# Disinformation Aff-GDI22-SCHOLARS

Contents

[Disinformation Aff-GDI22-SCHOLARS 1](#_Toc108268537)

[AFF Case 5](#_Toc108268538)

[1AC 6](#_Toc108268539)

[Contention 1 – Status Quo Flawed 7](#_Toc108268540)

[Contention 2 – Information Credibility 10](#_Toc108268541)

[Contention 3 – Democracy 14](#_Toc108268542)

[Contention 4 – Alliance Cohesion 17](#_Toc108268543)

[Contention 5 – Solvency 21](#_Toc108268544)

[Status Quo Flawed 24](#_Toc108268545)

[Reactive and Not Coordinated Now 25](#_Toc108268546)

[Investment Needed Now 28](#_Toc108268547)

[Uniqueness – Disinformation Modern Threat 29](#_Toc108268548)

[AT – Russian Disinfo Declining 31](#_Toc108268549)

[AT – Deepfakes Get Debunked 33](#_Toc108268550)

[AT – Russian Disinfo Ineffective 36](#_Toc108268551)

[Information Credibility 38](#_Toc108268552)

[Disinfo Undermines Truth 39](#_Toc108268553)

[Disinfo Causes Confusion 42](#_Toc108268554)

[Disinfo Causes Polarization 46](#_Toc108268555)

[Disinfo Undermines Intelligence 49](#_Toc108268556)

[Disinfo Undermines Expert Credibility 53](#_Toc108268557)

[Disinfo Undermines Civilization 55](#_Toc108268558)

[Deepfakes Collapse Info Cred 56](#_Toc108268559)

[Internal Link – Bioweapon Proliferation 61](#_Toc108268560)

[Disinfo Undermines Public Health 62](#_Toc108268561)

[Impact – Public Health/Infodemic 64](#_Toc108268562)

[Impact – Nuke War, Climate, Civilization 69](#_Toc108268563)

[Impact – Civilization 73](#_Toc108268564)

[Nuclear War Impacts 77](#_Toc108268565)

[AT – No One Fooled by Disinfo 82](#_Toc108268566)

[AT – No One Fooled by Russian Disinfo 84](#_Toc108268567)

[AT – NATO engages in Disinfo 87](#_Toc108268568)

[Democracy 88](#_Toc108268569)

[Disinformation Undermines Trust 89](#_Toc108268570)

[Disinformation Undermines Democratic Values 90](#_Toc108268571)

[Democracy Good – Prevents Conflict 92](#_Toc108268572)

[Russia-China Spreading Authoritarianism 94](#_Toc108268573)

[China Threat Now 97](#_Toc108268574)

[Democratic Counter-Disinfo Key 99](#_Toc108268575)

[Democracy Good – Climate 102](#_Toc108268576)

[Democracy Good – Environment 103](#_Toc108268577)

[AT – Plan Censors/Hurts Democracy 105](#_Toc108268578)

[Alliance Cohesion 107](#_Toc108268579)

[Now Key Time 108](#_Toc108268580)

[Internal Link – Disinformation Undermines Alliance 112](#_Toc108268581)

[Russian Hegemony – DRAFT 117](#_Toc108268582)

[1AC – Russian Hegemony – DRAFT 118](#_Toc108268583)

[Internal Link – Russian Disinfo Globalized 124](#_Toc108268584)

[Internal Link – Regional Instability 128](#_Toc108268585)

[Internal Link – Balkans 129](#_Toc108268586)

[Plan Ideas 132](#_Toc108268587)

[Plan Concepts 133](#_Toc108268588)

[Student Ideas 134](#_Toc108268589)

[Solvency 135](#_Toc108268590)

[Proactive Solvency 136](#_Toc108268591)

[Systemic Solvency 137](#_Toc108268592)

[Coordinated Solvency 143](#_Toc108268593)

[Resilience Solvency 147](#_Toc108268594)

[Tech Solvency 151](#_Toc108268595)

[Democracy Solvency 153](#_Toc108268596)

[Deepfakes Solvency 154](#_Toc108268597)

[AT – Disinfo Shifts 156](#_Toc108268598)

[AT – Attacker Has Advantage 162](#_Toc108268599)

[AT – Internal Disinfo Alt Cause 164](#_Toc108268600)

[AT – Aff Can’t Solve without Private Sector Involvement 165](#_Toc108268601)

[AFF Off-Case Answers 167](#_Toc108268602)

[Topicality 168](#_Toc108268603)

[Topicality – Cyber 169](#_Toc108268604)

[Topicality – Disinformation 170](#_Toc108268605)

[Topicality – Artificial Intelligence 173](#_Toc108268606)

[US Key 174](#_Toc108268607)

[US Key – Alliance Strength 175](#_Toc108268608)

[US-EU Coop CP Answers 176](#_Toc108268609)

[Coop Fails 177](#_Toc108268610)

[EU CP Answers 178](#_Toc108268611)

[Solvency Deficit – US Key – EU Alone Won’t Solve 179](#_Toc108268612)

[Permutation Solves Best 180](#_Toc108268613)

[Canada CP Answers 183](#_Toc108268614)

[Canada CP Answer – Perm Do Both 184](#_Toc108268615)

[Canada CP Answer – No Middle Power/Liberal Order Solvency 185](#_Toc108268616)

[K Answers 187](#_Toc108268617)

[Security K Answer - Permutation 188](#_Toc108268618)

[Security/IR K – Alternative Fails 189](#_Toc108268619)

# 

# AFF Case

## 1AC

### Contention 1 – Status Quo Flawed

#### Current NATO approach is reactive and discoordinated – proactive and harmonized NATO cooperation key to countering disinformation threats

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 292-5, accessed 6-22-22, AFB]

NATO’s Approach to Disinformation

Since its founding, NATO’s approach to countering disinformation has evolved alongside the threat environment. The Alliance has always recognized that security and stability derive from military as well as non-military means but has historically prioritized the former over the latter. It took several years and the proliferation of direct disinformation attacks against NATO for the Alliance to recognize the threat and begin operationalizing a response—an ongoing process that continues today.

During the Cold War, NATO prioritized conventional defense and deterrence and only tangentially considered disinformation. The 1956 Committee of Three report acknowledged that Soviet leaders had “been sowing seeds of falsehood” against the Alliance for many years and that some within NATO believed the Alliance was no longer necessary after serving “a useful defensive and deterrent role in the Stalinist era.” The report also lamented NATO’s failure to inform its member states’ publics “of the importance of the part played by NATO in preserving freedom,” limited coordination on national information policy, and low financial support for expanding information activities.13 The 1967 Harmel Report addressed disinformation only indirectly, stating that NATO’s main function was “to maintain adequate military strength and political solidarity to deter aggression.”14 Disinformation threatened to undermine solidarity and cohesion, but the existential security threat posed by the Soviet Union led NATO to prioritize conventional defense and deterrence.

After the dissolution of the Soviet Union, the conventional military balance shifted in NATO’s favor. The Alliance began focusing on non-military threats, although not always disinformation. In 2010, an independent expert group commissioned by NATO argued that “the Alliance has ample grounds for confidence” given the lower risk of conventional military aggression and cautioned against unconventional threats but not disinformation specifically.15 Official communiqués also exemplify this trend. The 2014 Wales Summit Declaration suggested “enhancing strategic communications” to counter hybrid threats without naming disinformation.16 NATO’s current Strategic Concept likewise excludes disinformation from its list of unconventional threats.

Since the Kremlin’s illegal and illegitimate invasion of Ukraine and annexation of Crimea in 2014, disinformation narratives targeting NATO have intensified and so-called fake news, manipulated facts, and slanted narratives have become a daily reality.17 Short-term false narratives have targeted Alliance operations, including a NATO military jet colliding with a Russian commercial airplane,18 the Alliance assembling 3,600 tanks on Russia’s border,19 and civilians being killed or harmed during NATO military exercises.20 Other narratives are longer-term, strategic, and target the Alliance’s enduring purpose and solidarity, claiming that NATO’s exercises are dangerous and threaten Russia’s security, defense expenditures are excessive, the Alliance disingenuously justifies new deployments,21 and that NATO broke a promise by continuing to expand and is encircling Russia.22 These narratives are not new but their proliferation since 2014 has unambiguously brought disinformation onto NATO’s agenda.

While NATO was quick to enhance conventional defense and deterrence along the eastern flank after 2014,23 there was insufficient support within the Alliance to similarly adapt its non-military means. The 2016 Warsaw Summit Communiqué mentions hybrid threats broadly, and it was not until the 2018 Brussels Summit that an official summit declaration named disinformation specifically. Most recently, the NATO 2030 initiative was launched at the 2019 London Summit—and on the heels of President of France Emmanuel Macron calling the Alliance “braindead”24—to “further strengthen NATO’s political dimension.”25 This was a forewarning of sorts that NATO’s non-military malaise could have wider consequences.

This proved prescient during the COVID-19 pandemic. The Kremlin’s disinformation has targeted land- and sea-based military exercises and NATO’s presence in Lithuania, Latvia, and Poland.26 Narratives have also claimed inter alia that NATO created COVID-19, the pandemic would cause NATO to disintegrate, and the Alliance is inept against the virus.27 China’s increasingly assertive public diplomacy campaign—and outright fabrication, for example, that the virus originated in Italy28—aims to undermine trust among Allies, promote its own system over democracy,29 and increase its influence and standing vis-à-vis Europe.30 Although Russia and China’s disinformation specifically targeted NATO, created narratives blaming troops for spreading the virus,31 and attempted to undermine the Alliance’s public health messaging, NATO’s response early in the pandemic was limited to correcting facts and false narratives ex post after they had entered the public domain.32 The volume of NATO’s online communication, especially during the first few months of the pandemic, was also far smaller than what hostile actors were able to project through their massive state media and social media networks.33 Looking towards the coming decade, three common themes have emerged. First, while NATO has bolstered its public diplomacy and strategic communications in recent years, its response to disinformation has largely remained reactive rather than proactive, focusing primarily on positive messaging and countering narratives after they appear. Its twin-track “understand and engage” model tracks the information environment, tailors communications,34 corrects facts, and improves media literacy.35 This likely derives from NATO’s defensive strategic culture and is therefore unlikely to fundamentally change. Nonetheless, it has at times placed the Alliance at a distinct disadvantage from the Cold War to the COVID-19 pandemic. Second, national and Alliance-level efforts are not fully aligned. National militaries are adapting more quickly to counter disinformation and other unconventional threats. US Army Europe has initiated drills to prepare against disinformation and cyberattacks, and implemented a sensor network to monitor news across Europe to increase its speed of response.36 When the Kremlin’s disinformation narratives targeted the Defender 2020 military exercise last year, the US coordinated bilaterally with Allies to respond rather than at the multinational level.37 The broader challenge is harmonizing national information policy. The US Department of State’s Center for Information Analysis and Response, which collects and analyzes foreign information warfare efforts, and the government of Lithuania’s “national information influence identification and analysis ecosystem”38 are two recent examples which have remained at the national level. Third, NATO has yet to define precisely where disinformation fits among the constellation of emerging security threats. This is inherently difficult because it presents simultaneous operational, strategic, and existential challenges and is impossible to measure with confidence. The Alliance includes disinformation within hybrid and grey zone threats.39 For example, the 2018 Brussels Declaration warned that NATO faces “hybrid challenges, including disinformation campaigns and malicious cyber activities.”40 The NATO 2030 Reflection Group’s report linked disinformation to grey zone activities, which have “eroded the traditional boundaries of conflict” and “weaken and divide Allies from within by undermining societal cohesion and our way of life.”41 This illustrates a compartmentalized rather than harmonized view of the threat environment, particularly towards non-military threats. The 2021 Brussels Summit Communiqué shows progress by more frequently mentioning disinformation in the context of hybrid threats, highlights the capabilities of Counter Hybrid Support Teams, and recognizes Russia and China as perpetrators of disinformation.42 Looking to 2030, NATO’s non-military approach must continue to evolve.

### Contention 2 – Information Credibility

#### Must act now to prevent disinformation – Disinformation magnifies all impacts – it is a force magnifier, spoiler and entangler – undermining democratic institutions, deterrence, and NATO cohesion

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 289-90, accessed 6-22-22, AFB]

Disinformation, fake news and—since the COVID-19 pandemic erupted in 2020—“infodemics” have been added to the vocabulary of societies across the world. Often conflated with other terms including misinformation, tainted leaks, and propaganda, disinformation is the use of false or manipulated information to distort the truth, weaken trust, and undermine democratic discourse and practices. It has become a catch-all for information manipulation operations and has fundamentally altered the way we view geopolitical competition, warfare, and security.

For NATO, a defensive military alliance based on collective defense—“an attack against one is an attack against all”—disinformation has until recently been rarely discussed, much less considered. Article 2 of the North Atlantic Treaty, however, underscores that “peaceful and friendly international relations” come not from military strength alone, but strong and free member state institutions and an understanding of the principles behind them.1 Disinformation, which is part of broader malign influence operations, directly threatens these principles and institutions. Its acceleration in recent years has brought disinformation onto the transatlantic agenda.

In the coming decade, NATO is likely to face an increasingly complex and contested strategic environment. Disinformation will lurk as a force-multiplier, spoiler, and entangler. Russia and China have demonstrated willingness to deploy non-military means against NATO and could intensify the use of disinformation with the benefit of emerging technologies. At the operational level, disinformation could increasingly probe and erode NATO’s defense and deterrence. At the strategic level, long-term information operations and narratives skeptical of NATO’s enduring purpose could weaken solidarity and cohesion. To protect its political center-of-gravity, NATO should crystallize where disinformation fits among the multiplicity of threats likely facing the Alliance in the emerging security environment and then further evolve its approach to countering disinformation.

#### Disinformation is a force factor in international conflicts, combined with other attack vectors it pushes countries to the brink of conventional warfare.

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 5-6, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

Several countries have already contextualized disinformation as a national security threat. The US State Department defines disinformation as a ‘quick and fairly cheap way to destabilize societies and set the stage for potential military action’.15 A joint US State Department and Joint Chiefs of Staff white paper later posited that: *“Information has been weaponized, and disinformation has become an incisive instrument of state policy*”.16 Russian General Valery Gerasimov wrote in a 2013 article portraying disinformation as crucial: “The role of nonmilitary means of achieving political and strategic goals *has grown, and, in many cases, they* have exceeded the power of force of weapons in their effectiveness”.17 Similarly United Nations Development Program discourse also constructs disinformation as a weapon – a trend, which began with the COVID-19 pandemic.18 In the same vein, NATO’s securitization of disinformation began with the first Ukraine war (2014) and remained as a crucial component of hybrid warfare in NATO doctrines.19 The concept of a digital information war had already been included in Russian 2010 Military Doctrine, which was broadened in its 2014 update to include social media and ICTs.20 Since then, both practices and allegations of disinformation have proliferated across other governments including China, UK, France, Italy, South Africa, Turkey and Kenya (among others), where disinformation is used domestically to discredit political opponents, a foreign policy tool to confuse international rivals and a key threat that has to be defended against – all at the same time.21

Indeed, disinformation is increasingly being used as a force factor during international crises. During the 2017 Gulf crisis between Saudi Arabia, Qatar and the UAE, a robust disinformation campaign, followed by cyber-attacks, brought them to the brink of limited conventional war and required significant diplomatic effort to disentangle the damage caused by disinformation.22 In that case, disinformation had significantly aided in the escalation of the crisis, increasing the costs of backing down by raising audience costs. Following the shooting down of its SU24 in northern Syria, Russia had launched a major disinformation campaign against Turkey, drawing a wedge between Ankara and other NATO countries on the Syrian war, damaging intra-alliance cohesion and ultimately creating itself a relatively unchallenged information space as it entered the Syrian theatre militarily.23 In Nigeria, the government employed a disinformation campaign in the last decade targeting international aid agencies and workers, significantly impairing the ability of those agencies to work on humanitarian relief in the country.24 From click farms of Indonesia to the ‘black campaigning’ in the Philippines, disinformation is being deployed as a distinct strategy to discredit and demobilize regional politics in Southeast Asia and more recently, to sow mistrust towards China’s SinovacCoronaVac vaccine.25

#### The impact is existential - Compromised information undermines Civilization, threatens Elections, Lives, and the Economy, and magnifies the likelihood of Nuclear War and Climate Change.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 3-5, accessed 7-8-2022) SS:/

Founded in 1945, the Bulletin first focused on the existential threat from nuclear war. The atomic scientists of the Manhattan Project did not believe that the miniature suns let loose on Hiroshima and Nagasaki in themselves posed an existential threat to human existence.4 But most of them recognized that they were omens of a future in which nuclear weapons, used on a large scale, could indeed threaten human existence, and even used on a smaller scale could threaten modern human civilization.

After sporadically reporting on climate change for decades, in 2007 the Bulletin formally expanded its concept of existential threat to include that and nuclear war.5 Where large-scale nuclear war threatens to snuff out hundreds of millions of lives in a matter of hours, climate change threatens to alter the planetary ecosystem. Here the effects are more subtle and less easily noticed because they are cumulative over decades. There is no single cataclysmic event in the offing, and yet myriad smaller regional disasters will result: more intense and more frequent forest fires, heat waves, and storms; vastly increased coastal flooding and rising sea levels; loss of arable land; severe shortages of food and water; and mass migrations and relocations.

