybersecurity here. User access control, strong passwords, mandated multi-factor authentication, fraud detection, and identity theft prevention were just some of the cybersecurity best practices that failed to combat Russian disinformation just as much as fact-checking mechanisms or counter-narrative strategies.

These **technical and behavioral failures** didn’t just compromise the integrity of information, a **pillar of cybersecurity**; they also enabled the campaign to become incredibly more effective. As the hackers planned to **exploit the polarized election environment,** access to American profiles made this far easier: by **manipulating** and distorting **info**rmation **to make it seem legitimate** (i.e., opinions coming from actual Americans), these Russians **undermined law enforcement operations, election processes**, and more. We are quick to ask: how much of this information was correct and how much of it wasn’t? **Who can tell whether the information originated from un-compromised, credible sources** or from credible sources that have actually been hacked?

However, we should also consider another angle: what if the hackers hadn’t won access to those American profiles in the first place? What if the hackers were forced to almost entirely use fraudulent accounts, which are prone to be detected by Facebook’s algorithms? It is for these reasons that **information warfare is** so **critical for cybersecurity**, and why **Russian information warfare campaigns of the past cannot be** equally **compared to** the **digital info**rmation **wars** of the modern era.

The global cybersecurity community can take an even greater, active role in addressing the account access component of disinformation. Additionally, those working on information warfare and other narrative strategies could leverage cybersecurity for defensive operations. Without a coordinated and integrated effort between these two sectors of the cyber and security communities, the inability to effectively combat disinformation will only continue as false information penetrates our social media feeds, news cycles, and overall public discourse.

More than ever, a demand signal is present to educate the world’s citizens on cyber risks and basic cyber “hygiene,” and to even mandate the use of multi-factor authentication, encrypted Internet connections, and other critical security features. The security of social media and other mass-content-sharing platforms has become an information warfare issue, both within respective countries and across the planet as a whole. When rhetoric and narrative can spread (or at least appear to spread) from within, the effectiveness of a campaign is amplified. The cybersecurity angle of information warfare, in addition to the misinformation, disinformation, and rhetoric itself, will remain integral to effectively combating the propaganda and narrative campaigns of the modern age.

### 1AR---W/M---No Distinction

#### We meet---no functional distinction between disinformation and cyberattacks

#### EU 21, Official EU document citing 2016 Cybersecurity Strategy, “Why Disinformation is a Cybersecurity Threat,” https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat//

Overview

The EU’s “Cybersecurity Strategy for the Digital Decade” is a compelling attempt to link the various foreign, digital, penal, and economic dimensions of the EU’s cybersecurity strategy, it is therefore essential that **disinformatio**n be **firmly included** in this frame. Especially now. Over the course of the Coronavirus pandemic, **disinformation and cyberattacks have grown in parallel,** exposing existing fragilities and novel risks. For end-users and cybersecurity professionals, the growing attack surface and the growing quantity of data make distinguishing safe and unsafe content more difficult. Meanwhile it remains all too easy to create and maintain assets for **cybercrime** and disinformation campaigns (single-use email addresses, fraudulent domains and accounts, etc.). The EU’s Cybersecurity Strategy must show an evolved understanding of what constitutes abusive and illegal behavior. **The EU should recognise** high-impact coordinated **disinfo**rmation campaigns **as cyber attacks.** This recognition will allow it to establish the frameworks needed for effective attribution and dissuasion, first and foremost by improving information sharing and situational awareness among stakeholders from both the disinformation and cybersecurity fields, as well as governments, the private sector, and the technical community.

Context: Why Disinformation is a Cybersecurity Issue

Drawing on our research into coordinated disinformation campaigns and our own experience as an NGO in the field, we wish to highlight four areas of convergence between disinformation and cybersecurity of relevance to EU policymakers: the “terrain” on which disinformation is distributed (the social web and the internet stack, networking infrastructure, routing services), the “tactics” that increasingly combine disinformation as part of the cyberattack delivery package, the “targets” leading to victims of cyberattacks simultaneously being victim of disinformation, and what we could call the “temptation”, ie. the lucrative possibility of both disinformation campaigns and cyberattacks.

Terrain: While there is much focus on disinformation across major social media platforms, disinformation is an inherently distributed phenomenon. Disinformation campaigns continue to make use of networking infrastructure and routing services, leveraging different levels of the internet stack. As EU DisinfoLab’s recent investigations have demonstrated, social media platforms often serve as gateways and amplifiers of disinformation websites. In this way, disinformation and cybersecurity implicate many of the same members of the private sector and the internet technical community.

Tactics: There is significant overlap between disinformation and cybersecurity regarding the tools and methods of attack. Disinformation is increasingly part of the cyberattack delivery package, used to deliver malware by manipulating people’s fears and heightened emotions (for instance the deployment of “fearware”, a subset of phishing lures that rose in prominence during the pandemic and rely on anxieties and informational deficits). The continuous proliferation of hack and leak operations as well as the coordination between hybrid tactics (illustrated in the Sandworm case) demonstrates this convergence. There is also significant convergence between disinformation campaigns and the tactics used in cybercrime, for example, via illegal dark web transactions, illegally obtained documents, and various kinds of fraud.

Targets: **Disinformation campaigns and cyberattacks** can cause similar harms and are sometimes combined to reach the same targets**. While a data breach can compromise information security, so can the manipulation of data.** We saw an example of this related to Covid-19 vaccines early this year, when **hackers stole confidential documents** from the European Medicines Agency (EMA) a European Union regulatory body **to sow mistrust** in the Pfizer-BioNTech vaccine. Meanwhile, so-called “anti-democracy attacks” and “cyber influencing attacks” like media manipulation and astroturfing in the context of elections **illustrate the hybrid nature** of interference in democratic processes.

Temptations: Hacking, cybercrime and influence operations are lucrative endeavors, often outsourced to skilled professionals. While individuals and businesses may have increased their readiness for ransomware attacks, disinformation strategies like defamation and extortion are now being used to cause reputational damage and seek profit. These activities all have strong financial incentives and as yet insufficient consequences, due in part to the challenges of attribution but also to the lack of dissuasive/restrictive measures.

### 1AR---C/I---DI=CS

This ev is gas

#### Preventing disinformation is cybersecurity---their ev is disinformation!

Saj Huq 20, leads cyber innovation at Plexal and is director of Lorca, the London Office for Rapid Cybersecurity Advancement, “It’s time to accept that disinformation is a cyber security issue,” Computer Weekly, 12/23/2020, https://www.computerweekly.com/opinion/Its-time-to-accept-that-disinformation-is-a-cyber-security-issue

The internet, as life-changing as it can be for digitising businesses, connecting communities and informing individuals, doesn’t come with a user guide to help us navigate it. And as people become more aware of the dark side of the web, they are looking for tools that help to defend them against campaigns designed to manipulate how they think or behave.

**Mis**information **and disinformation** are rife, but so far it’s been **seen as a challenge** for policy-makers and big tech, including social media platforms. However, because disinformation is by nature an online risk, it is a challenge **for our cyber security** ecosystem to tackle, too.

But tackling the manipulation of truth is no easy task. The sheer volume of data being created makes it hard to tell what’s real and what’s not. From destroying 5G towers to conspiracies like QAnon and unfounded concern about election fraud, distrust is becoming the default – and this **can have incredibly damaging effects** on society.

**Disinfo**rmation and **fake news** is also part of the delivery package, rather than being the end goal – it **is increasingly being used to deliver malware** by **manipulating** people’s **fears** and heightened emotions. For example, Avast has found that **fake shops claiming to sell Covid-19 cures** that use the World Health Organization’s logo were **intended to get people to download malware.**

So far, the tech sector – primarily social media companies, given that their platforms enable fake news to spread exponentially – have tried to implement some measures, with varying levels of success. For example, WhatsApp has placed a stricter limit on its message-forwarding capability and Twitter has begun to flag misleading posts.

Despite these efforts, reports stressing concerns about the issue from intelligence services and independent committees are being overlooked, while policies can’t be put in place fast enough to keep up with the ever-changing ways that fake news spreads. But it’s not just an issue of having more laws – in fact, too much regulation in some cases can be used as a guise for clamping down on free speech. We should be very wary of overusing it as a tool.

We are also seeing the rise of tech startups that are exploring ways to detect and stem the flow of disinformation, such Right of Reply, Astroscreen and Logically. These companies don’t tend to refer to themselves as cyber security companies, but you can argue that this is, in effect, what they are.

**It’s a question of definitions**: **if we agree that cyber security isn’t just about data breaches** but data integrity, then it’s clear that **these companies come under the umbrella of security.**

More than that, **disinformation has the potential to undermine national security** – and it **should be at the core of** our **cyber defences.**

However, the cyber security innovation ecosystem as a whole has been under-utilised and under-motivated to play a role in this landscape. Plenty of spinouts and startups have the tools to combat disinformation and take on botnets, such as automated threat detection, but don’t regard stemming the flow of disinformation to be in their domain.

This will change as businesses increasingly become the target of disinformation, which will create more market demand among IT teams. We are seeing cyber espionage techniques such as creating fake news to hold influential members of a competitor company ransom or damage the reputation of a brand, and this will shift our perception of the challenge as it becomes more rife in the corporate world.

Data breaches result in the loss of value, but so can data manipulation. This reflects the changing nature of cyber security at large – it’s now more about protecting an enterprise’s values, brand and reputation rather than just a network security issue.

Disinformation is still an emerging frontier for cyber security, and we will need unconventional techniques far beyond data breach notifications and regulatory fines. New alliances and partnerships must emerge between industry and government. More than that, our fundamental assumptions of what a cyber attack looks like must also evolve

But **the first step is recognising it as** a new type of online risk where effective **cyber security** is part of the solution.

### 1AR---C/I---Disinfo = Cyberattack

#### It’s definitely cybersecurity---prefer consensus of experts with an overwhelming intent to define and include---it’s the greatest cyber-threat of all!

Kevin Caramancion et al 22, internationally acclaimed author and speaker on information disorder research currently affiliated with the University at Albany, Yueqi Li, Elisabeth DuBois, Ellie Seoe Jung, College of Emergency Preparedness, Published 4/12/22, <https://www.mdpi.com/2306-5729/7/4/49/pdf?version=1649824663>

According to a report by the Institute for Public Relations, 63% of Americans view **disinformation** as **a major problem** in society, yet there are limited avenues to combat it outside of media literacy and news spaces [1]. similarly, a report by Neustar International Security Council (NISC) found that **48% of cybersecurity professionals think of disinformation as a threat**, of which **49%** say the threat is **very significant**. The study also found that 91% of cybersecurity professionals thought that stricter measures should be implemented on the Internet [2]. **The gravity of the impact** of disinformation on the confidentiality, integrity, and availability of information **makes it necessary** **to view disinformation** not simply as an error of information but **as a form of cyberattack.**

**Cybersecurity** relates to the **protection and defense of personal information, computer systems,** **and** critical **infrastructure.** Cyber threats tend to **compromise the confidentiality, integrity, and availability** of technology systems. Disinformation, the sharing of deliberately misleading or biased information, has been formally classified as an information disorder by the Council of Europe (2017) [3]. The goal of disinformation is to change an individual’s thoughts and behaviors, consequently influencing public opinion by altering one’s view of reality or accentuating one’s prior held beliefs to disrupt truth-seeking. Deceptive **information can leave people confused about basic facts and current events**, creating a dangerous situation **affecting public safety,** organizational **reputations,** or **governmental functions.** In many ways, **disinformatio**n is thus **similar to a cyberattack**, where **instead of compromising a computer system,** it **compromises our cognitive abilities**. Such disruptions have been coined **cognitive hacking**—where such practices can **result in a greater threat** than a cyberattack on critical infrastructure [4]. The **damage** caused by disinformation **can be challenging to repair**, as people form opinions based on cognitive and confirmation biases. T**he deceptive nature of disinformation is** further **accentuated by** economic pressures and advertisement-centric **models that incentivize disinformation** to overload information channels, often **drowning the truth.** **Just as tech**nology and **social media expansion** **increase cybersecurity risks,** **they exacerbate the** impact of **disinformation.**

# Disads

## DOD Tradeoff

### No link---normal means

#### Normal means is the CRIF---no tradeoff with Taiwan.

USC 22, US Code, 1-3-2022, "22 USC CHAPTER 102, SUBCHAPTER II: COUNTERING RUSSIAN INFLUENCE IN EUROPE AND EURASIA," <https://uscode.house.gov/view.xhtml?path=/prelim@title22/chapter102/subchapter2&edition=prelim>, cy

§9543. Coordinating aid and assistance across Europe and Eurasia

(a) Authorization of appropriations

There are authorized to be appropriated for the Countering Russian Influence Fund $250,000,000 for fiscal years 2020, 2021, 2022, and 2023.

(b) Use of funds

Amounts in the Countering Russian Influence Fund shall be used to effectively implement, prioritized in the following order and subject to the availability of funds, the following goals:

(1) To assist in protecting critical infrastructure and electoral mechanisms from cyberattacks in the following countries:

(A) Countries that are members of the North Atlantic Treaty Organization or the European Union that the Secretary of State determines—

(i) are vulnerable to influence by the Russian Federation; and

(ii) lack the economic capability to effectively respond to aggression by the Russian Federation without the support of the United States.

(B) Countries that are participating in the enlargement process of the North Atlantic Treaty Organization or the European Union, including Albania, Bosnia and Herzegovina, Georgia, Macedonia, Moldova, Kosovo, Serbia, and Ukraine.

(2) To combat corruption, improve the rule of law, and otherwise strengthen independent judiciaries and prosecutors general offices in the countries described in paragraph (1).

(3) To respond to the humanitarian crises and instability caused or aggravated by the invasions and occupations of Georgia and Ukraine by the Russian Federation.

(4) To improve participatory legislative processes and legal education, political transparency and competition, and compliance with international obligations in the countries described in paragraph (1).

(5) To build the capacity of civil society, media, and other nongovernmental organizations countering the influence and propaganda of the Russian Federation to combat corruption, prioritize access to truthful information, and operate freely in all regions in the countries described in paragraph (1).