Nuclear war and climate change threaten the physical infrastructure of human civilization as well as the underlying geochemical processes and the ecology of the planet. Because most people depend on both physical infrastructure and our global ecology for food, energy, and other necessities of existence, nuclear war and climate change put the lives of the great mass of humanity at risk. Because nuclear war and climate change threaten massive changes in cultural identity and the loss of historical resources, our civilization and our legacy are at stake, too. In those ways, both nuclear war and climate change pose existential threats to humanity. But these are not the only such threats to civilization as we know it.

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 environment)—in many ways has become central and often critical to the way people now live all over the world.

In the words of Yale Law School’s information scholar Jack Balkin, “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.”6 Consider that nations require good information to allocate benefits and social services to the populace; to administer mechanisms for public safety (e.g., law enforcement, 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 clients; 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 services; and to maintain their accounting and finances. Construction and manufacturing projects entail the coordination of dozens, hundreds, or thousands of parties—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 political candidates standing in elections; to know as consumers 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 effectively or efficiently; and in truly countless other ways.

Nations also engage extensively in information production. They provide education for young people; support 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 information 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 crippled, as they could and likely would make bad or at least suboptimal decisions about war and peace, the economy, law enforcement, housing, food production, energy, and the many other important matters for which governments have some responsibility.

### Contention 3 – Democracy

#### Disinformation undermines trust in government – it is the greatest threat to liberal democracies

**Boudreau, Veritas Strategic Communications Principal Consultant, 22**

[Brett, 2022, Canadian Global Affairs Institute,The Rise and Fall of Military Strategic Communications at National Defence 2015-2021: A Cautionary Tale for Canada and NATO, and a Roadmap for Reform, Retrieved from <https://policycommons.net/artifacts/2460847/the-rise-and-fall-of-military-strategic-communications-at-national-defence-2015-2021/> on 01 Jul 2022. CID: 20.500.12592/527c47. HC)

Executive Summary

On November 2, 2020, the Ottawa Citizen ran the front-page headline “Canadian Military Wants to Establish New Organization to Use Propaganda and Other Techniques to Influence Canadians.” This seemed an unbelievable story, and one initially denied by a spokesperson for the minister of National Defense. Just three days later, though, then-chief of the Defense Staff (CDS) Gen. Jonathan Vance shuttered the group in question, terminating an initiative more than five years in the making that called into question the Department of National Defense’s (DND) commitment to objective and appropriate public communication, at a time when truth decay, misinformation and disinformation have gained much traction around the world and in Canada. In June 2021, the day Parliament adjourned for the summer, DND acknowledged to select media that acting CDS Lt.-Gen. Wayne Eyre and then-deputy minister Jody Thomas had determined the initiative was “incompatible” with government communications policy and the vision, mission and principles of DND Public Affairs. In a surprising self-indictment, the leaders also admitted a lack of “institution-wide strategic level direction and guidance,” to build information-related capabilities that were “governed by appropriate authorities and oversight.” Deliberate influence campaigns by malign state, non-state and increasingly by domestic actors to disturb, disrupt and create disorder in democratic societies have become widespread and commonplace. The volume of vitriol is increasing. This is fast eroding citizen faith, trust and confidence in government and public institutions and may be the greatest contemporary threat liberal democracies face – arresting this trend and then restoring trust, the ultimate challenge. National Defense’s entire program – to be successful on operations; secure sufficient funding; recruit, train and retain; effect culture change; reconstitute the force post-pandemic and procure the equipment needed to contest, confront and defeat adversaries – will largely depend on whether the institution can modernize its approach to strategic communications to maneuver more agilely and to better effect in a complex, frenetic and hostile information environment. Recently, National Defense has suffered a significant self-inflicted setback in that regard.

#### Weaponization of data and disinformation undermines democratic institutions and strengthens authoritarianism

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 298-9, accessed 6-22-22, AFB]

Technological innovation has also brought about another set of threats that are still underexplored: the ability to collect huge amounts of data. This can serve political warfare purposes, such as data dumps56 or tainted leaks,57 political repression and authoritarian strengthening—something that China is currently perfecting and other states, including Russia, are beginning to utilize on a wider scale by benefiting from Western technological innovation enablers, such as internet platforms. Furthermore, the COVID-19 crisis and the use of tracking technologies might have opened the door for another set of technological advances that are likely to further strengthen digital authoritarian practices and regimes.58 The combination between surveillance, massive troves of data and technologies that make its processing faster and enable the manipulation of the information space will be part of the future in ways that are hard to anticipate.

For now, democracies are still dealing with harms that arise from a combination of known disinformation tactics, existing means of communication and social media platforms, and rapid innovations in this space—including migrating between different social platforms and an increased use of encrypted communication platforms. Analysis of the Russian Main Intelligence Administration’s (GRU) operations since 2014 do not show significant technological leaps59 and similarly in the case of China, existing disinformation and propaganda capabilities are only enhanced by technology, but not necessarily defined by new technologies.60 The main threat of disinformation stems from its use in conjunction with other tactics like political corruption, use of proxies and unwitting allies, deceit, and human intelligence.61

China in particular presents a growing threat, the magnitude and long-term implications of which remain largely unaddressed in the national and Alliance decision-making circles. The Chinese Communist Party’s efforts to manipulate the global information ecosystem in the past decade surpass the ambitions and capabilities of other authoritarian actors. These capabilities include an oversized propaganda machine, disinformation, repressions of information and dissent domestically and abroad, and investments in media markets or “key nodes in the information flow.”62 Adding massive data collection and surveillance technologies to the mix amplifies the potential for a major disruption of the free flow of information and possible major value shifts in global public opinion with long-term implications for democratic values, institutions, and security.

#### Sustaining democracies is imperative to avoid conflict and preserve peace

Reiter, Harvard National Security post-doctoral fellow, 17

[Dan, 1-25-2017, Oxford Research Encyclopedia of Politics, "Is Democracy a Cause of Peace?,", https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-287#acrefore-9780190228637-e-287-div1-2, 7-2-2022, LASA-LR]

There is enough evidence to draw the conclusion that joint democracy does cause peace, and that the dyadic democratic peace is a law. None of the spuriousness critiques, though intriguing, have sufficiently withstood scholarly rebuttals to justify dismissing as spurious the very strong correlation between joint democracy and peace, especially given the experimental, case study, and other quantitative observational work that provide support for different elements of the democratic peace argument. That said, the spuriousness critiques suggest possible modifications of the law of the democratic peace, such as perhaps that the democratic peace could be weaker in less-developed regions. Regarding the causal arrow thesis, though there is evidence that peace may cause democracy as well as democracy causing peace, the evidence is much weaker that peace causes democracy but not vice versa. Further, the claim that peace causes democracy but not the reverse contains theoretical inconsistencies.

That said, it is of course conceivable that future studies may emerge that cast decisive doubt on the proposition that democracy causes peace. Data collection in international relations is never going to be as decisive in supporting or refuting theory as data collection in fields like physics or chemistry, where highly precise, often non-probabilistic theory permits point predictions that can be tested many times in controlled laboratory settings. It also will not be as decisive as data collection in the medical sciences, where theories are probabilistic but experiments can be conducted on thousands of subjects and repeated dozens of times. That said, the evidence that dyadic democracy causes peace is as strong as the evidence supporting essentially any theoretical proposition in international relations, other than relatively trivial propositions such as that adjacent states are more likely to fight each other than nonadjacent states. Echoing his 1989 assessment, Levy (2013, p. 587) remarked that in international relations “no one has identified a stronger empirical regularity” (Levy, 2013, p. 587). That is, if the dyadic democratic peace is not a law, it’s as close to a law that we have in international relations, and probably as close to a law as we are ever going to see.

Even accepting that neither cluster of critiques dislodges the conclusion that democracy cause peace, the inescapable conclusion is that we live in a complex, multi-causal world. As the democratic peace advocates themselves have long recognized, many factors beyond democracy cause peace (Russett & Oneal, 2001). Democracy and peace likely mutually cause each other. Further, as Kant envisioned, this variety of factors each cause each other. Development may cause peace, but democracy also causes development (Przeworski et al., 2000). Gender equality and democratization are likely tightly connected in complex ways. Future empirical work using observational, experimental, and case study methods should continue to unpack and describe this web of complex and important relationships.

### Contention 4 – Alliance Cohesion

#### Must act now to prevent disinformation – Disinformation magnifies all impacts – it is a force magnifier, spoiler and entangler – undermining democratic institutions, deterrence, and NATO cohesion

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 289-90, accessed 6-22-22, AFB]

Disinformation, fake news and—since the COVID-19 pandemic erupted in 2020—“infodemics” have been added to the vocabulary of societies across the world. Often conflated with other terms including misinformation, tainted leaks, and propaganda, disinformation is the use of false or manipulated information to distort the truth, weaken trust, and undermine democratic discourse and practices. It has become a catch-all for information manipulation operations and has fundamentally altered the way we view geopolitical competition, warfare, and security.

For NATO, a defensive military alliance based on collective defense—“an attack against one is an attack against all”—disinformation has until recently been rarely discussed, much less considered. Article 2 of the North Atlantic Treaty, however, underscores that “peaceful and friendly international relations” come not from military strength alone, but strong and free member state institutions and an understanding of the principles behind them.1 Disinformation, which is part of broader malign influence operations, directly threatens these principles and institutions. Its acceleration in recent years has brought disinformation onto the transatlantic agenda.

In the coming decade, NATO is likely to face an increasingly complex and contested strategic environment. Disinformation will lurk as a force-multiplier, spoiler, and entangler. Russia and China have demonstrated willingness to deploy non-military means against NATO and could intensify the use of disinformation with the benefit of emerging technologies. At the operational level, disinformation could increasingly probe and erode NATO’s defense and deterrence. At the strategic level, long-term information operations and narratives skeptical of NATO’s enduring purpose could weaken solidarity and cohesion. To protect its political center-of-gravity, NATO should crystallize where disinformation fits among the multiplicity of threats likely facing the Alliance in the emerging security environment and then further evolve its approach to countering disinformation.

#### Disinformation fuels authoritarianism and poses an existential threat to the alliance, undermining democratic models, principles, and decision-making that are key to the alliance

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 290-292, accessed 6-22-22, AFB]

The Threat of Disinformation

Disinformation is used strategically to challenge the very foundations of liberal democracy and of transatlantic relations by affecting political decision-making, societies, and the very functioning of democratic institutions. Political warfare and disinformation allow authoritarian regimes to present the authoritarian governance model—and during COVID-19 its crisis management—as a superior alternative to democracy.2 Given the magnitude and resources of their state-owned media operations and global ambitions, Russia and increasingly China are the most prominent authoritarian adversaries for the transatlantic Alliance.3 But the use of disinformation is proliferating among a multitude of state and nonstate actors, including most notoriously the Islamic State (ISIS). US law enforcement agencies noted in a report about foreign interference in the 2020 elections that Iran, Venezuela, and Cuba are also present in this space, as well as other nonstate actors like Hizballah.4 Worryingly, various actors within democratic societies and NATO members are also turning to disinformation and information suppression to advance their political goals domestically.5 A prominent tool of political warfare during the Cold War—Soviet campaigns of “active measures” and dezinformatsiya6—propaganda and disinformation went under the radar for the better part of the past 30 years in the West. The Kremlin’s military aggression in Ukraine and illegal annexation of Crimea in 2014 revealed Russia’s use of information as a weapon, amplified and strengthened by modern technologies, social media, and a revamped state-media apparatus. Disinformation campaigns became a central tool for denying, justifying, and supporting its actions in Ukraine. It created an alternate reality meant not only to obscure Russia’s involvement, but also to completely discredit theidea of factuality, truth, and trust in the possibility or mere existence of facts (“implausible deniability”).7 This became a core tactic for the Kremlin’s power projection in Europe and particularly in former Soviet or satellite states. The attempt by pro-Kremlin actors to influence the 2016 US election was another turning point. It revealed the vulnerability of consolidated democracies and the irrelevance of geography when it comes to new modes of political warfare. Disinformation and other means of malign influence build over time, prey on local conditions, prime audiences for future attacks and are mobilized at crucial moments such as elections, requiring significant resources to investigate and uncover them. Disinformation is deployed as a force multiplier, part of a toolkit of malign influence tactics to ensure the success of broader strategic aims.8 These can be military operations, such as Russia’s war against Georgia and Ukraine or its intervention in Syria, or intelligence operations, such as the Skripal poisoning case in the United Kingdom, whereby the Kremlin sought to provide a cover for its unlawful incursion on UK territory in a cloud of disinformation and competing narratives. During the first peak of the COVID-19 crisis, the use of disinformation, propaganda, and coordinated digital deception by both Russia and China went hand in hand with so-called ‘mask diplomacy,’ a media strategy accompanying the delivery of medical supplies by Russia and China to Europe.9 These information operations were meant to highlight the European Union (EU) and NATO’s lack of solidarity with their members and incapacity to act swiftly and effectively. China also branded a new, more aggressive approach to engaging with Western counterparts—so-called ‘wolf-warrior diplomacy’—both in official communication and by leveraging its state media and an increased social media presence.10

Disinformation has become a weapon to undermine and potentially distort the outcomes of democratic elections, introduce wedges in the transatlantic alliance, deepen public health crises, and change the nature of conflict. Thus, the salience of disinformation has grown exponentially among researchers, civil society, and policy makers in civilian and military structures alike. Increasingly, military structures are starting to incorporate countering disinformation in their strategies11 because ambiguity and masked intentions could negate readiness and delay reinforcement.12 Supranational structures like the EU, NATO, and G-7 also have dedicated programming on tackling disinformation. With this, it has become a pressing national and transatlantic security threat and poses a long-term existential challenge to the values and principles underpinning the North Atlantic Treaty.

#### A strong NATO is the cornerstone of global stability

Burns, Harvard Kennedy School Practice of Diplomacy and International Relations Roy and Barbara Goodman Family Professor, 18

(Nicholas, 9-5-2018, Belfer Center for Science and International Affairs, "Assessing the Value of the NATO Alliance", https://www.belfercenter.org/publication/assessing-value-nato-alliance, accessed on 7-8-2022, SR)

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

### Contention 5 – Solvency

#### Plan

The United States federal government should substantially increase coordinated cooperation with the North Atlantic Treaty Organization on proactive and system-wide counter-disinformation cyberspace initiatives.

#### Plan solves – Broadening NATO mandate to integrate proactive and coordinated counter disinformation policy system-wide key to reducing disinformation risks

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 300-303, accessed 6-22-22, AFB]

Encourage greater alignment of national and NATO-level information policy.

Article 3 of the North Atlantic Treaty states that Allies should “maintain and develop their individual and collective capacity to resist armed attack,”65 which should include countering malign influence and disinformation. NATO should create a more cohesive definition of information operations, of which disinformation is a key element, their potential impact, and their role within NATO’s understanding of conflict to provide the political impetus for member states to align national security concepts. NATO could create a reporting mechanism for Allies to share developments or publicize progress in addressing disinformation at each NATO summit. The overarching goal is for the North Atlantic Council to become a more frequent forum for consultation on national information policy, thereby creating a more united strategic communications front and enhancing coordination of national and multinational efforts to counter disinformation. NATO should also increase intelligence-sharing—which now occurs primarily between national intelligence services66—and mainstream national responses based on shared best practices. Updating the Strategic Concept to reflect these priorities could encourage closer alignment of national information policy.

The Alliance should also expand and integrate the political mandates of NATO divisions and departments focusing on emerging security challenges, including disinformation. Increasing internal coordination would harmonize its organizational approach. NATO could borrow from its approach to hybrid and in particular cyber security threats, as in the Emerging Security Challenges Division (ESCD) and include disinformation and influence operations among other emerging threats. This would first and foremost signify that threats to information integrity would be elevated to the same importance as other types of hybrid aggression. As in the cyber domain,67 NATO should maintain a degree of ambiguity about whether disinformation constitutes an attack on the Alliance.

While NATO’s Public Diplomacy Division (PDD) coordinates Alliance-wide communications, NATO needs to develop a more coherent internal mechanism that deals with information operations at a strategic and policy level. This would be an important step towards equalizing threat perceptions of disinformation within the Alliance and create a set of common denominator policies that would create more national information policy coherence.

Improve proactive, transparent communication to NATO member state publics.

NATO needs to tell its own story better, prevent malign actors from shaping the narrative, and adopt a preventative approach to disinformation that builds on best practices. Disinformation preys on existing vulnerabilities and opportunistically utilizes events or crises. NATO activities are transparent and known in advance (summits, military acquisitions, exercises) so there should be a preemptive effort to gain a f irst-mover advantage and set the narrative. This can also include opensource intelligence-gathering using social media and other technologies to understand the social context and monitoring how potential target communities attach meaning to or interpret disinformation narratives.

The Alliance should also publish regular fact-based threat assessments of the security environment and NATO’s efforts to mitigate them. Public support for NATO generally increases when threats against the Alliance are readily apparent. The challenge is that today’s unconventional threats are less visible and therefore perceived as less alarming than for instance conventional or nuclear threats. Nonetheless, the Alliance stands at a “strategic crossroads” and is as relevant as ever.69 NATO communication already alludes to its enduring purpose but regularly publicizing concise, fact-based threat assessments could help stabilize public support. To this end, it could task the NATO Strategic Communications Center of Excellence (StratCom COE)—an independent multinational organization supported by seven member states—and encourage more Allies to support it.