(6) To assist the Secretary of State in executing the functions specified in section 1287(b) of the National Defense Authorization Act for Fiscal Year 2017 (Public Law 114–328; 22 U.S.C. 2656 note) for the purposes of recognizing, understanding, exposing, and countering propaganda and disinformation efforts by foreign governments, in coordination with the relevant regional Assistant Secretary or Assistant Secretaries of the Department of State.

(7) To assist United States agencies that operate under the foreign policy guidance of the Secretary of State in providing assistance under section 9563 of this title.

### No link---burden sharing

#### The aff shares the fiscal burden with allies---solves tradeoff.

Melissa Dalton and Hijab Shah 20, senior fellow with CSIS, associate fellow with the International Security Program at CSIS, “Partners, Not Proxies: Capacity Building in Hybrid Warfare.” Center for Strategic and International Studies (CSIS), 2020. <http://www.jstor.org/stable/resrep24784>, cy

Identify How Burden-sharing Creates Opportunities:

Burden sharing enables allies to optimize for their comparative advantages based on political, economic, cultural, operational, and informational capabilities. It not only makes fiscal and strategic sense, but it also can open opportunities for future combined approaches to planning, resourcing, and execution. For example, pooled donor funds used for northeast Syria stabilization enabled coalition civil-military operations to proceed even as direct U.S. political and fiscal support waned. This model could be replicated in terms of its bureaucratic and financial structures for other contexts.

Create Dynamic Campaign Approaches:

Hybrid warfare environments will move swiftly past static coalition plans, as competitors routinely test the boundaries and thresholds of what the allies will abide, including coercion of partner institutions, disinformation and misinformation operations, and cyber intrusions. The allies must create dynamic campaigns with an adaptable mandate for partners that can flex to the evolving threats from competitors while bound by the guidelines discussed above. Combined allied planning for campaign design and monitoring and evaluation of its implementation will be important

## Politics

### 2AC---No Link---CIA Normal Means

#### Normal means is CIA---shields the link.

Catherine A. Theohary 18, Specialist in National Security Policy, Cyber and Information Operations, “Information Warfare: Issues for Congress,” Congressional Research Service, crsreport: R45142 version 5 //chico

The Central Intelligence Agency (CIA) has a history of conducting information warfare or psychological operations, particularly with respect to countering guerilla organizations abroad. Monitoring Soviet disinformation was once solely the purview of the CIA, until the Active Measures Working Group was established in 1981 and tasked with coordinating the activities of multiple, disparate activities within the U.S. government.

# Counterplans

## DoS

### Note

DOD key/military key from the solvency section should be incorporated into DoS 2AC

### 2AC---DoS CP---PDCP

#### SC encompasses the DoS---SA is merely a subset of SC.

DSCA 14, Defense Security Cooperation Agency, 2014, “Chapter 1: Introduction,” https://www.dsca.mil/sites/default/files/1-introduction\_0.pdf, RMax

1.2 SECURITY COOPERATION

The Department of Defense (DoD) broadly defines Security Cooperation (SC) as those activities conducted with allies and friendly nations to build relationships that promote specified U.S. interests, build allied and friendly nation capabilities for self-defense and coalition operations, and provide U.S. forces with peacetime and contingency access. SC encompasses a combination of legal authorities, annual appropriations, organizations, and initiatives from within DoD, Department of State (DoS), or the Executive Office of the President (EOP) resources.

1.2.1 SECURITY ASSISTANCE

As a subset of SC, Security Assistance (SA) encompasses a group of programs, authorized by law, through which the DoD or commercial contractors provide defense articles, services, and training in support of national security policies and objectives. The Defense Security Cooperation Agency (DSCA) is responsible for supervising the implementation and execution of worldwide SA programs to include Foreign Military Sales (FMS) and Foreign Military Financing (FMF), and for DoD appropriated programs which implement the Secretary of Defense (SECDEF) Security Cooperation Plan, to include Regional Centers (RC) for Security Studies; Warsaw Partnership for Peace (PfP); Counter Terrorism Fellowship Program (CTFP); Stability Operations Fellowship Program (SOFP); Irregular Warfare and Stability, Security, Transition and International Outreach (IWSSTIO); and International Programs Security Requirements Course (IPSR); Coalition Support Funds (CSF); Global Train and Equip (T&E); and the Overseas Humanitarian, Disaster and Civic Aid Appropriation (OHDACA).

#### GEC is under the DOS.

Catherine A. Theohary 18, Specialist in National Security Policy, Cyber and Information Operations, “Information Warfare: Issues for Congress,” Congressional Research Service, crsreport: R45142 version 5 //chico

Who Is Responsible for the “I” in DIME?

As a source of national power, information is a critical strategic asset, and currently the information element is shared within the U.S. government.21 During the Cold War, the U.S. Information Agency (USIA) was responsible for supporting U.S. national interests abroad through information dissemination. It was later folded into the State Department’s Bureau of Public Diplomacy and Public Affairs before being disbanded in 1999. Today, the Department of State-led interagency Global Engagement Center (GEC) is charged with many of the former USIA activities. According to Steve Goldstein, then Undersecretary for Public Diplomacy, the GEC recently launched a new $40 million initiative to battle state-sponsored disinformation and propaganda targeting the United States and its interests.22 It also plans to launch a series of pilot projects with the Department of Defense, using additional DOD funding.

### 2AC---DoS CP---Links to DOD DA

#### The DoS drains DoD resources

Pecquet 22 (Julian Pecquet, the founder and editor of Foreign Lobby Report, a US news site that offers comprehensive coverage of foreign influence operations in Washington and beyond, 5-25-2022 "US looks to expose Russian propaganda in Africa," Africa Report, https://www.theafricareport.com/207268/us-looks-to-expose-russian-propaganda-in-africa/, DOA: 6-30-2022//Smarx Ahsan---Edited for Spelling)

The State Department's counter-propaganda arm has released its first-ever report on Russian disinformation in Africa as the Joe Biden administration looks to expose the Kremlin following the invasion of Ukraine.

The Global Engagement Centre, which leads and coordinates US efforts to “recognize, understand, expose, and counter foreign propaganda and disinformation”, released a three-page bulletin on Russian activities on 24 May. The report focuses particularly on Mali and other Sahel countries where the Kremlin-linked Wagner Group of mercenaries operates.

“Russia deploys disinformation across different continents for varied objectives, often working through tested proxies to support Kremlin foreign policy objectives indirectly, which provides a level of deniability,” the report states. “In some parts of Africa – including, most recently, Mali – Kremlin-linked proxies exploit instability to gain influence, particularly through disinformation and the deployment of the Wagner Group forces.”

A spokesperson for the State Department describes the report as “part of the State Department’s overall public exposure efforts to counter Russian disinformation”.

“We are releasing these substantive products to the public to counter Russia’s false narratives and propaganda with reporting that shines the light on Kremlin lies,” the spokesperson tells The Africa Report. “This bulletin is our first on Russia’s disinformation efforts in Africa.”

Evolving target

The Global Engagement Centre was created under President Barack Obama in March 2016. Its original mission was to contest the “information battlespace” with the Islamic State and “break the recruiting efforts of violent extremists abroad”, according to its first coordinator, Michael Lumpkin.

Disinformation is one of the Kremlin’s most important and far-reaching weapons

Housed at the State Department, the interagency organization also draws on staff from the departments of Defence, Treasury, Justice and Homeland Security as well as the Intelligence Community and the US Agency for International Development. Its mandate: to coordinate, integrate, and synchronize government-wide communications with foreign audiences to counter disinformation campaigns.

### 2AC---DoS CP---DOD Key

#### DoD action is key---military capabilities are significantly lacking.

James Davitch 22, U.S. Air Force Lieutenant Colonel, M.S. in Airpower Strategy and Technology Integration from Air University, M.A. in Interdisciplinary from the University of Oklahoma, March 2022, “Dealing with Disinformation: The Barriers to Success and a Path Forward,” *Air and Space Operations Review*, Vol. 1, Issue 1, pp. 4-17, RMax

The US military’s approach to information warfare relies on personnel, organizations, techniques, and procedures grounded in conventional doctrine.1 When it comes to tactical information operations, instead of doing what the Joint force needs them to do, US military members do what they know how to do. This reality leaves combatant commanders at a comparative disadvantage relative to foes who use the information space to exploit a vulnerability of the United States while avoiding its historic conventional military strengths. Winning in the information domain today and tomorrow will require the Department of Defense to acquire a new capability. In conflicts with peer competitors, clear, concise, and correct communication is a major weapon of warfare.

This article advocates for a new kind of fires team to assist with this problem. The proposed “anti-disinformation” cell would compete in the cognitive rather than physical domain. The Department should begin to think about force packaging that includes not only traditional military hardware like ships, aircraft, and munitions, but also people who can help understand the geopolitical situation and communicate in a way advantageous for US national interests. Recommendations in this article are also pertinent to civilian national security leaders as they consider ways to respond to adversary moves and inform public opinion to help achieve political ends.

In a prescient 1997 essay, Richard Szafranski lays bare the consequences of falling behind adversaries who attempt to gain information advantages. When a citizenry’s will, their country’s technological edge, and that nation’s claim to the moral high ground are in alignment, the pursuit of the profession of arms is useful and important. “If, however, the moral high ground is lost, a domino effect occurs: public support is lost, the technological high ground is lost, and the armed forces are lost.”2

#### CYBERCOM action is key.

Simon Handler 21, assistant director of the Atlantic Council’s Cyber Statecraft Initiative under the Snowcroft Center for Strategy and Security, former special assistant in the U.S. Senate; and Justin Sherman, a fellow at the Atlantic Council’s Cyber Statecraft Initiative, 4/22/2021, "The United States Needs a Public Strategy for Deterring Disinformation," National Interest, <https://nationalinterest.org/feature/united-states-needs-public-strategy-deterring-disinformation-183373>, RMax, language edited in brackets

In cyberspace, U.S. Cyber Command (USCYBERCOM) can play an important role in disrupting adversary disinformation campaigns. Operations such as USCYBERCOM’s campaign against the TrickBot botnet in the lead up to the 2020 general election and its paralysis [stoppage] of Russia’s Internet Research Agency on the day of the 2018 midterms must continue for effective deterrence by denial.

Information conflict is reshaping the future of cyber conflict. If the U.S. national security community continues to focus just on the 1s and 0s, it will doom the United States to continually suffer successful attacks against its democracy and security. Similarly, to the extent that the government continues to pursue cyber conflict as a purely government problem, as opposed to part of a broader contest involving the likes of media outlets and internet platforms, the United States will fail to mount the society-wide response needed to effectively deter harmful foreign activities and better compete in this contest for information.

### 2AC---DoS CP---DoS Fails

#### The DoS fails---surge capacity, expeditionary capability, and flexibility limit their effectiveness.

Christopher Paul 16, senior social scientist at the RAND corporation, Ph.D. from University of California, Los Angeles, 9/1/2016, “Enhancing US Efforts to Inform, Influence, and Persuade,” *Parameters*, Vol. 46, No. 3, <https://doi.org/10.55540/0031-1723.2756>, RMax

Also, Defense responsibilities for contingency response necessitate retaining capabilities to inform, influence, and persuade. Even the most robust State Department imaginable will lack the kind of surge capacity and expeditionary capability needed to respond to the crises and contingencies for which our military prepares. When the US military presence in a foreign country expands from negligible to massive, who will be alongside the operating forces, explaining and making their presence palatable? The answer is military communicators. If all the military communicators went away, no one would conduct critical inform, influence, and persuade missions at the outset of an emergent crisis, which is why the DoD needs to remain capable. In fact, Defense personnel, as argued above, should continue to become more capable, given the possible savings for other defense capabilities.

Further, military leaders should be encouraged to use informational combat power as part of their combined arms approach to prevail over our nation’s foes, rather than outsourcing the capability to other parts of the government.

The existing structure and organization at DoS limits its absorptive capacity for quickly building new or assuming existing responsibilities for informing, influencing, and persuading. Considerably smaller than DoD, State personnel allocations are also less flexible. Culturally, the State Department views its primary mission as traditional state-to-state diplomacy, not public diplomacy, and the public diplomacy apparatus is currently quite small.30 To become the home for government capabilities in this area, DoS will need to pursue organizational and cultural changes and increase or transfer resource allocations in moderate, absorbable amounts.

## International Law

### I-Law Fails

#### I-law constraints fail.

Dr. Waseem Qureshi 20, Advocate Supreme Court of Pakistan, 2020, “Information Warfare, International Law, and the Changing Battlefield,” *Fordham International Law Journal*, Vol. 43, No. 4, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=2786&context=ilj, RMax

V. INTERNATIONAL LAW AND INFORMATION WARFARE

This Part of the Article includes an explanation of the relevant rules of international law that can be applied to the sphere of information warfare. Some of these rules—for instance the Outer Space Treaty 1967—end up indirectly facilitating the conditions that support the continuation of information warfare, leaving information warfare unchecked under international law. On the other hand, the complex and variegated arena of information warfare makes it challenging for international norms and principles to regulate and control information operations.177 For instance, although the law of war, the law of armed conflict, and IHL make attempts to regulate the conduct of actors involved in information warfare, the intangibility of the damage caused by information warfare makes it difficult for IHL to impose restrictions on information warfare.178

A. The Law of War

The law of war or the law of armed conflict protects civilians and noncombatants in an armed conflict.179 Likewise, the law of war also attempts to protect civilians from any information warfare attack. That is, the parties engaged in information warfare must cause no harm to the civilian population.180 This rule can be applied to the activity of hacking or the disruption of any technological transmission of an adversary state by a wager of information warfare.181 If such an activity harms civilians in any manner—for instance in disrupting their businesses, daily routines, etc.—then such an activity ought to be considered illegal under IHL or the law of war.182 Several other inferences can similarly be made that could ensure protection for civilians and noncombatants.183

B. Challenges Faced by International Law in Regulating Information Warfare

In fact, there are many challenges faced by international law, in particular by IHL or the law of war, in regulating information warfare.184 These challenges mainly derive from the intangibility of the damage brought up by information warfare. Unfortunately, because of such challenges, international law becomes paralyzed [stymied] in an attempt to regulate or control the broad and complicated field of information warfare.185

1. Intangibility

The essential challenge to international law posed by information warfare is the intangibility of the damage caused by the information operations instituted by an entity against its adversary.186 International law, in particular the international law of armed conflict, is silent on any intangible damage caused to an adversary in times of war and peace.187 Therefore, it becomes difficult for international law to regulate or restrict those information operations that specifically produce intangible damages in times of war and peace.188

## Private Sector

### Private Sector Fails

#### Private sector actions fail. Enforcement gets politicized, technical limitations, perceived as overreach, identification is difficult, and actors shift to other platforms or make new accounts.