The Alliance should also consider organizing regular ministerials in Ally capitals other than Brussels. Holding such a prominent multinational event on a rotating basis across capitals could help harmonize public perceptions of NATO’s enduring purpose across all member states and increase public engagement particularly where fewer independent media options exist.

Finally, NATO should develop a more robust measure of public opinion in member state populations. The effect of disinformation is inherently difficult to measure. While the EU tracks favorability towards its institutions and policies through annual Eurobarometer polls, NATO relies on piecemeal information. The Alliance should consider a new mechanism to measure public opinion—the Estonian Defense Ministry’s national-level studies70 could provide one model—at regular intervals combined with other tools to test what might be influencing shifts in public sentiments.

Integrate disinformation into military exercises.

NATO has developed robust public diplomacy efforts around military exercises in Europe, but hybrid threats, including disinformation and attempts to influence behavioral outcomes, should be mainstreamed into regular exercises and simulations. NATO members have already experimented with some tools at the national level. The UK and the US militaries are integrating these tools into regular training71 and joint exercises have included behavioral science research and embedded experts.72 However, Allies often resort to bilateral cooperation against disinformation, often leading to uneven efforts among member states which need to be fully applied at the Alliance level. NATO should also regularly exercise scenarios where decision-making is delayed in the face of an ambiguous or unclear information environment.

The Alliance should follow the example of US Army Europe and build upon or establish disinformation sensor networks to monitor news in real time—including potentially viral story lines—during exercises and incorporate response training at the multinational level. NATO StratCom CoE has developed resources and knowledge that have already been utilized in military exercises to expose vulnerabilities. This could become the norm for future deployments.73 More broadly, Allies should follow the example of Norway and recognize that militaries are not omnipresent and therefore not well-suited to counter emerging threats alone. Folding civilians into joint training exercises at both the national and multinational levels could encourage early recognition of operational ambiguity.74

## Status Quo Flawed

### Reactive and Not Coordinated Now

#### Current approach is playing whack-a-mole – need proactive approach to counter-disinformation

Ling, investigative journalist, 22

[Justin Ling, works in journalism as an investigative journalist whose areas of interest include, misinformation, extremism and national security, 5-21-2022, Center For International Governance Innovation Online, "NATO Should Elevate Its Cyber Game, and Quickly", <https://www.cigionline.org/articles/nato-should-elevate-its-cyber-game-and-quickly/>, accessed on 7-2-2022, MG]

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.”

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. 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.

### Investment Needed Now

#### With increasing tech innovation and disinformation it is NATO’s responsibility to invest in the protecting their democracies in the face of aggressive disinformation attacks

NATO Reflection Group 20

[NATO reflection group, 11-25-2020, NATO, https://www.nato.int/nato\_static\_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, Page 48, 7-2-2022, LASA-LR]

Strategic communications are a critical tool of deterrence and defence. Effective deterrence rests on clear projection of the ability and resolve to act if necessary. For some adversaries and challengers, information is now a domain of contest. The information environment is contorted by misinformation, disinformation, and deception from these actors. These techniques aim to disseminate manipulated information with the intent of undermining trust in democratic institutions. Disinformation, propaganda, and misinformation are especially dangerous in times of rapid technological advancements and when generational changes continue to alter perceptions of NATO among Allied publics.

The rapid pace of digitisation across all walks of life poses a particular challenge to NATO Strategic Communications. NATO and Allied audiences are increasingly drawing their information from, and are influenced by, information delivered via digital means. Strategic competitors continue to demonstrate their growing capability and will to deploy the latest digital technologies against NATO and Allies, particularly in the information environment. Building resilience across Allied populations is the primary responsibility of Allies themselves. However, across the board, Allies have not invested sufficiently in the human, technical, and financial resources required to engage in a consistent and sustained manner on issues related to security and defence. Neither have they prioritised proactive and consistent communications in support of Alliance aims and objectives. Recognising the threat posed by state and non-state actors who deploy aggressive tactics below the threshold of conventional force to challenge and undermine Alliance values and cohesion, NATO must ensure that it is aware and able to prevent and respond with objective and factual information.

### Uniqueness – Disinformation Modern Threat

#### 81 countries participate in state sponsored disinformation campaigns and are intensifying commitments

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 2, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

Governments, state agencies and foreign policy institutions are increasingly deploying organized disinformation to distract and confuse their adversaries. In their 2020 report, Oxford Computational Propaganda Project identified organized, state-sponsored disinformation campaigns in 81 countries with rapidly increasing number of ‘cyber troops’ (semi-officially employed individuals working on state-sponsored information operations) and campaign intensities.1

#### Old tactics are becoming obsolete, the digitization of disinformation makes new tactics necessary

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 2-3 https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

Propaganda, manipulation and misdirection have been long-standing tactics of diplomacy and international competition. In the last decade, and especially around the 2016 US Presidential election, ‘fake news’ and disinformation became buzzwords of sorts that led to a rediscovery of the role of information in political competition. The biggest difference between the traditional and more recent debates on the matter is the digitalization of information warfare and the subsequent scale, volume and speed advantages brought by this digitalization. The advent of Information and Communications Technologies (ICTs) brought about a faster information exchange medium where traditional gatekeepers like editors, censors or curators are of secondary importance and often irrelevant. While in more traditional media forms, broadcast is dependent on the approval of an intermediary individual or a group, with ICTs and social media, this approval is often hard to enforce with the sheer scale of information poured into such media venues. Although automated content moderation works in most cases, it can easily be circumvented.7 With information gatekeepers out of the way, information becomes disintermediated (reduction in the use of intermediaries), with information suppliers (citizen journalists or anyone with access to social media) directly able to reach information consumers around the world, in real time.8 The disintermediated nature of modern information exchange has rendered ICTs a conducive ground for misinformation (unintended spread of false information), disinformation (purposeful creation and dissemination of false information) and malinformation (deliberate use of accurate or inaccurate information with the purpose of harming an individual or people).9

#### Disinformation is used by both weak and strong actors in both active conflicts and non-military pursuits.

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p.7, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

When an international dispute is pursued through non-military terms, disinformation can be used both to further escalate a crisis (especially when the Attacker is distinctly superior to the Defender), or to de-escalate one (when the Attacker is distinctly weaker than the Defender). Current empirical evidence and the relevant literature makes it hard to present a conclusive statement about whether disinformation is the ‘tool of the weak’.28 Stronger states have used disinformation against weaker adversaries as much as vice versa, and such disinformation has been deployed during active conflicts as much as non-militarized disputes. While there is a tendency to portray democracies as primary targets of disinformation, democracies have been sources of disinformation as well, preventing a clear regime type argument to materialize.29

### AT – Russian Disinfo Declining

#### Even when disinfo decreases, can’t let our guard down – vigilance is key to preventing info warfare

Bushwick, Scientific American associate editor covering technology, interviewing Edelson, misinformation research & New York University computer science PhD candidate, **22**

[Sophie & Laura, 3-8-2022, Scientific American, "Russia’s Information War Is Being Waged on Social Media Platforms", <https://www.scientificamerican.com/article/russia-is-having-less-success-at-spreading-social-media-disinformation/> accessed on 6-27-2022 hooch//cs]

Days after Russia invaded Ukraine, multiple social media platforms—including Facebook, Twitter and YouTube—announced they had dismantled coordinated networks of accounts spreading disinformation. These networks, which were comprised of fabricated accounts disguised with fake names and AI-generated profile images or hacked accounts, were sharing suspiciously similar anti-Ukraine talking points, suggesting they were being controlled by centralized sources linked to Russia and Belarus.

Russia’s Internet Research Agency used similar disinformation campaigns to amplify propaganda about the U.S. election in 2016. But their extent was unclear until after the election—and at the time, they were conducted with little pushback from social media platforms. “There was a sense that the platforms just didn’t know what to do,” says Laura Edelson, a misinformation researcher and Ph.D. candidate in computer science at New York University. Since then, she says, platforms and governments have become more adept at combating this type of information warfare—and more willing to deplatform bad actors that deliberately spread disinformation. Edelson spoke to Scientific American about how an information war is being waged as the conflict continues.

[An edited transcript of the interview follows.] How do social media platforms combat accounts that spread disinformation? These kinds of disinformation campaigns—where they are specifically misleading users about the source of the content—that’s really easy for platforms to take action against because Facebook has this real name policy: misleading users about who you are is a violation of Facebook’s platform rules. But there are [other] things that shouldn’t be difficult to take down—that historically Facebook has really struggled with—and that is actors like RT. RT is a Russian state-backed media outlet. And Facebook has really struggled historically on what to do with that. That’s what was so impressive about seeing that [Facebook and other platforms] really did start to take some action against RT in the past week, because this has been going on for such a long time. And also, frankly, [social media platforms] have had cover from governments, where governments in Europe have banned Russian state media. And that has given cover to Facebook, YouTube and other major platforms to do the same thing. In general, banning anyone—but especially banning media—is not a step anyone should take lightly. But RT and Sputnik [another Russia state-backed media outlet] are not regular media: they have such a long track record of polluting the information space.

What else can be done to fight harmful false information? One of the things that the U.S. did really well going into this conflict—and why, at least from a misinformation [controlling] perspective, the first week went very well—is that the U.S. government was really aggressive with releasing information about what it knew about the ground realities in Russia and Ukraine. That was really helpful for creating a space where it was difficult for the Russians to put out misinformation about those same things. Because the U.S. government was very forthcoming, it didn’t leave a lot of room; there wasn’t an information vacuum that the Russians could step in and fill. And then the Ukrainian government has been tremendously savvy in telling the story of the Ukrainian resistance. There are definitely times when it has stepped over the line into propaganda. But in general, it has made sure that the world sees the Ukrainian resistance and the fight that the Ukrainian people are willing to put up. That [helps] people see what is going on and understand that the people who are there fighting are real people who, not that long ago, were not fighters. They were civilians, and now they are defending their country.

I think both of those things are going to be difficult to maintain over time. But if they are not maintained, then the window for Russian misinformation will open. A challenge we are all going to have to deal with is that this war is not going to be over in the next few days, but the news cycle cannot maintain this level of focus on these events. It’s shocking to say, but in three weeks’ time, you will have hours go by without thinking about it. And that is when people’s guards are going to go down. If someone is trying to spread some kind of [disinformation]—maybe the Russians make up some fake Ukrainian atrocity or something—that’s when the world is going to be susceptible to that kind of thing. And that’s when we’re going to have to remember all this stuff of “Who was telling you the story? Do we trust them? How verifiable is this account?” This is going to be part of how conflict is waged going forward. But this is something that is new for all actors, and everyone is going to have to get used to keeping up their ground game in the information war, not just in the kinetic war.

### AT – Deepfakes Get Debunked

#### Deepfakes have an impact even if some are poor fakes – multiple examples prove deepfakes pose a destabilizing theat

**Giansiracusa,** Bentley University mathematics and data science assistant professor**, 22**

[Noah, 3-23-2022, Slate, "The Destabilizing Effects of Even Low-Quality Deepfakes", [https://slate.com/technology/2022/03/zelensky-deepfake-video-surrendering.html accessed on 6-27-2022](https://slate.com/technology/2022/03/zelensky-deepfake-video-surrendering.html%20accessed%20on%206-27-2022) hooch//cs]

Since the weeks leading up to Russia’s invasion of Ukraine, warnings have been circulating that Russia might use deepfake videos—convincing fake videos created with artificial intelligence— in the surrounding information war. Perhaps they would use deepfakes to fabricate a pretext for the invasion, or to have Ukrainian President Zelensky issue an order to surrender. With bated breath we waited, but no sign of deepfakery occurred. Then finally, on March 16—20 days into the invasion and 13 days after Ukraine warned this exact scenario might happen—a deepfake of Zelensky surrendering indeed appeared, and it was … unconvincing and obvious.

The video editing was low-quality, and the voice was noticeably off; few people seem to have been fooled by it. Not to take any chances, Zelensky himself quickly addressed the deepfake, leaving no doubt about its falsity.

One is tempted to conclude from this episode that deepfake algorithms are just not powerful enough yet, that the dreaded moment when deepfakes wreak havoc in political arenas is still off in the distant future, if it ever arrives. However, a closer inspection of the past few years reveals a different story: The destabilizing effects of deepfakes in politics have already arrived—not in a single widely publicized scandal or a flood of numerous incidents, but in an ominous trickle of subtle yet impactful incidents that largely slipped under the radar. This Zelensky deepfake was quickly put to rest, but there are other videos from past years whose authenticity is unclear—even today we don’t know whether they are deepfakes or real. The difficulty in debunking deepfakes isn’t just a question of technological sophistication.

Three years ago, Mother Jones reported a story surrounding Ali Bongo, the president of Gabon. Bongo was hospitalized for an undisclosed illness in October 2018. Two months later, the vice president announced that Bongo had suffered a stroke but was recovering and doing well. However, other than a few photos and a silent video released by the government, there were no signs of Bongo during this time. Speculation proliferated that the officials were lying, that Bongo was in far worse condition than they admitted—and possibly even dead. To help allay these concerns, on Jan. 1, 2019, the government posted to social media a video of President Bongo giving the customary New Year’s address.

But something didn’t seem right.

Bruno Ben Moubamba, a prominent Gabonese politician who ran against Bongo in the previous two elections, claimed the video was a deepfake. He argued that Bongo’s face seemed strangely immobile and that his eye movements did not appear synchronized with his jaw movements. Julie Owono, the international technology lawyer who brought this Bongo saga to the attention of Mother Jones, noted that Bongo blinked only 13 times during the two-minute video, which she said was less than half the typical amount. The deepfake theory rapidly gained a sizable following. Activists argued that Gabon’s ruling party used deepfake technology to hide Bongo’s dire state of health in order to avoid a special election mandated by law to occur if the president is unfit to lead.

One week after the release of the enigmatic New Year’s video, Gabon’s military attempted a coup and explicitly cited the oddness of the video as evidence that the president was absent and that the government was lying about it. The coup failed and the government retained control, and in August 2019 Bongo finally made his first public appearance since the stroke.

We still don’t know whether Bongo’s party used a deepfake video to deceive the public long enough for him to recover—and in doing so illegally avoided a special election that might have led to his ouster. One of the complications is that all the oddities in the New Year’s video that suggest it’s a deepfake could also be the result of Bongo’s stroke.

This event in Gabon foreshadows one that took place in the United States a year later.

On Oct. 2, 2020, just weeks before one of the most important elections in American history, news broke that President Trump had tested positive for COVID-19. Questions mounted throughout the day over the severity of his illness. At 6:31 p.m., he tweeted an 18-second video in which he said that he was heading to Walter Reed, but he reassured people that he thinks he is doing very well.

Just as with Bongo’s New Year’s address, this video looks very strange. Trump has an uncharacteristically flat affect, motionless manner, and vacant look in his eyes. Immediately there was talk on social media of it being a deepfake to hide the dire state of the president’s health.

This time, suspicion quickly faded as more footage of Trump appeared. The theory was fully dispelled when he gave a live address upon departing Walter Reed a few days later. But for a brief moment, it really was hard to know what was going on and what to believe. The existence of deepfake technology meant that Trump’s 18-second video raised more questions than it answered. In hindsight, the things that made the video appear to be a possible deepfake were likely just a result of the president being ill and possibly medicated.

Days later, Trump’s team posted a video of him speaking from the White House lawn, and once again skepticism arose. Some claimed that it looked like the background was “glitchy,” as though there were a green screen behind him. But Slate quickly debunked the doubts.

A few months later, another instance of deepfake dystopia occurred, this time in Myanmar. On Feb. 1, 2021, a military coup officially began when Prime Minister Aung San Suu Kyi—who in the 2010s played a key role in transitioning Myanmar from military rule to partial democracy—was arrested and deposed, along with other members of her ruling party. The president of the U.N. General Assembly called for her immediate release; the U.N. secretary-general said the coup is a “serious blow to democratic reforms in Myanmar.” Suu Kyi is a Nobel Peace Prize Laureate, and while she has received international criticism for her country’s role in the genocide of the Rohingya people and her denial of the atrocities that were committed, she is a legitimate democratically elected leader; the military needed to justify the brazen steps it took.

A military-run TV station broadcast a video recording of a detained former regional chief minister providing a public confession in which he said he bribed Suu Kyi. This seemed to establish the military’s claims that Suu Kyi is corrupt and violated ethics laws. Some claimed the minister’s voice in the video doesn’t sound like his usual one and noted that the visuals look strange: his facial movements follow a repetitive pattern and his expression looks oddly emotionless. To this day, some people suspect it is a deepfake, while others believe the unnaturalness observed in the video is the result of it being a forced confession and poor teleprompting. Once again, we don’t know for sure. The video is somewhat low-resolution and grainy, which makes distinguishing between a deepfake and an authentic video particularly challenging. Suu Kyi is currently under military arrest and facing an array of charges, including corruption—which carries a maximum penalty of 15 years in prison.

What we see in these examples is that the context of a video plays an enormous role in how difficult it is to determine its authenticity. People speak in a somewhat unusual manner in deepfake videos—but, as became apparent with both the Trump and Bongo incidents, people also do so when infirm. The stress of duress, such as the Myanmar official was experiencing, could also alter one’s speech patterns. And the resolution of a video matters: the flaws in deepfakes are more apparent in high-res footage. Finally, the political situation matters. For instance, the Zelensky deepfake was a foolish endeavor not just because it was too amateur to be convincing—it was easy to debunk because Zelensky could respond to it.

Don’t be lulled into a false sense of security by this ill-conceived Zelensky deepfake. More difficult deepfake situations have already occurred in the past and more will surely arise in the future.

### AT – Russian Disinfo Ineffective

#### Russian disinfo has multiple audiences – even if debunked in some places, it may still be confusing others

**Tucker,** New York University Jordan Center for Advanced Study of Russia director**, 22**

[Joshua A, 4-12-22, Slate, "The People Who Believe Russia’s Disinformation", [https://slate.com/technology/2022/04/russia-disinformation-china-africa-latin-america.html accessed on 6-27-22](https://slate.com/technology/2022/04/russia-disinformation-china-africa-latin-america.html%20accessed%20on%206-27-2022) hooch//cs]

Every day we wake up to new Russian atrocities—and new Russian lies about those atrocities—in Ukraine. The latest example is in Bucha, a Kyiv suburb where retreating Russian forces “left behind dead civilians lining the streets—some with their hands bound, some with gunshot wounds to the head.” The Kremlin quickly issued denials and claimed the evidence was fabricated.

After weeks of war, much has been written about the success and failures of Russia’s disinformation and propaganda. These tactics, of course, are not new. Russia has been running propaganda campaigns since the Cold War. What does feel new is the preponderance of true information available—and perhaps equally importantly, the speed at which it spreads. Social media, satellite imagery, and 24/7 reporting are directly refuting Russian disinformation in real time.

That news is only reaching some people, however. It’s worth stepping back to consider the various audiences for Russia’s disinformation campaigns and examine where they’re working and where they’re not.

First, where it’s not: Ukraine and the West. Russia and Putin have spread a long line of falsehoods about Ukraine. They claimed that Russian language speakers in Ukraine would welcome a Russian invasion. They’ve denied Ukrainian statehood, claiming Ukraine has always been part of Russia. They said this “special military operation” was necessary to “liberate” Ukrainians from their “Nazi leaders.” And with the war underway, government officials now claim Ukrainians, not the Russians, are shooting and bombing their own people.

None of this is true, of course. These falsehoods fell apart immediately, both in Ukraine and in the West, largely because true information won out. The Biden administration released intelligence that was remarkably accurate in predicting Putin’s next moves. Social media users in Ukraine have posted videos documenting the brutal invasion from Russian forces. Journalists have used that evidence, along with satellite imagery and other tools, to debunk false claims. As a result, foreign audiences can not only see for themselves what’s really happening in Ukraine, but also read the heart-wrenching stories of citizens caught in the crossfire and fleeing for their lives.

That leads us to where the disinformation campaigns may be working, at least for now: Russia, China, and the world beyond NATO, the EU, and their allies.

As with Soviet-era propaganda campaigns, Putin is trying to seal off his population from information to control the narrative. Authorities have shut down independent media and blocked most Western social media. For many, the only viable option left is state-controlled media, which pushes Putin’s false narratives.

Reports indicate this is working—at least to some extent. We read stories of Ukrainians with family members in Russia who don’t believe the war is real. “Every day I send them the necessary information, but the response is that ‘This is some kind of fake information, that this cannot be the case at all, that no one can or will shoot at civilians,’” said one Ukrainian woman, speaking about her sister and cousins who don’t believe what’s happening.

Likewise, a recent poll found Russians’ support for Putin has actually increased from 71 to 83 percent since the war started, although the more repressive a regime, the harder it can be to know what people are truly thinking. Indeed, a recent study using a more sophisticated methodology designed to elicit opinions on sensitive topics found actual support for the war to be 15 percentage points—53 percent vs. 68 percent—lower than reported using traditional survey methods. On the one hand, it is interesting that even in the current climate close to one-third of Russians were willing to explicitly tell pollsters that they oppose the war. On the other, even with the more sophisticated methods, more than half of Russians still expressed support for the war, so the fact that many Russians genuinely support the war should not be discounted – the phenomenon of “rallying round the flag” in times of war is a real one. Either way, true information will be critical to topple this digital iron curtain and pressure Vladimir Putin to end the war.

We also see evidence of Russia’s disinformation narratives spreading outside of Europe and the Western world. One recent New York Times story, for example, revealed how China’s Communist Party is using university classes, the media, and videos to push “a campaign that paints Russia as a long-suffering victim rather than an aggressor and defends China’s strong ties with Moscow as vital.” Another piece in the New York Times reports on research showing how Chinese state media is directly parroting Russian propaganda talking points. Beyond China, one study discovered a coordinated network of new, fake, and hacked Twitter accounts in Africa and Asia sharing pro-Putin messages. Another study found more than 170 websites in various languages pushing war disinformation, and NBC recently reported on Russian disinformation in Latin American media. The extent to which these messages will resonate outside of the NATO countries and their allies that are directly supporting Ukraine remains to be seen, but recent votes at the United Nations show that governments in the Global South remain much more conflicted about withdrawing support for Russia, suggesting such campaigns remain important.

## Information Credibility

### Disinfo Undermines Truth

#### Russian disinformation undermines truth

Grimes, Committee for Skeptical Inquiry post-doctoral fellow, 2**2**

(David Robert, 3-28-2022, Scientific American, "Russian Misinformation Seeks to Confound, Not Convince", https://www.scientificamerican.com/article/russian-misinformation-seeks-to-confound-not-convince/, accessed on 7-6-2022, SR)

Rather than take a side, these campaigns create decision paralysis that leads to inaction

As war envelops Ukraine, Russian sources have strived to create a miasma of disinformation about the invasion. Among ample efforts to distort reality, the Russian Ministry of Defense asserted recently that U.S.-backed labs in Ukraine have been developing bioweapons. Outlandish as this falsehood may be, Fox’s Tucker Carlson gave it credence by arguing that the U.S. government’s response was a “cover-up.”

As the Russia-Ukraine war intensifies, so too will the flow of disinformation. This is an age-old strategy Russia has long history of employing, and a playbook that others, most notably anti-vaccine activists, have borrowed from liberally. Yet, rather than focusing effort on convincing people of a falsehood, the Russian strategy takes a tack reminiscent of a strategy long employed by the tobacco industry: to sow so much doubt about what is true that it sends people into decision paralysis. Faced with a cacophony of wild and conflicting claims, people do nothing, unsure of what is right.

Despite constituting only a small part of our media diet, disinformation campaigns, in our digital world, can be devastatingly effective. We are intrinsically biased towards information that is emotionally visceral. We afford more weight to content that frightens or outrages us, with the ability to induce anger serving as the single greatest predictor of whether content goes viral. This propels the most visceral, divisive narratives to the forefront of discourse, creating a sound and fury of passionately debated claims and counter claims. In that atmosphere, it becomes increasingly difficult to ascertain what to believe, and easy to abandon the task of discerning the truth.

If we are not to fall victim to such rank dishonesty, it is crucial now that we question our sources more carefully than ever before.

Indecision and distraction have long been central to Russia’s dezinformatsiya (disinformation) policy, a term Stalin himself is credited with coining. While an ancient concept, Russia had by the imperial age mastered dark obfuscation techniques refined for the era of mass communication. By the dawn of the Soviet empire, they realized this potential on an industrial scale, establishing the world's first office dedicated to disinformation in 1923. In the 1960s, the KGB covertly sponsored American fringe groups, amplifying conspiratorial narratives about everything from the assassination of president John F. Kennedy to water fluoridation.

The goal, as KGB Major General Oleg Kalugin elucidated in 1998, **was “not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America....”**. Operation INFEKTION, a mid-1980s clandestine effort to spread the myth that AIDS was a CIA-designed bioweapon, was but one infamous exemplar. While utterly fictious, it resonated with communities ravaged by HIV and neglected by the callous indifference of the Reagan administration. Despite Russian intelligence taking responsibility for this lie in 1992, the legacy of AIDS denialism persists to this day worldwide.

During the Cold War, the doctrine of “active measures” was the beating heart of Soviet intelligence. This philosophy of political and information warfare had wide remit, including front groups, media manipulation, counterfeiting, infiltrating peace groups and even the occasional assassination.

And in our media-saturated era, Russia has been, by far, disinformation’s most enthusiastic user. Take the 2016 U.S. presidential election and the contentious Brexit referendum; Russia appears to have influenced both via lies and distortions.

But disinformation is not solely confined to geopolitics. By summer 2020, the European Commission identified a concerted Russian drive to propagate COVID disinformation worldwide. From the outset of the pandemic, Kremlin-backed troll farms pushed the narrative that COVID was an engineered bioweapon, peddling the explosive fiction that 5G radio frequencies caused the virus—a lie that resulted in dozens of arson attacks on cell towers worldwide.

There is a dark irony in the observation that conspiracy-minded people can be weaponized in plots to which they’re entirely oblivious. The enduring popularity of the virus-as-a-bioweapon mantra is a stark reminder that in the age of social media, such manipulation has become ever easier and more effective. Perhaps the most odious example of this is the cynical rise of anti-vaccine propaganda.

The sheer efficacy of vaccination is scientifically incontrovertible, and after clean water, immunization is the most life-saving intervention in human history. Despite this, the last decade has witnessed precipitous drops in vaccine confidence worldwide. The renaissance of once-virtually-conquered diseases prompted the WHO to declare vaccine hesitancy a top-10 threat to public health in 2019.

Sign up for Scientific American’s free newsletters.

Vaccine hesitancy is a spectrum rather than a simple binary, and exposure to anti-vaccine conspiracy theories nudges recipients towards rejection. But critically, many who decline vaccination are not dyed-in-the-wool anti-vaccine zealots, but simply scared by what they have heard, unsure what to believe. Our tendency towards the illusory truth effect exacerbates this inertia, as the mere repetition of a fiction is enough to prime us to accept it, even if we know it to be false on an intellectual level. While Russia has often amplified anti-vaccine conspiracy theories to increase tensions, the anti-vaccine movements exist independently of these efforts, and are masters at sowing the seeds of doubt with torrents of conflicting and emotive claims.

This illustrates the grim reality that disinformation has no need for consistency and zero commitment to objective reality; claims are frequently contradictory, arguing both sides of the coin in exaggerated and divisive ways. This “Russian firehose” model of propaganda is high-output, contradictory and multichannel. The stream encourages us to sleepwalk into apathy, distrustful of everything. This renders us supremely malleable, and dangerously disengaged.

When it comes to vaccination, concerned parents often opt to stay with the devil they know, delaying or even rejecting vaccination rather than sifting through the symphony of conflicting claims to which they’re subjected. Similarly, the outpouring of fictions about Ukraine, its president, Volodymyr Zelensky, and the war is designed to overwhelm our capacity to analyze, inducing us to implicitly accept uncertainty over aggressor and aggrieved—a manufactured doubt benefitting Russia and other nations.

**Conviction is not the chief goal of disinformation; instilling doubt is.** This is why anti-vaccine activists have been so successful online, and why Russian troll-farms push ample resources into hawking lies virtually everywhere. The ubiquity of these fictions gives them an implicit veneer of legitimacy, fueling polarization and distrust.

This is the strategy Putin continues to pursue; already Russian propaganda has tried to paint Ukraine (or NATO / America) as aggressors with staged disinformation. This has been rendered less effective by the Biden administration’s creative approach of releasing intelligence prior to the operation. Across social media, Russian front organizations still try to induce doubt, efforts that will only intensify as the war wages on. Truth, the old adage insists, is the first casualty of war.

### Disinfo Causes Confusion

#### Disinformation attacks seek to destabilize and confuse adversaries during time sensitive events

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 6, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

The most commonly agreed-upon purpose of disinformation in both domestic and international politics is to distract, confuse and demobilize adversaries.26 The chain of thought is as follows: disinformation seeks to confuse an adversary to such a degree that even if it is debunked later on, the short-term distraction yields sufficient strategic payoff for the source of disinformation (‘Attacker’) in the form of demobilizing and dividing the other side (‘Defender’). Since disinformation attempts often get fact-checked and debunked, their strategic utility is often short-term.27 Therefore, disinformation works best during time sensitive events such as elections, diplomatic crises, emergencies and natural disasters.

In the case of an election, the ‘Attacker’ attempts to boost the chances of the friendly candidate and weaken the hostile one in the ‘Defender’ country, increasing the likelihood of the friendly candidate getting elected. If the hostile candidate’s victory is inevitable, the purpose of disinformation becomes weakening the hostile candidate’s winning margin so that their rule becomes more difficult and contested. This prevents the hostile candidate’s ability to focus on the Attacker country after the election.

In the case of a diplomatic crisis or escalation, the logic works similar: by distracting and confusing an adversary, the Attacker seeks to gain short-term strategic payoff either by reducing the level of support for the Defender government or its policies, or slow down and demobilize its current course of action. In cases of direct armed conflict, disinformation is used to demoralize, demobilize, discredit and slow down the adversary’s diplomatic and military efforts.

#### Disinformation in cyber warfare causes chaos and confusion to create fake narratives that undermines truth-

**Szabó, security engineer & International Centre for Migration Policy Development research intern, 22**

[Réka Szabó, works for the International Team for the Study of Security Verona in the International Centre for Migration Policy Development as a research intern, 6-18-2022, International Team for the Study of Security Verona, "Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?", <https://www.itssverona.it/wp-content/uploads/2022/06/Reka-Szabo.pdf>, p. 9-10, accessed on 7-2-2022, MG]

Russia, similarly to its activities during the annexation of Crimea, used fake news to strengthen the Russian narrative about events. Disinformation has been a significant part of cyber warfare, aimed at undermining public opinions. According to Meduza, Russian media portrayed a Ukrainian refugee from Mariupol as a testimony of atrocities committed by Ukrainian soldiers against civilians, and who blames the mayor of the city for having abandoned the people. The video containing such fake pieces of information was distributed by the FSB.36 Bot farms, supported by the Russian state, were also active on social media and distributed fake news about the war. Not only Russia-based actors have had a huge part in cyberattacks in this war. The Belarus APT Group launched disinformation campaigns (by hacking social media platforms of high profile Ukrainians) and phishing campaigns with malware, against ”European government personnel involved in managing the logistics of refugees fleeing Ukraine.

#### Information proliferation can be weaponized by increasing the amount of disinformation and taking advantage of the lack of attention the public gives to where the “information” came from

**Hills, University of Warwick Psychology professor, 18**

(Thomas, 11-28-18, Perspectives on Psychological Science, "The Dark Side of Information Proliferation, <https://doi.org/10.1177/1745691618803647>, SAGE journals, accessed on 07-1-22 SR)

Anti-expert speech, fake news as a political weapon, the replication crisis, relentless health warnings associating cancer with everything we eat, and the richly documented pathologies of online inattention are all symptoms of a rising awareness that information is not benign (Bawden & Robinson, 2009; Carr, 2011; Eppler, 2015; Jacoby, Speller, & Kohn, 1974; Schoenfeld & loannidis, 2012; Schwartz, 2004). A common contributor to each of these problems and the focus of this article is information proliferation—the capacity to access and contribute to a growing quantity of information. According to the International Telecommunications Union (2017), more than 4 billion people are now mobile-broadband users, granting each near instantaneous power to access, create, and share information. This represents a 5-fold increase since 2010. Simultaneously, our technological capacities to store and share information have soared (Hilbert & Lopez, 2011; van den Bosch, Bogers, & de Kunder, 2016). The result of this proliferation is that information is placed increasingly under the influence of an attention economy (e.g., Lanham, 2006) in which a growing number of people influence the evolution of information by what they pay attention to (e.g., Bakshy, Messing, & Adamic, 2015; Gentzkow & Shapiro, 2010).

Herbert Simon (1971) captured the central constraint on this attention economy when he noted that “information . . . consumes the attention of its recipients, (p. 40). We are limited in how much information we can attend to from outside sources (sometimes called the cocktail party problem; e.g., Conway & Cowan, 2001) and how much information we can process (e.g., in working memory; Miller, 1956). Thus, too much information threatens us with information overload and other pathologies of attention that have been well- documented elsewhere (Bawden & Robinson, 2009; Carr, 2011). This articles focuses on a less well- documented but perhaps more pernicious problem: how information-rich environments place information under the forces of cognitive selection, driving the evolution of information much like other forms of selection drive biological evolution.

#### Russian mass disinformation uses disinfo to cause confusion and deflect blame for food crisis

Department of State, 22

(United States Department of State, "Russia’s Disinformation Cannot Hide its Responsibility for the Global Food Crisis," 6-22-2022, https://www.state.gov/disarming-disinformation/russias-disinformation-cannot-hide-its-responsibility-for-the-global-food-crisis/, accessed 7-1-2022) jh

Russian President Putin’s illegal and unprovoked war against Ukraine has had catastrophic effects on Ukraine, its neighbors, and people across the globe. The Kremlin’s war in Ukraine has wreaked death and destruction, killing thousands of civilians , displacing millions , making refugees of millions more, and massively damaging civilian infrastructure . The devastating effects of Russia’s aggression have disrupted Ukraine’s economy , which in turn has exacerbated global food insecurity. Ukraine has long been the “breadbasket of Europe, ” feeding millions of people across the globe. It is a top grain supplier to dozens of African and Middle Eastern countries. Now, after Russia’s February 24 all out invasion, Ukraine has turned “from a breadbasket to a breadline, ” while the Russian government uses disinformation to mislead the world about the cause of this crisis.