Kathleen Mary Carley 22, Professor of Computer Science, Institute for Software Research at Carnegie Mellon University, “COVID-19 Disinformation: A Multi-National, Whole of Society Perspective,” Advanced Sciences and Technologies for Security Applications, ISBN 978-3-030-94824-5, Springer Cham, DOI: <https://doi.org/10.1007/978-3-030-94825-2>, p. 13 (found under, “Chapter 1: A Political Disinfodemic”) //chico

On the good news side, social media platforms took action and new laws regulating disinformation came into play. However, many of the laws are difficult to enforce. Actions taken by the platforms have not been universally welcomed as: they often appear capricious, may be interfering with free speech, might not be applied in a uniform non-partisan global fashion, may be based on biased algorithms, afford the platforms too much power, and interfere with science. The global nature of social media, countering laws focused on freedom of speech, and technical difficulties in identifying the actual human behind specific posts effectively makes policy and law enforcement difficult. From a platform perspective it is important to note that there is an ecology of platforms. Information or actors banned from one platform may simply migrate to another platform. For disinformation, it often simultaneously exists on multiple platforms—so banning it from one is a temporary measure as it will simply get rewritten, turned into a meme, or combined with other information and then re-appear on the platform that banned it. Since a typical user employs eight social media platforms, it is relatively easy for anyone to move disinformation between platforms.

# Kritiks

## Broad/1AC

### 1AC---Framework

#### The 1AC’s model is pedagogically beneficial---anticipating cyber futures teaches political efficacy and strategy.

Andreas Haggman 20, Ph.D. in cyber security from Royal Holloway University, 2020, “Imagining and Anticipating Cyber Futures with Games,” *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Chapter 11, https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030\_Horizon-Scanning-and-Analysis.pdf, RMax

2. FUTURES AND IMAGINATION

The further we seek to gaze into the future, the more we have to employ our imaginative rather than our analytical faculties because of the increased uncertainty. Just consider science fiction literature, which often seems to become more far-fetched the further into the future it is set. At the same time, futures imagined on a shorter time frame can often be realistic; consider the apparent prescience of some of the works from authors like H. G. Wells (1908).

When we play games, we exercise our ability to imagine the future because we need to imagine the context in which future game actions will take place. After studying competitive chess players, Gary Fine (2014) concluded that players’ strategy, consisting of a series of planned moves—or ‘the line’—is the core mechanic in that game, not the moves themselves (p. 323). These ‘lines’ require an ability to anticipate the opponent’s strategy to construct the imagined game future.

Chess, however, is a highly abstract game and teaches us little about contemporary strategy or politics. In his later life, political theorist Guy Debord attempted to amalgamate the imaginative capacities of wargaming with his leftist political ideals. His Game of War set out to capture the struggle between a bleak ‘historical present’ and an unattainable future of ‘utopian imagination’ (Galloway, 2009: pp. 151-152). Ultimately, Debord became obsessed with ‘the sublimation of antagonistic desire into an abstract rulebook’ and Game of War ended up as something which looked more like chess with some added mechanics around military logistics than a game of political strife (Galloway, 2009: p. 28).

Perhaps Debord, and others seeking to invoke imagined futures, can learn from Pericles of ancient Athens. Pericles was a master orator, able to convincingly convey potential futures to spur Athenians to action. What made Periclean futures so potent was their grounding in reality. According to Lawrence Freedman (2013), Pericles drew ‘from an existing reality but moved beyond it’ and the plausibility of a future was ‘derived from its practicability’ (p. 49). As an example, in cyber security, a future where only friendly actors derive the benefits from a technology like quantum computing seems more Debordian than Periclean. Instead, an imagined future involving quantum computing must consider the viability of this technology also being in the hands of hostile actors.

When designing wargames, the key to success is to understand the purpose of the game and the future it is intended to explore. A tactical awareness training tool might lend itself to a chess-like design where players can imagine ‘lines’ such as hopping from node to node while penetrating a network. Conversely, a strategic game exploring international political dimensions may need less of a strict rule set and instead provide realistic foundations for players to extrapolate their own imagined futures.

3. FUTURES AND ANTICIPATION

As an extension of imagining futures, anticipation has been described by Vincanne Adams et al. (2009) as ‘an epistemic orientation towards the future’ (p. 254). In other words, anticipating futures involves creating knowledge about the future, thereby negating surprise. In everyday usage, ‘surprise’ can be used either positively or negatively—compare a surprise birthday party to a surprise conference paper rejection. Wargaming is often concerned with negating negative surprises. David Hulse et al. (2016) identify that a core use of modelling (closely allied to wargaming) is understanding ‘when, where and how “reducible ignorance” can be most effectually reduced vis-a-vis anticipated surprises’ (p. 41). As tools for anticipating futures, wargames enable knowledge creation which can help reduce surprise.

An important aspect of anticipation is the emotion contained within surprises. A birthday party is a pleasant surprise, while a paper rejection is unpleasant. When it comes to drivers of human behaviour, Roy Baumeister et al. (2007) attest that ‘anticipation of emotion is more important than the actual emotion’ (p. 174). While writing a paper, an author might contemplate the hurt associated with rejection and be compelled to make a greater effort to write a brilliant paper.

Because of its ludic nature, wargaming is closely associated with competition and personal performance. Wargames usually have winners and losers; the winners experience joy, elation and satisfaction, the losers are disappointed, angry and dissatisfied. One of the insidious features of wargaming is that players’ in-game behaviour can be driven by anticipation of these emotions, rather than reasoned actions. However, the other side of this coin is that players become better prepared for the future by anticipating and eventually experiencing these emotions in the safety of the game environment. Wargames can help desensitise players to the extremes of emotions contained within surprises—or, indeed, other adverse experiences such as frustration, confusion, information deficiency or excess—so that when they encounter similar surprises and emotions in real life, the effects on their behaviour are not as drastic.

4. CYBER FUTURES

As domains of warfare have increased from two (land and sea), to three (air), to four (cyberspace) and five (space) (NATO, 2020), wargaming has been increasingly challenged to tackle the technological developments of the day. Sharon Ghamari-Tabrizi (2000) writes that during the Cold War, ‘the technical horizon within which future wars would be fought would change constantly, albeit uncertainly’ (p. 164). In the Cold War context, nuclear weapons dominated wargaming scenarios, yet the ‘technical horizon’ did not fluctuate as wildly as game designers of the time might have envisaged. With the benefit of hindsight, we can say that nuclear weapons of greater yields could be delivered further and faster in the 1980s than the 1950s, but the overall nature of these weapons did not change, and indeed remains the same today.

With cyber capabilities, wargaming finds itself looking at another technical horizon. The past 15 years have only provided glimpses of what cyber operations might look like at full scale—Estonia in 2007, Stuxnet in 2010 and NotPetya in 2017 are excellent examples. It is possible to imagine a future where cities go dark as power plants are shut down at the whim of an adversary. Indeed, such doom-mongering has been successful at capturing public and political attention—not dissimilar from the scenarios of the Cold War.