Food insecurity has risen because of Putin’s war of choice. It was not caused, as the Kremlin claims, by sanctions that the United States and many other countries have imposed in response to Russia’s horrific aggression against Ukraine. Food insecurity was rising before the invasion, and Putin’s war exacerbated that trend. Russia mined Ukrainian grain fields, attacked merchant shipping on the Black Sea, and blocked Ukrainians from exporting their own grain. Russia is also plundering Ukrainian grain for its own profit, pilfering grain from Ukrainian warehouses according to credible reports. All these actions have worsened food insecurity around the world.

Conversely, the United States and its partners have taken great care to avoid exacerbating food insecurity. U.S. sanctions, for example, are specifically written to prevent food insecurity: they include carveouts for agricultural commodities and permit transactions for the export and re-export of food to and from Russia, even with a sanctioned individual or entity. Moreover, the United States has pledged $2.6 billion this year in humanitarian food assistance to help alleviate world hunger, with an added $5 billion to be added over the next five years.

Russia’s government officials, Russian state-funded media, and Kremlin-aligned proxy disinformation actors are attempting to deflect attention from Russia’s responsibility for worsening global food insecurity by blaming sanctions, “the West,” and Ukraine. In fact, the Kremlin and its proxies’ massive disinformation campaign is heavily targeting the crisis’s most heavily impacted regions – the Middle East and Africa. These false narratives are amplified by Kremlin-controlled state outlets such as RT Arabic and RT en Francais , as well as the People’s Republic of China (PRC) state media .

As it has with past false narratives about bioweapons in Ukraine , the Russian government’s top diplomats and its embassies spread disinformation, often concentrating on African and Middle Eastern audiences. Some recent false claims include:

Russia’s Ministry of Foreign Affairs’ spokeswoman Maria Zakharova called Russia’s blockade of Ukrainian grain “Western and Ukrainian disinformation .”

In his May 19 United Nations Security Council speech on conflict and food security, Russia’s UN Ambassador Vasiliy Nebenzya accused Europe of “hoarding” Ukrainian grain and engaging in “grain for weapons ” exchanges with Kyiv.

Russia’s embassy in Egypt blamed “illegal unilateral sanctions ,” while Russia’s embassy in Zimbabwe claimed “Western interference ” in the Global South.

In his May 25 Africa Day speech, Russia’s Foreign Minister Sergei Lavrov attempted to de-legitimize Ukraine and urged African ambassadors in Moscow to demand the removal of “illegal, anti-Russian” sanctions in order to strengthen food security.

OneWorld , a website with ties to Russia’s military intelligence, according to U.S. officials, echoed Lavrov’s claims, accusing President Zelenskyy of supporting a U.S.-led “global food cartel ” that will wield control over global food supply as a “new hybrid weapon ” against the Global South.

In his May 26 interview with RT Arabic, Foreign Minister Lavrov accused the West of neo-colonialism and of blackmailing African and Arab countries to join “anti-Russia” sanctions, in a bid to build solidarity against what Russia’s propaganda calls the “imperial West .”

This disinformation is intended to both hide Russia’s culpability and persuade leaders of at-risk countries to support an end to sanctions designed to stop Russia’s unjust and brutal war in Ukraine.

The Russian government’s attempts to deflect responsibility for its actions by blaming others for the worsening crisis in the global food system are reprehensible. This crisis is keenly felt in many Middle Eastern and African countries that import at least half of their wheat from Ukraine. According to World Food Program, millions of people are at risk of famine and malnutrition in these regions, as Putin’s reckless war increases the price of bread, taking money from the pockets of the most vulnerable families. “Russia is solely responsible for this food crisis … despite the Kremlin’s campaign of lies and disinformation,” said European Council president Charles Michel as Russia’s UN Ambassador Nebenzya stormed out of a June 6, 2022, UN Security Council meeting.

The Russian government continues spreading disinformation about its unjustified war’s disastrous consequences, including global food insecurity. The Russian government should stop weaponizing food and allow Ukraine to safely ship out its grain so that millions of hungry people in the Middle East and Africa can be fed.

### Disinfo Causes Polarization

#### Disinformation deepens polarization in political, economic, and social cultural spheres.

**Colomina College of Europe Associate Professor European Union Research Fellow, et al., 21**

(Carme, Hector Sanchez Margalef Barcelona Centre for International Affairs Researcher, and Richard Youngs, Carnegie Europe Democracy, Conflict, and Governance Program Senior fellow, 4/2021, European Parliament, “The Impact of Disinformation on Democratic Processes and Human Rights in the World”, p. 21-2, <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf>, accessed on 6-28-2022, SR)

Disinformation impacts not only the political sphere, but also economic, social and cultural aspects of life, from personal mindsets about vaccinations to disavowing cultures or different opinions. Disinformation feeds polarisation and erodes trust both within institutions and amongst communities. Such manipulation tactics can damage personal rights to health and education, participation in cultural life and membership of a community. There are several economic, social and cultural rights that can be disrupted by disinformation, such as those included in Article 25(1) UDHR: ‘Everyone has the right to a standard of living adequate for the health and well-being of himself and of his family, including food, clothing, housing and medical care and necessary social services, and the right to security in the event of unemployment, sickness, disability, widowhood, old age or other lack of livelihood in circumstances beyond his control’. Article 12 of the ICESCR affirms: ‘1. The States Parties to the present Covenant recognise the right of everyone to the enjoyment of the highest attainable standard of physical and mental health.’ The most prominent recent example relates to disinformation around COVID-19, which has distorted freedom of choice even within a health context (see also Chapter 4 on COVID-19). Blackbird55, an organisation whose purpose it is to enhance decision making and empower the pursuit of information integrity’ 56, released studies analysing the volume of disinformation generated on Twitter as a result of the COVID-19 outbreak. In one of its reports57, Blackbird identified one of the disinformation campaigns unfolding in Twitter as ‘Dem Panic’, which had the goal of de-legitimising the Democratic Party in the US for their early warnings about the coronavirus and the need to introduce preventative measures. Downplaying effects of the virus can clearly have negative impacts on public health. The Lancet warned in October 2020 that the anti-vaccine movement together with digital platforms are becoming wealthier by hosting and spreading disinformation campaigns in social media58. It is claimed that ‘anti-vaxxers have increased their following by at least 7·8 million people since 2019’ and hence ‘the anti-vaccine movement could realise USD 1 billion in annual revenues for social media firms’.

#### Russian disinformation discredits politicians and weakens historical and cultural ties to community, weakening institutions.

Erlich, **McGill University Department of Political Science** Assistant, and Garner University of Washington Political Science PhD Candidate, 21 (Aaron and Calvin, 11-1-2021, SAGE Journals, "Is pro-Kremlin Disinformation Effective? Evidence from Ukraine", https://journals.sagepub.com/doi/full/10.1177/19401612211045221#\_i3, accessed on 7-6-2022, SR)

Our first contribution is to classify and quantitatively measure belief in various types of pro-Kremlin disinformation statements according to the topic they cover and the strategic objective they advance. Since these disinformation campaigns have covered a wide range of events, we sought to systematically categorize them. Our close reading of pro-Kremlin disinformation articles leads us to argue for a topic categorization similar to Meiselman et al. (1987), who wrote of Soviet disinformation during the Cold War, “There are basically three types of disinformation: political disinformation, military disinformation, and economic disinformation” (33). Indeed, we argue that many contemporary pro-Kremlin disinformation stories can be grouped into the three high-level topics Meiselman et al. (1987) identify. To these three topics, we add a fourth category, historical/cultural claims or statements (we label these historical for brevity), which we found abundant and which did not fit into the three previous categories. Indeed, we chose these four areas because of their relevance in both historical and contemporary Russian disinformation efforts. We present each of these categories, which should apply generally to pro-Kremlin disinformation, but focus on Ukrainian examples, given our study is carried out in Ukraine.

Economic coverage may be a fecund area in which to sow disinformation, particularly in countries with a history of economic mismanagement such as Ukraine. Citizens may be susceptible to stories that disparage the domestic economy because they are accustomed to hearing true stories of economic mismanagement and corruption. Such mismanagement has pervaded Ukraine’s post-Soviet history (Åslund, 2005) and continues to plague contemporary Ukraine (Denisova-Schmidt and Prytula, 2017). Citizens may also believe political disinformation in nascent and noninstitutionalized democracies, such as Ukraine, because of the weakness of political and democratic institutions (Way, 2015). Therefore, similar to the relationship between weakening political institutions in OECD democracies and increased belief in disinformation (Bennett and Livingston, 2018), the lack of political institutional authority makes it more likely that citizens will believe disinformation about politics. Indeed, Ukrainians often view political actors as likely to deceive them and engage in unscrupulous behavior (Chudowsky and Kuzio, 2003, 278). As with the economic topic, disinformation about Ukrainian politicians or governing structures may sway audiences accustomed to hearing negative news about their politicians.

Pro-Kremlin disinformation claims about the military deserve particular attention in Ukraine. Military-related disinformation forms a recurring part of Russia’s global disinformation efforts and was part of Russian efforts to distract or mislead the international community and the Ukrainian population in response to Russia’s invasion of Crimea and support for insurgents in eastern Ukraine (Iasiello, 2017). Additionally, Russia has used disinformation aimed at discrediting NATO and other Western institutions to reduce their allure within Ukraine (Lange-Ionatamišvili, 2015). Finally, Russia has spread falsehoods about the actions of the Ukrainian military (Khaldarova and Pantti, 2016). Prior research suggests that military-related disinformation could be highly believable because, as with rumours, citizens usually do not have firsthand information about a conflict, and latching onto the disinformation claim can be a mechanism to cope with anxiety (Greenhill and Oppenheim, 2017).

We also find a large quantity of pro-Kremlin disinformation attempting to taint Ukrainian leaders with unsavory historical or cultural connections. This type of disinformation leverages the propaganda technique that Sproule (2001) has classified as “name-calling” and has been found to be prevalent in other contemporary propaganda contexts (e.g., Lakomy, 2020). Russia’s use of “name-calling” in the history topic likely also emerges out what have been dubbed the “memory wars” (Koposov, 2017). Russian leadership maintains the Soviet view that Russia was a liberating victor of World War II that vanquished the Nazis. Therefore, disinformation claims that fall in the historical topic tend to paint individuals or governments as having fascist or Nazi connections and attempt to reinforce Russia’s historical propaganda.

Along with varying topics, pro-Kremlin disinformation also appears to pursue varying strategic objectives. In one analysis, Kragh and Åsberg (2017) investigate a corpus of 3,963 Swedish Sputnik articles published in 2015 and find ten strategies, such as sowing “crisis in the West,” promoting a “positive image of Russia,” highlighting “Western aggressiveness,” and others. In a meta-analysis of annual reports from security services in 11 countries, Karlsen (2019, 10) similarly finds a common strategy is to blame problems on Western actions. In the Baltic States, common claims focus on the return of Nazism and fascism, and emphasize Soviet heroism in WWII and NATO aggression. We categorize all of these strategies into three types emerging from both recent scholarship and the literature on Soviet disinformation practices: “Undermine the government of the country” (undermine Ukraine), “Build up Russia” (pro-Russia), and “Disparage Western partners” (anti-West).

### Disinfo Undermines Intelligence

#### Pervasive disinformation undermines credibility of intelligence sharing and integrity of the information space – which undercuts threat assessment and management

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 295-7, accessed 6-22-22, AFB]

The Future is Here

Questions about the evolution of the disinformation threat strike at the core of NATO’s political mandate as a military alliance and its ability to assess and respond. “Netwar” has changed the nature of conflict with profound implications for disinformation. The term was used in 1992 in a prescient analysis by RAND alluding to both the role that the internet would have in shifting the realities of conflict and national security, and the way that conflict would morph into a structure that relied more on networks than strict hierarchies and command chains.43 Disinformation and the more general manipulation of the information space (through political, economic, technological, cyber or social engineering tools) have emerged in the past decade as profound mutations in the way we understand security. First, online conflicts have merged with offline conflicts. War is declared online: social platforms are used to amplify the perception of war or the strength of the enemy, to recruit combatants and report from the battlefield, while at the same time creating far deeper divisions that can in fact expand the causes of war.44 “Social media has changed not just the message, but the dynamics of conflict” to the extent that researchers are questioning the very definition of war.45 Both ISIS and Russia offer ample illustrations of how disinformation and digital manipulation are fully integrated with physical aggression and military operations. In the case of Russia, the integration of information operations with war fighting—the so-called “Gerasimov doctrine”— became an important topic for NATO and allied decision-makers.46 Second, disinformation and digital deception are used in the battle to achieve cognitive and behavioral outcomes in societies. National militaries are reorienting to also face information warfare. Significantly, domestic politics has also reordered around the ability to create and influence (or manipulate) online constituencies. Political actors in most countries, whether democratic or not, now rely on troll armies and digital influencing campaigns to alter democratic processes.47 This shift in domestic political debate also has an impact on the Alliance’s internal functioning. As political actors in some member states are increasingly utilizing information and digital manipulation, they are not only departing from principles and values NATO is built upon (and clearly outlined under Article 2 of the NATO Charter) but are also creating additional avenues for malign foreign actors to infiltrate democratic societies and weaken them from within. Third, authoritarian nations attempt to polarize and weaken national security structures, diminish trust in alliances, and thus hamper the cohesion and effectiveness of national and supra-national defense structures. NATO has been a primary target. Anti-NATO narratives and conspiracies are an important tool in the arsenal of digital manipulation campaigns undertaken by pro-Kremlin groups. NATO is portrayed as an alliance that fosters insecurity, rather than protect its members. It is depicted as an extension of the US military-industrial complex, as a platform for war-mongering elites to demonize Russia and fuel Russophobia, and as a tool in the hands of bigger, more powerful democracies to dominate smaller countries and use them as cannon fodder in case of a conflict. Defense contractors have also come under attack by disinformation perpetrators with the aim to discredit them and deflate public trust in the operations and relevance of these companies.48 Military personnel and particularly NATO troops are being targeted during military exercises,49 such as the “Lithuanian Lisa case” and in Defender 21.50 Similarly, adversaries use cyber and information tactics to collect troves of data over a long period of time that could be used against military targets or during military operations.51 An underexplored area is also the impact that disinformation might have on intelligence collection and sharing. It is unclear whether disinformation, which targets the integrity of and ability to verify information, could be altering open-source intelligence gathering or hampering exchanges between allies, particularly as some domestic actors engage in disinformation operations themselves. The integrity of the information space is crucial for equalizing threat perception among Allies and accurately defining security threats.

#### Information space is exploited by Russia to continue to spread disinformation

**Hakala, NATO Strategic Communications Centre of Excellence researcher and Melnychuk, Canadian Department of National Defence Communications Officer, 21**

[Janne & Jazlyn, 6-15-21, NATO Strategic Communications Centre of Excellence, "RUSSIA’S STRATEGY IN CYBERSPACE", <https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf>, p. 5-7, accessed on 7-2-22, MG]

Russia’s conceptualization of ‘information confrontation’ and the role of cyberspace within it is outlined in strategic policy documents, such as National Security Strategy (2015), Foreign Policy Concept (2016), Information Security Doctrine (2016), Military doctrine (2014), Conceptual Views on the Activity of the Armed Forces in the Information Space (2016), as well as works and publications by Russian military thinkers.

From the Russian perspective, cyber warfare or the Russian equivalent ‘informationtechnological warfare,’1 is only a part of the overarching concept of “information confrontation” (informatsionnoe protivoborstvo). The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary’s information infrastructure while protecting its own objects from similar influence.2 The translation of the term informatsionnoe protivoborstvo into English has proven difficult, and has often incorrectly been translated as ‘information warfare’3 (‘informacionnaja vojna’), despite the fact that protivoborstvo refers to ‘counterstruggle’, ‘countermeasure’ or ‘counteraction’ rather than ‘warfare’.4 This paper uses the term ‘information confrontation’ due to its established status in discussions regarding hostile Russian informational activities.

The confrontation includes a significant psychological remit, whereby an actor attempts to affect informational resources (documents in information systems) as well as the minds of the adversary’s military personnel and population at large.5 Ultimately, cyber operations (or informationtechnical means) are one of many methods used to gain superiority in the information confrontation. Russia, and particularly Russian President Putin’s regime, sees the information confrontation as a constant geopolitical zero-sum competition between great powers, political and economic systems, and civilizations.6

Protecting ‘Information’: Cognitive and Technical Publicly available Russian doctrines and policy documents do not explicitly reference cyber operations. Furthermore, Russian documents do not use the term ‘cybersecurity’, but refer instead to ‘information security.’ This term differs from the Western notion of ‘information security’ (or in short: infosec) in that it encompasses not only the protection of critical digital networks, but society’s cognitive integrity as well.7 There are several reasons why Russian military thinkers apply the term ‘cyber’ when talking about Western threats and activities, but are reluctant to link the term to Russia’s own capabilities and actions. Some authors argue that this deliberate choice is related to negative connotations around Soviet-era ‘cybernetics,’ as well as the importance the term ‘information security’ holds for Russia’s own domestic politics 8.