However, perhaps these examples are more than glimpses—do these totemic operations represent the zenith of cyber capabilities? It is possible to imagine a future not unlike today where cyber capabilities are used sparingly because of their expense and their limited and unpredictable effects.

Or perhaps both of these imagined futures are incorrect and cyber capabilities have yet to reveal their final form. In the early 20th century, reams of strategic thinking were expounded on the novel concept of airpower and yet the technology that prompted this thinking was airships, not aeroplanes— recall that the Wright Flyer first took off in 1903, and that Giulio Douhet’s seminal The Command of the Air was not published until 1921. Strategic thinking around cyber has similarly boomed in the early 21st century, but cyber capabilities of the future may make Stuxnet look like an inflatable blimp by comparison. The point here is that it is difficult to know when, or even if, technology will outpace strategic thinking.

5. CYBER WARGAMING

When imagining and anticipating cyber futures, the lesson for wargaming is similar as for Wells’ science fiction, Wells himself being an avid wargamer. In The War in the Air, Wells’ characterisation of airpower was not wholly incorrect, though it was exaggerated because the technology in the novel was swiftly superseded. In cyber wargames, the technical aspects of cyber capabilities should be deemphasised and potential effects should be based on current observable reality rather than unsubstantiated hype.

That is not to say that cyber wargames should ignore technology. After all, cyber is a technical domain, not a natural one. But cyber wargames at the strategic level should not get bogged down in the relative merits of, say, ElGamal versus RSA encryption algorithms. Instead, the effect ‘data is encrypted’ would reasonably be the level of detail required for strategy games. By focusing away from the micro-level details of technology, participants in wargames can explore the macro-level strategic and political reasons why a cyber attack might occur and how to respond to it, without being burdened with the tactical minutiae of cyber security. These minutiae have their place in attack-defence exercises and capture-the-flag events, but these types of games do not readily lend themselves to the imaginative and anticipatory dimensions of wargaming.

From his experience of the 2010 Schriever Wargame organised by the US Air Force, George Foresman, former Undersecretary at the US Department of Homeland Security, stated that ‘the lessons identified [...] are not futuristic concepts’ (2010: p. 8). This sentiment seems to intimate a sweet spot for wargames to hit: create a scenario that participants can imagine as a plausible future and from which they can anticipate and learn lessons; but avoid a scenario that is overly ‘futuristic’ and which participants relegate to the realms of science fiction.

For those seeking to use wargames and who want to hit that sweet spot while avoiding the trappings of technology, a good starting point would be to keep it simple. A game does not necessarily need intricate graphics and advanced gameplay mechanics to be effective. For example, sample games found in Dark Guest (Curry & Rice, 2013) or The Handbook of Cyber Wargames (Curry & Drage, 2020) require only basic gaming paraphernalia – in many cases just a die. The real value comes from the players rather than the games themselves.

In the author’s own experience, a cyber strategy wargame with a moderate degree of gaming paraphernalia has been successful at eliciting learning moments for players (Haggman, 2019). The game in question was loosely based on the UK National Cyber Security Strategy (HM Government, 2016) and used a game board, cards, dice, player characters and a set of rules to convey some limited detail about cyber security topics and dynamics. This was less simple than a matrix game but provided very direct discussion opportunities because players could assess the game components. Asking players what they would add to the game was often revealing in terms of what they understood to be important in cyber security, at both strategic and operational levels. Moreover, because the game was relatively easy to learn and purposely designed to be fun, it was highly engaging for players. Overcomplication can discourage player engagement. Simplicity incites imagination and anticipation, thereby realising the benefits associated with wargaming futures.

### 1AC---Defensive Realism

#### Defensive realism best describes Russian info warfare.

Media Ajir 18, and Bethany Vailliant, instructors of political science and international relations at the University of Nebraska, Fall 2018, “Russian Information Warfare: Implications for Deterrence Theory,” *Strategic Studies Quarterly*, Vol. 12, No. 3, p. 70-89, https://www.jstor.org/stable/10.2307/26481910, RMax, language edited in brackets

While it is a common perception in the West that Russia is acting offensively, there lies explanatory power as well in understanding that the Russians view their actions as being defensive in nature. In the Russian view, technology is a particular method the West uses to “attack” it—but less for inflicting crippling [brutal] blows than as a way to spread unacceptable ideas, norms, practices, and behaviors. Russian intelligence services are increasingly worried about the potential detrimental national security effects arising from the internet. In fact, the vast majority of Russian writing on information conflict is defensive in tone and focused on information security due to their perception of the global information space as a serious threat to Russian sovereignty. The original Russian source government document “Doctrine of Information Security of the Russian Federation” states that there is a trend in foreign media to publish biased information about Russian state policy and that there is discrimination against Russian mass media. Additionally, they observe what they perceive as increasing pressure on the Russian population through Western propaganda efforts that “erode Russian traditional and spiritual and moral values.”2 The belief that the West was heavily involved in the color revolutions and in the Arab Spring, as well as with the protests preceding Putin’s reelection in 2012, is a deeply held one. In response, Russia views the media and the internet as tools to defend its authoritarian state and ideology both at home and abroad through dissemination of its own views and propaganda efforts. To understand this fully, one must first consider Russian information warfare concepts before examining three specific Russian information warfare tools.

### 1AC---NATO Good

#### Their criticism of LIO and NATO are essentialist. Even though not perfect, only multilateral action within NATO can combat fascism and create global peace.

Slavoj Žižek 22, Professor of Philosophy at the European Graduate School, “What Does Defending Europe Mean?” Op-ed featured in Project Syndicate (PS), Published Mar. 2 2022, <https://www.project-syndicate.org/commentary/europe-unequal-treatment-of-refugees-exposed-by-ukraine-by-slavoj-zizek-2022-03> //chico

And now some who call themselves leftists (I wouldn’t) are blaming the West for the fact that US President Joe Biden was right about Putin’s intentions. The argument is well-known: NATO was slowly encircling Russia, fomenting color revolutions in its near-abroad, and ignoring the reasonable fears of a country that had been attacked from the West in the last century.

There is, of course, an element of truth here. But saying only this is equivalent to justifying Hitler by blaming the unjust Treaty of Versailles. Worse, it concedes that big powers have the right to spheres of influence, to which all others must submit for the sake of global stability. Putin’s assumption that international relations is a contest of great powers is reflected in his repeated claim that he had no choice but to intervene militarily in Ukraine.

Is that true? Is the problem really Ukrainian fascism? The question is better directed at Putin’s Russia. Putin’s intellectual lodestar is Ivan Ilyin, whose works are back in print and given to state apparatchiks and military conscripts. After being expelled from the Soviet Union in the early 1920s, Ilyin advocated a Russian version of fascism: the state as an organic community led by a paternal monarch, in which freedom is knowing one’s place. The purpose of voting for Ilyin (and for Putin) is to express collective support for the leader, not to legitimate or choose him.

Aleksandr Dugin, Putin’s court-philosopher, closely follows in Ilyin’s steps, adding a postmodern garnish of historicist relativism:

“[E]very so-called truth is a matter of believing. So we believe in what we do, we believe in what we say. And that is the only way to define the truth. So we have our special Russian truth that you need to accept. If the United States does not want to start a war, you should recognize that [the] United States is not any more a unique master. And [with] the situation in Syria and Ukraine, Russia says, ‘No you are not any more the boss.’ That is the question of who rules the world. Only war could decide really.”

But what about the people of Syria and Ukraine? Can they also choose their truth or are they just a battlefield for would-be world rulers?

The idea that each “way of life” has its own truth is what endears Putin to right-wing populists like former US President Donald Trump, who praised Russia’s invasion of Ukraine as the act of a “genius.” And the feeling is mutual: When Putin talks about “denazification” in Ukraine, we should bear in mind his support for Marine le Pen’s National Rally in France, Matteo Salvini’s Lega in Italy, and other actual neo-fascist movements.

The “Russian truth” is only a convenient myth to justify Putin’s imperial vision, and the best way for Europe to counter it is to build bridges to developing and emerging countries, many of which have a long list of justified grievances against Western colonization and exploitation. It’s not enough to “defend Europe.” The true task is to persuade other countries that the West can offer them better choices than Russia or China can. And the only way to achieve that is to change ourselves by ruthlessly uprooting neo-colonialism, even when it comes packaged as humanitarian help.

Are we ready to prove that in defending Europe, we are fighting for freedom everywhere? Our disgraceful refusal to treat refugees equally sends the world a very different message.

## Security K

### 2AC---Link Turn

#### Information warfare orients our subjectivities toward ontological securitization and stability that turn the K.

Derek Bolton 21, Lecturer at the University of Bath, 2021, “Targeting Ontological Security: Information Warfare in the Modern Age,” *Political Psychology*, Vol. 42, No. 1, https://doi.org/10.1111/pops.12691, RMax

Our view of how states interact and compete is expanded when we combine IW with OS. Much as with any other interest (e.g., physical or economic security), the desire for OS can be manipulated and undermined. Facets of IW can thus be viewed as part of a spectrum of tactics used to target the endogenous sources of OS. While representational force and counterpower both target subjectivity, their applicability is limited, either to when a victim’s subjectivity depends upon its relationship with the speaker or to large egoistical states, respectively. Moreover, their overt nature means the speaker is exposed to backlash, potentially diluting the impact external actors have. Given these limitations, actors have impetus to pursue IW. By covertly perverting the information landscape, IW can manipulate domestic efforts at relating events or policies to national narrative, making certain options appear more/less shameful. Actors might also polarize debates between subgroups in an effort to undermine the perceived stability of the national narrative, erode a sense of home, and increase challenges to the positive recognition of subgroups. As seen during the 2016 U.S. election, Russia was able to exploit technological advances to exacerbate and polarize debates and foster misperceptions between ideological cleavages, eroding the foundations of OS and generating anxiety. The result was a divided American populace preoccupied with regaining stability and the preservation of specific interpretations of the meta-national narrative.

### 2AC---AT: Otherization Link

#### No turns case---hostility is malleable.

Mario Baumann 20, Brussels School of International Studies, February 2020, “‘Propaganda Fights’ and ‘Disinformation Campaigns’: the discourse on information warfare in Russia-West relations,” *Contemporary Politics*, Vol. 26, Issue 3, https://doi-org.proxy.lib.umich.edu/10.1080/13569775.2020.1728612, RMax

Conclusion and implications

This article has raised questions about the role of the prevalent discourses on information warfare in Russia and the West for the relations between them. On the basis of poststructuralist theoretical premises, it analysed Russian and German media publications since the onset of the Ukrainian crisis in 2014. The comparative Discourse Analysis revealed an ambiguous positioning of a Russian and a Western Self towards each other. With representations building on long-established genealogies, Russian and Western discourses engage interactively in political struggles.

But what are the implications of this discussion for Russia and the West as (discursive) subjects engaging in Russia-West relations? Wæver (2002) contends that ‘[overall] policy in particular must hold a definite relationship to discursive structures’ since it defines what is deemed sayable or doable (p. 27). This follows the Foucauldian tradition, seeking to elucidate ‘the rules for what can and cannot be said and the rules for what is considered true and false’ (Jorgensen & Phillips, 2002, pp. 12–13). It seems obvious that currently, both subjects are constrained by a rather hostile discourse that constructs the respective Other as offensive opponent. That the domestic discourse constrains extreme dissident positions became visible when Donald Trump was heavily criticised by both Democrats and Republicans for doubting Russian interference in the United States’ elections during a press conference with Putin in 2018.

However, the preceding discussion has shown, firstly, that these hostile dispositions are relatively malleable. Rhetoric and policies in the longer run are thus not necessarily doomed to remain confrontational. Moreover, the fact that the Western derogatory discourse is stuck primarily with the Russian government and President Putin suggests that any political change in Russia could facilitate a major change in discourse. Secondly, the sedimented nature of liberal ideals in the discursive structure implies that both Russia and the West still speak to some extent the same language. The current confrontational posture is thus not necessarily a long-term development. However, given that even the most sedimented discursive structures are not immune to change, it is likely that the antagonistic discourse becomes more fundamental, should the current cool down of relations persist. Finally, given that both discourses reveal each other’s contingency by representing different, alternative interpretations of the world, neither appears objective. For all participants within the West and Russia it thus appears less natural what is ‘right’ or ‘wrong’, ‘true’ or ‘false’.

### 2AC---Ontological Security

#### The drive for ontological security is inevitable but InfoWar flips that, generating mental crisis and polarizing nation-states further.

\*IW = Information War

\*OS = Ontological Security

Derek Bolton 20, received his PhD from the University, undertakes research in the realm of international security and Foreign Policy Analysis. Derek’s work has paid special attention to the role of identity in decision-making of Bath, “Targeting Ontological Security: Information Warfare in the Modern Age”, DOI: 10.1111/pops.12691 //lenox