When discussing the operational environment, Russia uses the term ‘information space’ (informatsionnoe prostranstvo), or ‘information sphere’ (informatsionnaya sfera), which again is more comprehensive than the Western concept of ‘cyberspace’ or ‘cyber domain.’ The 2016 Russian Doctrine of Information Security defines the information sphere as: “a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet […], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere”.9

The information space refers to activities to form, transform, and store information, as well as ‘influencing individual and public consciousness, information infrastructure and information itself.’10

According to Ofer Fridman, Russia conceptualizes cyberspace as the intersection between hardware, software, infrastructure, and content11. In this framework, the information-technological layer includes hardware, software and infrastructure, while the informationpsychological layer includes hardware, software and content.’ Irrespective of the means used – technological (for example, destroying digital infrastructure) or psychological (manipulating a message on social media) – activities in cyberspace are understood in terms of their effect in the information space.12 Importantly, Russia perceives the information space in very geopolitical terms, with their domestic information space representing a continuation of territorial state borders, which they view as constantly being violated by foreign intrusions.13

NATO doctrine understands cyberspace as an operational domain and considers it as part of the information environment. This environment is ‘[…] comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information’. The information processed through this environment provides the base for cognitive processes that affect individual decision-making and subsequently, behaviour. Those processes happen in three dimensions – physical, virtual and cognitive – and cyberspace involves all three of them. In this respect, NATO’s concept of the information environment is not that different from Russia’s understanding of ‘information space’ and the role of cyberspace within it. Similarly, the Russian concept of ‘information weapons’ (practically absent in Western parlance) includes more than just digital measures.14 Although the Russian Armed Forces vaguely defines them as “information technologies, means and methods used for the purposes of waging information war,” in practice the concept covers a wide array of activities (often with an emphasis on affecting the human mind); this includes the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.15

Contrary to the Western view of interstate conflict that is based on the international legal order outlined in international treaty and customary law (specifically the UN Charter and the Geneva Conventions) that makes a clear distinction between war and peace, Russia’s ‘information confrontation’ is constant and ongoing. This view is exploited by Russia to undertake activities beneath the threshold of armed conflict, allowing it to remain unpredictable and pursue strategic objectives short of causing kinetic conflict.16

A key goal of Western democracies is to maintain a free, stable and open Internet, where fundamental rights and freedoms are ensured. In this regard, ‘information security’ is perceived as the protection of data and systems, but not imposing control over the attitudes and beliefs that the users of those systems are expressing. At the same time, the principles of openness and freedom of speech upheld in Western democracies might be exploited by information and cyberattacks. Russia seeks to exploit this openness to gain ‘information superiority,’ notwithstanding whether it is in a conventional conflict with its opponents or not.

### Disinfo Undermines Expert Credibility

#### Disinformation discredits sources of higher epistemic quality promoting pseudoscientific hesitancy.

Mckay and Tenove, The University Of British Columbia Vancouver; Centre for the Study of Democratic Institutions Research Associate and Political Science Postdoctoral Research Fellow, 20

(Spencer Mckay, The University Of British Columbia Vancouver Centre for the Study of Democratic Institutions Research Associate, Chris Tenove, Chris Tenove, University of British Columbia Political Science Postdoctoral Research Fellow. SAGE Journals, 7-4-2020, "Disinformation as a Threat to Deliberative Democracy," Political Research Quarterly 2021, Vol. 74. No. 3, p. 708, https://journals.sagepub.com/doi/full/10.1177/1065912920938143, accessed 7-1-2022) SS:/

Inconsistent democratic oversight of platforms and other media entities allows disinformation campaigns to leverage algorithmic gatekeeping and opportunities for viral amplification to distribute false claims. The amplification and transmission of misleading claims across sites may undermine a deliberative system’s epistemic function because even incidental exposure can increase the probability of belief in false information (Feezell 2018; Pennycook, Cannon, and Rand 2018). These tactics can be seen in Russian campaigns that promote pseudoscientific conspiracies on vaccines and other issues (Broad 2020; Broniatowski et al. 2018; DiResta et al. 2018, 69). Simply examining the balance of true and false claims may not capture the full range of epistemic harm (Starbird, Arif, and Wilson 2019, 18–19). Disinformation actors not only propagate false and deceptive claims, they often seek to crowd out or devalue contributions from processes or institutions of higher epistemic quality (Hagen et al. 2020; Krafft and Donovan 2020). For instance, Russian disinformation actors routinely spread false news stories and attack professional journalism organizations (DiResta et al. 2018, 66–67; U.S. Senate 2019, 20–21); they also disparage science agencies while amplifying pseudoscientific conspiracies (Broad 2020; Broniatowski et al. 2018). These efforts built on increasing distrust of news media and institutions of expertise in the United States, particularly on the right (Mitchell et al. 2019). Research suggests that false claims are more likely to gain traction in a system where there is antipathy toward intellectuals, expert consensus, and scientific institutions (Stecula, Kuru, and Jamieson 2020).

#### Internal Link – Disinformation is used to create fake institutions that deck the credibility of legitimate institutions.

\*This card indites why we have become less trustful of journalists as qualified authors in debate. It also explains how we have become so concerned about disinformation that we disengage from news entirely.

Mckay and Tenove, The University Of British Columbia Vancouver; Centre for the Study of Democratic Institutions Research Associate and Political Science Postdoctoral Research Fellow, 20

(Spencer Mckay, The University Of British Columbia Vancouver Centre for the Study of Democratic Institutions Research Associate, Chris Tenove, Chris Tenove, University of British Columbia Political Science Postdoctoral Research Fellow. SAGE Journals, 7-4-2020, "Disinformation as a Threat to Deliberative Democracy," Political Research Quarterly 2021, Vol. 74. No. 3, p. 708, https://journals.sagepub.com/doi/full/10.1177/1065912920938143, accessed 7-1-2022) SS:/

In addition to attacking the credibility of institutions that claim higher epistemic quality, such as news outlets and think tanks, Russian disinformation campaigns also create faux versions of these institutions, which can promote competing claims on issues (Broad 2020). This tactic has long been used by “merchants of doubt” to sew confusion about climate change or the health risks of tobacco (Oreskes and Conway 2011) but is made easier by the problem of “source blindness” on social media (Pearson 2020). The proliferation of competing claims can contribute to the belief that truth claims, including expert claims, are largely dictated by political commitments. This cultivation of epistemic cynicism has been identified as part of the Russian government’s “firehose of falsehood” propaganda strategy, which promotes the belief that it is fruitless to seek true accounts of political matters in a media environment replete with conflicting and false claims (Paul and Matthews 2016; U.S. Senate 2019, 16). Online disinformation appears to pose a greater risk than previous attempts at overwhelming citizens with conflicting information due to the possibility of coordinated or algorithmic dissemination of content across platforms (Krafft and Donovan 2020; Wardle and Derakhshan 2017). False and conflicting stories can appear on many different sites and social media pages, creating a situation where individuals conclude, “I don’t know what to believe” (Toff and Nielsen 2018, 649–52). Polling has not only found that concerns about false news are pervasive among Americans, but it has prompted a substantial portion (42%) to reduce their information-seeking and simply consume less news (Mitchell et al. 2019).

### Disinfo Undermines Civilization

#### Internal Link – The corruption of the information ecosystem entails chaos which threatens prosperity and advancement, pillars of civilization.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 5, accessed 7-8-2022) SS:/

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.

### Deepfakes Collapse Info Cred

#### Weaponization of emerging technologies – like deepfakes and AI – destroy info credibility and risk catastrophic backfires

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 297-8, accessed 6-22-22, AFB]

Evolving Challenges

Technological advances tend to be front and center in the discussion about the future of disinformation and digital manipulation. Deepfakes (manipulated audiovisual content), artificial intelligence (AI), and natural language processing (NLP), and their timeline and potential deployment by malign actors are among the potential threats that researchers have been trying to understand. Synthetic online activity has already been piloted by malign actors in different ways online, most notably by Russia’s use of completely fake journalist personas who were getting published by different online news outlets.52 This is a warning of things to come once this technology becomes available and cheap enough for a wider set of malign actors to use.53 There is also the risk of unintended consequences with new technologies—for example, NotPetya malware unexpectedly boomeranged back to Russia and led to billions of dollars of economic loss worldwide. Similar unanticipated scenarios could occur with the rise of technology-backed influence operations, including by weaponizing the discourse around them, which further weakens trust in sources of information and creates additional burdens to prove authenticity.54

#### Widespread deepfake technology provides a new way to spread disinformation throughout the public media, and can be utilized by anyone for malicious use

Fowler, Washington Post Technology columnist, 21

[Geoffrey A., 3-25-21, Washington Post, “Anyone with an iPhone can now make deepfakes. We aren’t ready for what happens next,” https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/, accessed 7-1-2022, LASA-LR]

I’ve made George Washington sing disco and Marilyn Monroe blow me a kiss. With just a photo and an iPhone app, I can create a video of any face saying, or singing, whatever I want.

And now so can you. The technology to create “deepfakes” — videos of people doing things that never really happened — has arrived on smartphones. It’s simple, fun … and also troubling.

The past few months have brought advances in this controversial technology that I knew were coming, but am still shocked to see. A few years ago, deepfake videos — named after the “deep learning” artificial intelligence used to generate faces — required a Hollywood studio or at least a crazy powerful computer. Then around 2020 came apps, like one called Reface, that let you map your own face onto a clip of a celebrity.

Now with a single source photo and zero technical expertise, an iPhone app called Avatarify lets you actually control the face of another person like a puppet. Using your phone’s selfie camera, whatever you do with your own face happens on theirs. Avatarify doesn’t make videos as sophisticated as pro fakes of Tom Cruise that have been flying on social network TikTok — but it has been downloaded more than 6 million times since February alone. (See for yourself in the video I made on my phone to accompany this column.)

Another app for iPhone and Android devices called Wombo turns a straight-on photo into a funny lip-sync music video. It generated 100 million clips just in its first two weeks.

And MyHeritage, a genealogy website, lets anyone use deepfake tech to bring old still photos to life. Upload a shot of a long-lost relative or friend, and it produces a remarkably convincing short video of them looking around and smiling. Even the little wrinkles around the eyes look real. They call it “Deep Nostalgia” and have reanimated more than 65 million photos of people in the past four weeks.

These deepfakes may not fool everyone, but it’s still a cultural tipping point we aren’t ready for. Forget laws to keep fakes from running amok, we hardly even have social norms for this stuff.

All three of the latest free services say they’re mostly being used for positive purposes: satire, entertainment and historical re-creations. The problem is, we already know there are plenty of bad uses for deepfakes, too.

“It’s all very cute when we do this with grandpa’s pictures,” says Michigan State University responsible-AI professor Anjana Susarla. “But you can take anyone’s picture from social media and make manipulated images of them. That’s what’s concerning.”

So I spoke to the people making deepfake apps and the ethics experts tracking their rise to see if we can figure out some rules for the road.

“You must make sure that the audience is aware this is synthetic media,” says Gil Perry, the CEO of D-ID, the tech company that powers MyHeritage’s deepfakes. “We have to set the guidelines, the frameworks and the policies for the world to know what is good and what is bad.”

The technology to digitally alter still images — Adobe’s Photoshop editing software — has been around for decades. But deepfake videos pose new problems, like being weaponized, particularly against women, to create humiliating, nonconsensual fake pornography.

How to spot a fake video

In early March, a woman in Bucks County, Pa., was arrested on allegations she sent her daughter’s cheerleading coaches fake photos and video of her rivals to try to get them kicked off the squad. Police say she used deepfake tech to manipulate photos of three girls on the Victory Vipers squad to make them look like they were drinking, smoking and even nude.

“There’s potential harm to the viewer. There’s harm to the subject of the thing. And then there’s a broader harm to society in undermining trust,” says Deborah Johnson, emeritus professor of applied ethics at the University of Virginia.

Social networks say deepfakes haven’t been a major source of problematic content. We shouldn’t wait for them to become one.

It’s probably not realistic to think deepfake tech could be successfully banned. One 2019 effort in Congress to forbid some uses of the technology faltered.

But we can insist on some guardrails from these consumer apps and services, the app stores promoting them and the social networks making the videos popular. And we can start talking about when it is and isn’t okay to make deepfakes — including when that involves reanimating grandpa.

#### Deepfakes have an impact even if some are poor fakes – multiple examples prove they erode truth and the ability to verify information

**Giansiracusa,** Bentley University mathematics and data science assistant professor**, 22**

[Noah, 3-23-2022, Slate, "The Destabilizing Effects of Even Low-Quality Deepfakes", [https://slate.com/technology/2022/03/zelensky-deepfake-video-surrendering.html accessed on 6-27-2022](https://slate.com/technology/2022/03/zelensky-deepfake-video-surrendering.html%20accessed%20on%206-27-2022) hooch//cs]

Since the weeks leading up to Russia’s invasion of Ukraine, warnings have been circulating that Russia might use deepfake videos—convincing fake videos created with artificial intelligence— in the surrounding information war. Perhaps they would use deepfakes to fabricate a pretext for the invasion, or to have Ukrainian President Zelensky issue an order to surrender. With bated breath we waited, but no sign of deepfakery occurred. Then finally, on March 16—20 days into the invasion and 13 days after Ukraine warned this exact scenario might happen—a deepfake of Zelensky surrendering indeed appeared, and it was … unconvincing and obvious.

The video editing was low-quality, and the voice was noticeably off; few people seem to have been fooled by it. Not to take any chances, Zelensky himself quickly addressed the deepfake, leaving no doubt about its falsity.

One is tempted to conclude from this episode that deepfake algorithms are just not powerful enough yet, that the dreaded moment when deepfakes wreak havoc in political arenas is still off in the distant future, if it ever arrives. However, a closer inspection of the past few years reveals a different story: The destabilizing effects of deepfakes in politics have already arrived—not in a single widely publicized scandal or a flood of numerous incidents, but in an ominous trickle of subtle yet impactful incidents that largely slipped under the radar. This Zelensky deepfake was quickly put to rest, but there are other videos from past years whose authenticity is unclear—even today we don’t know whether they are deepfakes or real. The difficulty in debunking deepfakes isn’t just a question of technological sophistication.

Three years ago, Mother Jones reported a story surrounding Ali Bongo, the president of Gabon. Bongo was hospitalized for an undisclosed illness in October 2018. Two months later, the vice president announced that Bongo had suffered a stroke but was recovering and doing well. However, other than a few photos and a silent video released by the government, there were no signs of Bongo during this time. Speculation proliferated that the officials were lying, that Bongo was in far worse condition than they admitted—and possibly even dead. To help allay these concerns, on Jan. 1, 2019, the government posted to social media a video of President Bongo giving the customary New Year’s address.

But something didn’t seem right.

Bruno Ben Moubamba, a prominent Gabonese politician who ran against Bongo in the previous two elections, claimed the video was a deepfake. He argued that Bongo’s face seemed strangely immobile and that his eye movements did not appear synchronized with his jaw movements. Julie Owono, the international technology lawyer who brought this Bongo saga to the attention of Mother Jones, noted that Bongo blinked only 13 times during the two-minute video, which she said was less than half the typical amount. The deepfake theory rapidly gained a sizable following. Activists argued that Gabon’s ruling party used deepfake technology to hide Bongo’s dire state of health in order to avoid a special election mandated by law to occur if the president is unfit to lead.

One week after the release of the enigmatic New Year’s video, Gabon’s military attempted a coup and explicitly cited the oddness of the video as evidence that the president was absent and that the government was lying about it. The coup failed and the government retained control, and in August 2019 Bongo finally made his first public appearance since the stroke.

We still don’t know whether Bongo’s party used a deepfake video to deceive the public long enough for him to recover—and in doing so illegally avoided a special election that might have led to his ouster. One of the complications is that all the oddities in the New Year’s video that suggest it’s a deepfake could also be the result of Bongo’s stroke.

This event in Gabon foreshadows one that took place in the United States a year later.

On Oct. 2, 2020, just weeks before one of the most important elections in American history, news broke that President Trump had tested positive for COVID-19. Questions mounted throughout the day over the severity of his illness. At 6:31 p.m., he tweeted an 18-second video in which he said that he was heading to Walter Reed, but he reassured people that he thinks he is doing very well.

Just as with Bongo’s New Year’s address, this video looks very strange. Trump has an uncharacteristically flat affect, motionless manner, and vacant look in his eyes. Immediately there was talk on social media of it being a deepfake to hide the dire state of the president’s health.

This time, suspicion quickly faded as more footage of Trump appeared. The theory was fully dispelled when he gave a live address upon departing Walter Reed a few days later. But for a brief moment, it really was hard to know what was going on and what to believe. The existence of deepfake technology meant that Trump’s 18-second video raised more questions than it answered. In hindsight, the things that made the video appear to be a possible deepfake were likely just a result of the president being ill and possibly medicated.

Days later, Trump’s team posted a video of him speaking from the White House lawn, and once again skepticism arose. Some claimed that it looked like the background was “glitchy,” as though there were a green screen behind him. But Slate quickly debunked the doubts.

A few months later, another instance of deepfake dystopia occurred, this time in Myanmar. On Feb. 1, 2021, a military coup officially began when Prime Minister Aung San Suu Kyi—who in the 2010s played a key role in transitioning Myanmar from military rule to partial democracy—was arrested and deposed, along with other members of her ruling party. The president of the U.N. General Assembly called for her immediate release; the U.N. secretary-general said the coup is a “serious blow to democratic reforms in Myanmar.” Suu Kyi is a Nobel Peace Prize Laureate, and while she has received international criticism for her country’s role in the genocide of the Rohingya people and her denial of the atrocities that were committed, she is a legitimate democratically elected leader; the military needed to justify the brazen steps it took.

A military-run TV station broadcast a video recording of a detained former regional chief minister providing a public confession in which he said he bribed Suu Kyi. This seemed to establish the military’s claims that Suu Kyi is corrupt and violated ethics laws. Some claimed the minister’s voice in the video doesn’t sound like his usual one and noted that the visuals look strange: his facial movements follow a repetitive pattern and his expression looks oddly emotionless. To this day, some people suspect it is a deepfake, while others believe the unnaturalness observed in the video is the result of it being a forced confession and poor teleprompting. Once again, we don’t know for sure. The video is somewhat low-resolution and grainy, which makes distinguishing between a deepfake and an authentic video particularly challenging. Suu Kyi is currently under military arrest and facing an array of charges, including corruption—which carries a maximum penalty of 15 years in prison.

What we see in these examples is that the context of a video plays an enormous role in how difficult it is to determine its authenticity. People speak in a somewhat unusual manner in deepfake videos—but, as became apparent with both the Trump and Bongo incidents, people also do so when infirm. The stress of duress, such as the Myanmar official was experiencing, could also alter one’s speech patterns. And the resolution of a video matters: the flaws in deepfakes are more apparent in high-res footage. Finally, the political situation matters. For instance, the Zelensky deepfake was a foolish endeavor not just because it was too amateur to be convincing—it was easy to debunk because Zelensky could respond to it.

Don’t be lulled into a false sense of security by this ill-conceived Zelensky deepfake. More difficult deepfake situations have already occurred in the past and more will surely arise in the future.

### Internal Link – Bioweapon Proliferation

#### Bioweapon Impact - Russian disinformation undermines norms against biological weapons proliferation and increasingly normalizes their usage in conflict

Lenzos, King’s College Social Science Senior Research Fellow, 18

(Filipa, 11/19/2018/King’s college London research portal, The Russian Disinformation Attacks , p. 2, https://kclpure.kcl.ac.uk/portal/files/105122675/The\_Russian\_disinformation\_attack\_LENTZOS\_Published19November2018\_GREEN\_AAM.pdf, Accessed 6-28-2022, LASA-LR)

Disinformation attacks bring with them many dangers. Beyond sowing distrust and political dissent, they can prime a population for physical conflict, and in the case of Georgia, Russia may even be trying to justify future military interference with its neighbor. False claims about biological weapons in particular, though, create an additional grave danger: They erode the international norm against using them, making countries more likely to do so. While it is easy to dismiss the Russian messaging as nonsense, as the US Embassy in Georgia has done, it is important to actively counter the effect it will likely have on the norm against using biological weapons.

An intensifying, multi-channel attack. Stories about supposed US bioweapon labs in neighboring countries, and in particular about the Lugar Center, have circulated for a number of years in the Russian media. Indeed, Russia’s official national security strategy identifies the network of public health laboratories in the Caucasus and Central Asia funded by the US Defense Department as a strategic threat. That said, messaging about the Lugar Center significantly ramped up after Britain identified Russia as the perpetrator of a botched March 2018 murder attempt in Salisbury, England using the nerve agent novichok. (Russian agents tried to kill former Russian spy Sergei Skripal and his daughter Yulia, without success, but ended up inadvertently killing an English civilian.) In early April, embattled Syrian dictator Bashar al-Assad, who Russia supports militarily, attacked civilians in Douma with chlorine gas.

In April, within weeks of Britain pinpointing the Russian state as culpable for the Salisbury attack, and a day after Trump threatened Russia with US missile strikes on Syria in response to the Douma attack, Russian foreign ministry spokeswoman Maria Zakharova questioned the “real goals” of the American “chain of microbiological laboratories” in former Soviet states and of “the Pentagon’s largescale medical-biological activities near Russian borders.” After British counter- 3 terrorism police presented findings from six months of evidence-gathering on the Skripal case, and issued domestic and European arrest warrants for two Russian suspects on September 4, the accusations drastically intensified.

### Disinfo Undermines Public Health

#### Russia and China use disinformation to reduce US credibility on COVID

Bright et al., University of Oxford Oxford Internet Institution The Computational Propaganda Project, 20

(Jonathan, Hubert, Hannah, Mona , Marcel , Nahema , Christian, Katarina , and Philip N. , 04-8-20, Oxford Internet Institute, "Coronavirus Coverage by State-Backed English-Language News Sources", https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2020/04/Coronavirus-Coverage-by-State-Backed-English-Language-News-Sources.pdf, accessed on 7-2-2022, SR)

Criticizing the Democratic Response

**The first theme relates to articles and reports that criticise the responses of governments in Europe and North America.** Some reporting questioned how these countries handled the coronavirus pandemic. An article published by China Plus highlights a survey of US citizens that suggests that President Trump has not taken the situation seriously enough[12], and CGTN wrote that the coronavirus exposed the lack of international leadership from the US.[13] Turkey's TRT World highlighted that minority rights were allegedly under threat during the lockdown in France, labelling that country a place where ‘discrimination is rampant’ and constitutes a ‘societal sickness'.[14]

RT carried a piece claiming that the major pillars of European liberalism-such as the right to free movement—were being torn down.{15] Some reports also claim that Western financial speculators are taking advantage with a ruthless ‘opportunism’ by buying up cheap stock, and that Westerners are selling medical supplies on the black market for hugely inflated prices.(14] Further, some of the outlets ask whether the crisis would be used by Westem leaders to undermine constitutional democratic rights.[16] Iranian outlets such as Press TV have stated that US sanctions have greatly exacerbated the pandemic in their country.{17] Praising their Own Global Leadership

‘The second narrative theme we have identified is the ‘emphasis that state-backed outlets have placed upon the success of their home country in containing the virus.

Chinese state-backed outlets have been keen to ‘emphasise China’s successful containment of the virus, and position China as an exemplar to other nations. ‘Such claims allowed them to build the large amount of ‘love’ reactions referenced above. A People’s Daily article praised ‘academicians from the Chinese ‘Academy of Sciences and Chinese Academy of Engineering [who] have become known as “warriors in white”. They highlight China's resolution of the admissions crisis for the nation’s hospitals.[18] A China Daily article pronounces that ‘Wuhan provides hope for the rest of the world’, while a dedicated section of the China Daily website promotes ‘Fighting COVID-19 the Chinese way’, with links to “five potential treatments” that Chinese researchers have identified as potential treatments for coronavirus. The site also prominently features an article with the claim that “TCM (traditional Chinese medicine) [is] effective in treating COVID-19 patients” [19] Outside of China, TRT World has published articles portraying Turkey positively, asserting that Turkey is better equipped to handle the pandemic with a higher number of ICU beds per capita than China, Europe and the US.[20]

**These state-backed agencies\_\_ present their governments as world powers offing assistance to struggling democracies and other nations suffering from the pandemic**—help is greatly appreciated by those nations. China is especially engaged in a major effort to improve its international reputation by providing assistance to other countries during the pandemic, and these efforts have been widely covered in their state outlets. A CGTN article titled “China announces to help ‘82 countries fight COVID-19" highlights the wide scope of China's international aid.{21] Similar articles in Chinese state outlets show the distribution of Chinese medical supplies such as masks and respirators to highly affected regions such as Italy[22], Spain(23] and the UK.(24] In another instance, CGTN promoted a video showing Italians playing the Chinese anthem to thank China and singing “Grazie China\*[25], **which a number of independent researchers have claimed was manufactured.** Russian outlets employed similar narratives. One ‘Sputnik article claimed that "Russia may supply to Latin America, Africa mobile hospitals to combat COVID-19" Another notes Russia's efforts to provide aid to Italy, with “seven Russian Ilyushin IL76 military transport planes carrying medical supplies and experts to help Italy." RT aired a report about an Italian businessman who replaced an EU flag on his factory grounds with a Russian flag, “to thank Russia for sending 12 planes [while] the EU closes everything down."(26] Turkish Outlets also followed this line with, for example, Anadolu airing articles expressing support for Italy and Gaza.[27]

### Impact – Public Health/Infodemic

**Disinformation can dramatically undermine public health – COVID proves**

**Jenson, Technical University of Denmark Office for Communication and Media officer, , 22**

[Tore Jenson,. 2-18-22, American Association for the Advancement of Science, “Social media echo chambers spread vaccine misinformation”, <https://www.eurekalert.org/news-releases/943999>, accessed on 7-8-2022, MG]

WHO has named vaccine hesitancy one of the greatest threats to global health. Nonetheless, some people are hesitant or refuse to get vaccinated because they do not trust vaccines and health authorities. A new research result from DTU, published in the journal PLOS One, shows that misinformation on social media contributes to this distrust and creates a false image of benefits and disadvantages concerning vaccines.

"Where vaccine supporters often refer to news media and science sites when sharing knowledge about vaccines on Twitter, we can see that profiles belonging to anti-vaccine profiles far more often share links to YouTube videos and to sites that are known to spread fake news and conspiracy theories, which previous research has also shown," says Bjarke Mønsted who holds a PhD from DTU Compute. He continues:

" Furthermore, vaccine opponents profiles often link to commercial sites that sell alternative health products. This is surprising given that vaccine hesitancy often stems from a fear of financial conflicts of interest. Particularly because previous research has shown that 12 people globally are responsible for vaccine misinformation, including people who earn a fortune from the sale of alternative health products."

Along with Sune Lehmann from the Research Section for Cognitive Systems at DTU Compute, Bjarke Mønsted has analyzed some 60 billion tweets written before the pandemic to understand where the discussion about vaccines takes place on Twitter to better understand today's vaccine hesitancy on social media.

Anti- and pro-vaxxers do not talk to each other

Using newly developed methods in the area of artificial intelligence called' deep learning' and 'natural language processing, the researchers have taught a computer to identify which views on vaccines were expressed in a given tweet.

In doing so, they identified the users who consistently expressed strong views in favour of (provaxx) or against vaccines (antivaxx) and from which sources the profiles shared their vaccine information. Their work shows that 22.5 per cent of antivaxx-profiles' vaccine tweets link to YouTube videos.

The researchers then grouped the sources into five categories: Sites known for sharing pseudoscience and conspiracy theories, news sites, social media, YouTube (which was given its own category due to a large number of links), and finally, commercial sites relating to medicine and health.

The research confirms the echo chamber effect, making it hard for vaccine advocates and opponents to encounter each other's views on the internet—because social media algorithms ensure that people interact with others whose opinions align with their own.

" In fact, we discovered that the sources of information, which people are exposed to in their social networks, depend heavily on their own attitudes towards vaccines. The more resistance to vaccines a user expressed, the further from the norm was the media picture they were exposed to from their circle of friends," says Bjarke Mønsted.

Combatting misinformation is a joint responsibility

Suppose the health authorities want greater support for vaccines. In that case, the responsibility lies not just with the tech giants but also with media outlets when it comes to avoiding medical misinformation, says Bjarke Mønsted.

" Research clearly shows that combatting misinformation is a joint responsibility. It is important that media outlets do not create a false balance between views giving equal, or maybe even more, airtime to anti-vaccine arguments that are not substantiated by the scientific literature. Media should not portray medical information and misinformation as equivalent views," says Bjarke Mønsted.

Professor Sune Lehmann hopes that the novel method, which he and Bjarke Mønsted have developed and used to analyze the many billions of tweets, can provide a greater understanding of the vaccine discussion during the pandemic and in the future:

"Our research covers the period before COVID-19. And there is no doubt that vaccines have become a talking point in a whole new way in the last two years. It has gained a lot of attending and been overturned in a completely new way in the last two years. Vaccines have gone from being a topic that was primarily discussed among particular population groups to becoming a markedly more mainstream topic. Therefore, the exciting challenge going forward will be to use our methodological innovations to understand whether—and how—this shift has changed the discussion and the various actors' motives."

#### Disinformation is deadly and can cause preventable deaths – COVID infodemic proves

Gisondi et al., Stanford University Emergency Medicine professor, 21

[Michael A., Rachel Barber (Undergraduate degree in human biology), Jeremy Samuel Faust (emergency physician at Brigham and Women's Hospital and an instructor at Harvard Medical School), Ali Raja (Executive Vice Chair of the Department of Emergency Medicine at Massachusetts General Hospital), Matthew C Strehlow (Associate Professor, Vice Chair of Strategy, Director Stanford Emergency Medicine International (Emergency Medicine), Lauren M Westafer (University of Massachusetts Medical School Emergency Medicine Assistant Professor), Michael Gottlieb (Director of Emergency Ultrasound (Emergency Medicine)), 12-8-21, Journal of Medical Internet Research, "A Deadly Infodemic: Social Media and the Power of COVID-19 Misinformation", <https://www.jmir.org/2022/2/e35552>, accessed on 7-8-2022, MG]

The COVID-19 pandemic continues to have a substantial impact worldwide, with over 266 million diagnosed cases and over 5 million deaths [1]. In 2021, depending on the month, COVID-19 was either the first, second, or third leading cause of death in the United States, alongside heart disease and cancer [2]. People are still dying from COVID-19 despite a vaccine surplus in wealthy countries, public health interventions to curb viral transmission, new therapeutic options, and the heroic efforts of frontline care providers. Why? Although we initially focused on a deadly and contagious virus, we were simultaneously overwhelmed by the deadly and contagious impact of online misinformation and disinformation about that virus [3]. Much like the COVID-19 pandemic itself, we face a widespread disease with long-term consequences: the COVID-19 infodemic.

The World Health Organization defines an infodemic as “too much information or false and misleading information” that “causes confusion, risk taking behaviors...and mistrust of health officials” [4]. The United Nations Educational, Scientific, and Cultural Organization considers fake news a general term for false information that can be further defined by intentionality [5]. Misinformation consists of “information that is false but not created with the intention of causing harm,” whereas disinformation is “information that is false and deliberately created to harm a person, social group, organisation, or country” often orchestrated with financial or political motives [5]. Both are prevalent across all social media platforms [6]. Together, these serve to undermine trust in governmental interventions, public health responses, expert guidance, and scientific facts about COVID-19 [7,8]. Accordingly, we define the COVID-19 infodemic as the overwhelming amount of complex and often contradictory information available about COVID-19, inclusive of substantial fake news about the origins of the virus, treatment options unsupported by rigorous clinical data, and baseless claims regarding adverse effects of lifesaving vaccines; these false narratives may be spread by authoritative institutions or influencers who are otherwise thought to be trustworthy, and they play a substantial role in shaping views and influencing human behaviors that can lead to poor health outcomes.

The clinical impact of the COVID-19 infodemic is profound. Effective strategies such as masking and social distancing have been undermined to the detriment of those at greatest risk. With several effective vaccines now available for SARS-CoV-2, vaccine hesitancy and vaccine refusal—two distinct problems with different causes and different solutions—have become major issues. Vaccine hesitancy is prolonged deliberation or delay in accepting vaccination, even when supply is ample; this differs from vaccine refusal, which is defined by the specific intent not to vaccinate, similar to the “anti-vax” movement adherents, in which people refuse all vaccines including childhood vaccinations. Both vaccine hesitancy and refusal are fueled by misinformation on social media, and vaccine misinformation that initially manifests offline can quickly spread to social media platforms; the misinformation exchange is bidirectional [9]. In fact, the US Surgeon General warned in 2021 that misinformation is the greatest threat to COVID-19 vaccination efforts [10]. COVID-19 misinformation and disinformation on social media increases vaccine hesitancy, lowers vaccination rates, and causes preventable deaths, especially among certain demographic populations [11,12]. The COVID-19 infodemic remains deadly, and we must act.

To address this, the Stanford University Ethics, Society, and Technology Hub and the Stanford Department of Emergency Medicine cosponsored INFODEMIC: A Stanford Conference on Social Media and COVID-19 Misinformation. INFODEMIC convened experts from the fields of social media, medicine, public health, and biomedical ethics with a goal of identifying new best practices to combat COVID-19 misinformation online [13]. The corresponding Journal of Medical Information Research theme issue, “Social Media, Ethics, and COVID-19 Misinformation” builds upon this work to discuss the impact of this infodemic and approaches to ending it. In this editorial, we will examine the role of social media companies (executives, financiers, leaders, and users) in health misinformation and their obligations to mitigate the COVID-19 infodemic.

#### Hundreds dead and injured because of COVID misinformation

Coleman, BBC monitoring journalist, 20

[Alistair, 8-12-20, BBC News, "'Hundreds dead' because of Covid-19 misinformation", [https://www.bbc.com/news/world-53755067](https://www.bbc.com/news/world-53755067https://www.bbc.com/news/world-53755067), accessed on 7-8-2022, MG]

At least 800 people may have died around the world because of coronavirus-related misinformation in the first three months of this year, researchers say.