While sharing similar sentimentalities regarding how states “trap” one another, Steele (2007) views biographical narratives as the foundation of subjectivity. He argues that when responding to humanitarian crises, rather than appeal to international identities or norms, which large and proud states are likely to be unmoved by, reflexive discourse becomes a potent tool. Here weaker actors use rhetoric that openly acknowledges their asymmetric power relationship while also highlighting the incongruence between the larger state’s self-narrative and its failure to intervene, thereby provoking shame and stimulating behavioral change. This can be seen in the U.S. decision to increase funding for Asian tsunami relief after being labeled “stingy” by the U.N Undersecretary-General for Humanitarian Affairs. Reflexive discourse is one of three forms of counterpower—a challenge towards the aesthetics of a state. In other words, if the state is “a work of art,” counterpower are instances that stimulate the state to “engage its own ‘art of living’” (Steele, 2012, p. 47). The second form is parrhesia, instances wherein the parrhesiastes, a truth teller, openly criticizes and reveals contradictions within a dominant actor, removing their certainty over past and present behavior (p. 107). Cynic parrhesiastes do this through particularly “provocative dialogue” as exemplified by Osama bin Laden’s 2004 speech using specific examples to portray Washington as “incompetent, feckless, and even helpless” (p. 116). The final form is self-interrogative imaging—distributing images that force states to engage their sense of Self, as seen, for example, in the United States when images of prisoners in Abu Graib were circulated during the Iraq War. While providing important insight regarding the manipulation of endogenous sources of OS, counterpower’s emphasis on power disparity and its focus on large egoistical states (Steele, 2007, p. 906, 2012, Chap. 1) constrains its applicability. Moreover, given its overt nature, those employing counterpower risk being vilified as the targeted population seeks to maintain positive views of Self (Chernobrov,  2016), potentially limiting the influence of external actors. Thus counterpower is only momentary and ends once it is “captured by power…when it becomes ‘classified’” (Steele, 2012, p. 49), often allowing states to discredit external challengers. While similarly focused on the endogenous sources of OS, IW allows us to expand how, and to what end, actors target subjectivity and OS. By covertly distorting the information environment of any state, IW facilitates domestic questioning of the congruence between policy and national subjectivity and/or the very existence of national subjectivity itself. In this sense, IW provides fodder to encourage/strengthen domestic “counterpower,” making domestic actors the target of potential backlash. Indeed, part of IW’s power comes from encouraging such internal hostility. Rather than seeking behavioral adjustment by threatening the “exposure of intolerable incongruities” (Bially Mattern, 2004, p. 99) within a victim’s subjectivity, IW might thus enflame internal discrepancies towards this very end. Here the aim is not merely to encourage “engagement” with Self, but to radicalize internal debates to erode the Self, generating a sense of existential crisis and anxiety— ontological insecurity. To establish this process, we must begin with the fact that national narratives are not independent objects removed from human agency. They are formed and maintained through inherently political processes (Bell, 2003, p. 75). Tellingly, Renan (1992) writes “historical error” is essential for nations, while Smith (1999, p. 16) suggests internal diversity most likely prevents a single version of the past. At the same time, while nations are “contingent,” they are also “situated, ordered and bound” (Berenskoetter, 2014, p. 264), premised upon a “bedrock of shared meanings and ideals” (Smith, 1999, p. 56) upon which a dominant account usually takes hold (Ringmar, 2011, p. 7). While there is always negotiation and contestation amongst derivative narratives, this often occurs without jeopardizing the metanarrative (Berenskoetter, 2014, p. 279), allowing it to provide OS for a large majority of the population (Skey, 2010) who become emotionally attached to it (Steele, 2007, p. 912). IW allows external actors to impinge upon this process. Following the USSR’s collapse and unraveling of communist ideology, Thomas (1998, pp. 9–10) notes how Russian society lost its “cementing mechanism” and had to rely on controlling the information psychological to recoup mental stability. However, this position can easily be reversed; actors can employ IW to target OS by intruding upon domestic narrative debates. Turning to Berzina’s overview of Russian IW scholarship, this connection is seen rather explicitly. For example, given Russian scholars’ view of humans and nations as “informative self-learning systems,” IW can insert new information into this system to “destroy national consciousness” (Berzina, 2018, p. 165). Technological advances and the emergence of the “networked society,” which facilitated the rise of societal debate (Cronin & Crawford, 1999, p. 260), provide actors with increasing opportunities to pursue such aims. For one, debates are increasingly polarized, as technological advances enable the avoidance of dissonant, and acquisition of affirming, information (Lupovici, 2012, p. 818). Second, the Internet has become a primary “transitional object” for achieving OS, embedding individuals within online networks (Areni,  2019) that reinforce social affiliations and deliver digital sources of news (Milina, 2012, p. 55), providing the “warmth and information” critical for OS (Cohen & Metzger, 1998, p. 52). A consequence, however, is individuals are progressively interacting within “identity bubbles” (Kaakinen, Sirola, Savolainen, & Oksanen, 2020), helping increase partisanship as a salient social identity (Lupton, Singh, & Thorton, 2015; McCoy, Rahman, & Somer, 2018, p. 22). While ingroup bias does not presuppose intergroup conflict (Allport, 1954/1979, p. 42), IW is positioned to exploit the role digital and social media play in fostering/reinforcing partisan views to accentuate perceived incompatibility. Studies have already found consumers of partisan news “tend to express less accurate beliefs about a host of politically charged topics” (Garrett, Long, & Jeong,  2019, p. 490). Given digital and social media lack the restraints found in traditional media outlets (Cronin & Crawford, 1999, pp. 260, 492), external actors are readily able to interject dis/misinformation or masquerade as members of the targeted society to push these trends further, manipulating the propensity to seek out validating information and the ability to quickly circulate information throughout online identity bubbles to influence intergroup perceptions. As perceived estrangement and incompatibility grows, the subnational other progressively appears “undomesticated” (Skey, 2010, p. 729), as transgressing social convention and championing a radicalism that transforms them from “normal political adversar[ies]” into an “existential threat” (McCoy et al., 2018, p. 19). This can degrade into “mass hysteria” (Umbrasas, 2018)—periods when distorted perceptions of “social, cultural, or political issues” take hold, sparking anxiety. Instead of a “taken-for-granted” national identity (Skey, 2010, p. 716), individuals thus face intense competition for ownership over defining national subjectivity, particularly as subgroups strives to maintain positive self-images (Chernobrov, 2016). Accordingly, such rifts generate a breakdown in social interaction (Mitzen, 2006, p. 348) and disrupt daily life, making it difficult to sustain a sense of constancy in one’s “social and material environment”—of being “at home” (Kinnvall, 2004, p. 747). Individuals are thus faced with a “fateful moment”—“phases at which things are wrenched out of joint” and consequential decisions must be made (Giddens, 1991, pp. 113–114). As individuals seek to grapple with this challenge, they are simultaneously confronted with reduced cognitive certainty—the result of IW helping establish and then broadcasting the existence of alternative “perceptions of reality” (Umbrasas, 2018), making knowledge appear increasingly contingent. Through these processes, IW comes to challenge OS on two fronts. First, by undermining a stable metanarrative and sense of home, IW destabilizes individuals’ biographical narratives. Second, by polarizing debates and augmenting perceived incompatibilities to the point former compatriots appear “undomesticated,” IW subverts existing frameworks for managing anxiety around existential questions: eroding certainty over where threats reside (existence), undermining the stability of established belief systems (meaninglessness), and curbing positive subgroup recognition (condemnation). This results in heightened anxiety and an existential crisis as “the ‘business as usual’ attitude” critical to OS is eroded (Giddens, 1991, p. 114). Overall, the digitalization of society has raised the prospect for actors to target the endogenous sources of OS. Increasingly, this means all information is now strategic; for example, acquiring/stealing troves of digital data, personal and corporate, facilitates machine learning and refines algorisms to allow for more efficient messaging in IW (Rosenbach & Mansted, 2019, pp. 5–6). Russia has actively recognized and sought to capitalize on these changes (Gerasimov, 2016, p. 24), investing into “enabling factors to adapt the principles of subversion to the internet age” (Abrams, 2016, pp. 19–20; Giles, 2016a, pp. 27, 36)—tactics increasingly employed by other actors (Robinson et al., 2018). Fusing IW and OS helps to better conceptualize such efforts. Specifically, the next section further develops how actors target the endogenous sources of OS to influence policy or foster ontological insecurity with reference to various Russian IW operations.