A study published in the American Journal of Tropical Medicine and Hygiene also estimates that about 5,800 people were admitted to hospital as a result of false information on social media.

Many died from drinking methanol or alcohol-based cleaning products.

They wrongly believing the products to be a cure for the virus.

However, the actual figure may never been known, as data from Iran - where many of the supposed methanol poisoning deaths occurred - is difficult to verify.

The World Health Organization (WHO) has previously said that the "infodemic" surrounding Covid-19 spread just as quickly as the virus itself, with conspiracy theories, rumours and cultural stigma all contributing to deaths and injuries.

Many of the victims had followed advice resembling credible medical information - such as eating large amounts of garlic or ingesting large quantities of vitamins - as a way of preventing infection, the study's authors say. Others drank substances such as cow urine.

These actions all had "potentially serious implications" on their health, the researchers say.

The paper concludes that it is the responsibility of international agencies, governments and social media platforms to fight back against this "infodemic", but tech companies have been criticised for their slow and patchy response. In the UK, laws to regulate online harm might be several years away.

The BBC's own investigations found links to assaults, arson and deaths as a result of misinformation about the virus, and spoke to doctors, experts and victims about their experiences.

Online rumours led to mob attacks in India and mass poisonings in Iran. Telecommunications engineers have been threatened and attacked and phone masts have been set alight in the UK and other countries because of conspiracy theories that have been incubated and amplified online.

Social media also helps scammers to take advantage of the pandemic, selling ineffective badges that claim to ward off the virus, and urging followers to part with money in exchange for a "mineral miracle supplement", which is - in reality - diluted bleach.

As vaccines emerge, there is the further threat that anti-vaccine campaigners will use the platform provided by social media to persuade people not to protect themselves.

Despite social media companies removing or labelling misleading information about vaccines, recent polling in the United States showed that 28% of Americans believe that Bill Gates wants to use vaccines to implant microchips in people.

The achievement of an effective coronavirus vaccine could be completely undermined by misinformation, doctors told the BBC's anti-disinformation team.

### Impact – Nuke War, Climate, Civilization

#### Disinformation magnifies existing climate and nuclear impacts by removing potential safeguards and shatters the pillars of modern democratic government undermining civilization.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 2-3, accessed 7-8-2022) SS:/

The tweet depicted above obviously never happened. But given the ubiquity of social media today, it is interesting to consider what might have occurred if the Cuban Missile Crisis of 1962 had taken place in the global information environment of 2019.1

Nongovernmental open source intelligence organizations could have used commercial satellite imagery to detect the presence of these missiles and publicize them to the world on October 12, four days earlier than the president did. Pictures of Soviet missiles being deployed in Cuba might have found their way to social media, then going viral and alarming millions in the United States and around the world. Imagine that these images were accompanied by disinformation from internet trolls, tailored information leaks, and propaganda from adversaries, all seeking to cast doubt on the facts or to sow confusion among domestic populations and paralyze NATO leadership.

The shooting down of a U-2 spy plane over Cuba might have been news within an hour of its occurrence, soon accompanied by numerous tweets and relentless commentary on Facebook and other social media platforms, with some posts including realistic (though fake) video clips of what happened. When the Joint Chiefs of Staff recommendation to invade Cuba was overruled by President Kennedy, “alt” social media accounts that served as fronts for disgruntled Pentagon officials might have leaked the proposed invasion plan, hoping to induce the administration to reverse course on the chosen alternative, a blockade.

In the end, President Kennedy might not have had days to deliberate with the Executive Committee of the National Security Council before delivering a measured speech announcing to the world the discovery of Soviet medium- and intermediate-range nuclear-armed missiles in Cuba,2 but instead might have issued the tweet depicted above.

If the Cuban Missile Crisis, which many experts have characterized as the world’s closest approach to nuclear war, occurred today, the current global information ecosystem might very well have magnified the risk of war, escalating a high-stakes crisis into all-out nuclear exchange.3

The misuse of social media in the information environment has also made rational responses to the threat of climate change more difficult for national governments to reach, as companies and groups with financial and ideological interest in creating the appearance of doubt sow misinformation about consensus scientific view. That is, cyber-enabled information warfare is a threat multiplier in the climate change arena, just as it is in the nuclear policy area.

But corruption of the information ecosystem is not just a multiplier of two long acknowledged existential threats to the future of humanity—climate change and nuclear weapons. Cyber-enabled information warfare has also become an existential threat in its own right, its increased use posing the realistic possibility of a global information dystopia, in which the pillars of modern democratic self-government—logic, truth, and reality—are shattered, and anti-Enlightenment values undermine civilization around the world.

#### The impact is existential - Compromised information undermines Civilization, threatens Elections, Lives, and the Economy, and magnifies the likelihood of Nuclear War and Climate Change.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 3-5, accessed 7-8-2022) SS:/

Founded in 1945, the Bulletin first focused on the existential threat from nuclear war. The atomic scientists of the Manhattan Project did not believe that the miniature suns let loose on Hiroshima and Nagasaki in themselves posed an existential threat to human existence.4 But most of them recognized that they were omens of a future in which nuclear weapons, used on a large scale, could indeed threaten human existence, and even used on a smaller scale could threaten modern human civilization.

After sporadically reporting on climate change for decades, in 2007 the Bulletin formally expanded its concept of existential threat to include that and nuclear war.5 Where large-scale nuclear war threatens to snuff out hundreds of millions of lives in a matter of hours, climate change threatens to alter the planetary ecosystem. Here the effects are more subtle and less easily noticed because they are cumulative over decades. There is no single cataclysmic event in the offing, and yet myriad smaller regional disasters will result: more intense and more frequent forest fires, heat waves, and storms; vastly increased coastal flooding and rising sea levels; loss of arable land; severe shortages of food and water; and mass migrations and relocations.

Nuclear war and climate change threaten the physical infrastructure of human civilization as well as the underlying geochemical processes and the ecology of the planet. Because most people depend on both physical infrastructure and our global ecology for food, energy, and other necessities of existence, nuclear war and climate change put the lives of the great mass of humanity at risk. Because nuclear war and climate change threaten massive changes in cultural identity and the loss of historical resources, our civilization and our legacy are at stake, too. In those ways, both nuclear war and climate change pose existential threats to humanity. But these are not the only such threats to civilization as we know it.

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 environment)—in many ways has become central and often critical to the way people now live all over the world.

In the words of Yale Law School’s information scholar Jack Balkin, “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.”6 Consider that nations require good information to allocate benefits and social services to the populace; to administer mechanisms for public safety (e.g., law enforcement, 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 clients; 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 services; and to maintain their accounting and finances. Construction and manufacturing projects entail the coordination of dozens, hundreds, or thousands of parties—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 political candidates standing in elections; to know as consumers 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 effectively or efficiently; and in truly countless other ways.

Nations also engage extensively in information production. They provide education for young people; support 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 information 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 crippled, as they could and likely would make bad or at least suboptimal decisions about war and peace, the economy, law enforcement, housing, food production, energy, and the many other important matters for which governments have some responsibility.

#### Impact - Cyber-based disinformation makes solving for nuclear war and climate change impossible.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 10-11, accessed 7-8-2022) SS:/

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 cognitive limitations, the perpetrators of cyber-enabled information 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 election 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 cyberenabled information warfare. The problems of nuclear war and climate change are hard enough to solve even when well-intentioned, well-informed parties on all sides share a basic understanding and knowledge 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 holocaust or to make good decisions about nuclear weapons use in times of crisis? Without shared, fact-based understandings that rising atmospheric carbon dioxide concentrations caused by human beings result in corresponding increases in global temperature and climatic disruption, what hope is there for national leaders to reach agreements to begin serious efforts at decarbonizing their economies?

### Impact – Civilization

#### Unreliable information and information overload causes both legitimate and illegitimate actors to pressure leaders into rash escalatory responses.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 13, accessed 7-8-2022) SS:/

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.26 Central to this assumption is a rational adversary that can and does make a calculation of expected costs and benefits, compares 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, reflexive, heuristic System 1 thinking to make decisions, particularly when faced with time pressures, surprise and other obstacles to the deliberate calculation implied by System 2 thinking.27 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 instinctive 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.28 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 influential participants in one or another of them.

It is thus easy to posit that in this information environment, manipulated information— either artificially constructed or adopted by a strong grassroots base—could be used by interested parties to generate pressure on leaders to act. At the same time, leaders themselves are likely to be facing information overload and less able to distinguish analyzed information from their own intelligence sources and other, unvetted information originating from their constituencies.

#### Internal Link – Cyber-enabled information warfare replaces the pillars of logic, truth and, by exploiting our cognitive processes triggering widespread societal impacts.

Lin, Stanford University Center for International Security and Cooperation Senior Research Scholar, 19

(Herb Lin, Stanford University Center for International Security and Cooperation Cyber Policy and Security Senior Research Scholar and Hoover Institution Cyber policy and Security Hank J. Holland Fellow, ResearchGate, 7-1-2019, " The existential threat from cyber-enabled information warfare," Bulletin of the Atomic Scientists, Vol. 75, No. 4, p. 187-196 https://www.researchgate.net/publication/334089405\_The\_existential\_threat\_from\_cyber-enabled\_information\_warfare, p. 14-16, accessed 7-8-2022) SS:/

Nuclear war and climate change are arguably the most important existential challenges today that are compounded by the corruption of the information ecosystem. But even if a single miraculous stroke the laws of physics were changed to make nuclear weapons impossible to build and operate and to immediately eliminate anthropogenic emissions at zero cost, cyberenabled information warfare can still can lead to an information 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 reasonably 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 discredit political opponents (e.g., “showing” an opponent 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 information, 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 people choking amidst locally familiar locations (e.g., well-known fields or sport stadiums), cause spontaneous 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 provide 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 campaigns 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 clients, or take revenge on those who have harmed such children, all in anonymous and untraceable ways.

• Journalists, political leaders, and judges are compromised 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 comparable ones—will be the inevitable result if and when deployment and use of the tools of cyber-enabled information warfare become widespread. And even more troubling 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.

The Enlightenment established reason and reality as the foundational pillars of civilized discourse. In such discourse, logic matters, and a logical contradiction between statement 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, empirical 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 warfare, 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 information warfare campaigns in progress; good countermeasures 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 cyberenabled information warfare operations. All of this is easier said than done, however, as cyberenabled 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 fracture, the end of the Enlightenment, and the start of an informational Dark Age.

### Nuclear War Impacts

#### Must act to prevent nuclear war – impacts would be globally catastrophic

Sparks, New York Post, 7-8-22

[Hannah, 7-8-22, New York Post, “Nuclear war would create ‘dire’ worldwide hellscape: scientists”, <https://nypost.com/2022/07/08/nuclear-war-would-create-dire-worldwide-hellscape-scientists/>, accessed 7-9-22, AFB]

The threat of nuclear war goes well beyond the warfront.

Even far away from the terror seen by citizens and soldiers on the frontlines, Russia’s ongoing advancement into Ukraine has unsettled global economies as well as a sense of freedom and security abroad.

As it should, say scientists, who warn of the grave danger that the aftermath of nuclear war poses for the planet.

Just nine nations of the world are in control of more than 13,000 nuclear weapons, according to the Stockholm International Peace Research Institute. With that in mind, earth sciences and computational researchers aimed to better understand — so we can better prepare for — the dystopian landscape that could result from nuclear war.

Various computer simulations of nuclear firestorms saw a future with scarce sunlight, food and resources — globally.

As soot and smoke from the blasts fill the upper atmosphere, temperatures would plunge 13 degrees Fahrenheit in the first month — bigger than the drop that occurred during the last ice age.

With clouds blocking the Sun, crops would fail, while algae — the basis of the marine food chain — would disappear, thus halting major fisheries. Meanwhile, expanding ice coverage due to the cold shock — growing by more than 6 million square miles and 6 feet deep — would block major ports from receiving shipments of food and other goods across seas, from Shanghai to Copenhagen.

“It doesn’t matter who is bombing whom. It can be India and Pakistan or NATO and Russia. Once the smoke is released into the upper atmosphere, it spreads globally and affects everyone,” said Cheryl Harrison, an assistant professor at Louisiana State University, in a statement on behalf of a team of international researchers. Their work was published on Thursday in the journal Earth and space sciences journal AGU Advances, a Wiley publication.

Their simulations examined outcomes following drops of 4,400 100-kiloton nuclear weapons between the US and Russia, which would release more than 330 billion pounds of smoke and sunlight-absorbing black carbon into the upper atmosphere — or if 500 bombs weighing 100 kilotons each were detonated between India and Pakistan, which would see somewhere between 11 billion to 103 billion pounds of ash and smog ejected. (For comparison, the bombs that hit Nagasaki and Hiroshima in 1945 were 21 and 15 kilotons, respectively.)

It’s critical for world leaders to consider their findings, said study co-author Alan Robock, a professor in the Department of Environmental Sciences at Rutgers University.

“Nuclear warfare results in dire consequences for everyone. World leaders have used our studies previously as an impetus to end the nuclear arms race in the 1980s, and five years ago to pass a treaty in the United Nations to ban nuclear weapons,” Robock said. “We hope that this new study will encourage more nations to ratify the ban treaty.”

Current global affairs should be a wake-up call, added Harrison.

“The current war in Ukraine with Russia and how it has affected gas prices, really shows us how fragile our global economy and our supply chains are to what may seem like regional conflicts and perturbations,” she said.

Their models are not unlike what happens during massive volcanic eruptions, researchers noted.

“We can avoid nuclear war, but volcanic eruptions are definitely going to happen again. There’s nothing we can do about it, so it’s important when we’re talking about resilience and how to design our society that we consider what we need to do to prepare for unavoidable climate shocks,” Harrison said. “We can and must, however, do everything we can to avoid nuclear war. The effects are too likely to be globally catastrophic.”

#### Nuclear war would have catastrophic environmental and food security impacts – simulations prove

Harrison et al., Louisiana State Department of Ocean and Coastal Science professor, 22

[Cheryl S., Tyler Rohr (Australian Antarctic Partnership Program), Alice DuVivier (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Elizabeth A. Maroon (University of Wisconsin–Madison Department of Atmospheric and Oceanic Sciences), Scott Bachman (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Charles G. Bardeen (National Center for Atmospheric Research Atmospheric Chemistry Observations and Modeling Laboratory), Joshua Coupe (Rutgers University Department of Environmental Sciences), Victoria Garza (Louisiana State Department of Ocean and Coastal Science), Ryan Heneghan (Queensland University of Technology School of Mathematical Sciences), Nicole S. Lovenduski (University of Colorado Boulder Department of Atmospheric and Oceanic Sciences, & Institute of Arctic and Alpine Research), Philipp Neubauer (Dragonfly Data Science), Victor Rangel (Texas A&M University Aerospace Engineering Department), Alan Robock (Rutgers University Department of Environmental Sciences), Kim Scherrer (University of Bergen Department of Biological Sciences, & UC Santa Barbara Bren School of Environmental Science and Management), Samantha Stevenson (UC Santa Barbara Bren School of Environmental Science and Management), & Owen B. Toon (University of Colorado Boulder Laboratory for Atmospheric and Space Physics & Department of Atmospheric and Oceanic Sciences), August 2022, AGU Advances, Volume 3, Issue 4, “A New Ocean State After Nuclear War,” <https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2021AV000610>, p. 2-3, accessed 7-9-22, AFB]

There are more than 13,000 nuclear weapons in the world controlled by nine nations (SPIRI, 2020). States with nuclear weapons, including the United States, Russia, China, India, and Pakistan, have recently embarked on plans to modernize or expand their nuclear arsenals, while North Korea has developed, and Iran is at risk of devel-oping new nuclear weapons capabilities (SPIRI, 2020). The presence of these weapons creates a risk that they will be launched intentionally or by mistake, by unstable leaders, hackers, or computer failure (Ellsberg, 2017; Perry & Collina, 2020). In addition to the devastating loss of human life (Robock et al., 2019; Toon et al., 2019), it is important to quantify the expected collateral damage to the Earth system and all its inhabitants of such a nuclear crisis. Here, we examine the hysteresis response of the ocean to global cooling events driven by the deto-nation of nuclear warheads.

Hysteresis is the property of a system that has a response that “lags behind” the forcing variable, meaning that the system depends on the history of the forcing (e.g., Visintin, 2013), either resulting in a new state when forcing is removed (irreversible or rate-independent hysteresis), or slowly returns to the initial state (dynamic or rate-dependent hysteresis). In Earth system science, hysteresis has been discussed in reference to the global ocean overturning circulation (Kageyama et al., 2010; Rahmstorf, 1995) and the Antarctic ice sheet (Garbe et al., 2020; Pollard & DeConto, 2005), which both have multiple steady states depending on the forcing history. Other stud-ies have defined rate-dependent hysteresis as not returning to the unperturbed state within a time frame relevant for humans or other organisms (Jeltsch-Thömmes et al., 2020), as in the asymmetry of the climate response to increasing then decreasing CO2, a temporal lag largely caused by the slow adjustment timescales of the ocean physical and biogeochemical state (Hofmann et al., 2019; Jeltsch-Thömmes et al., 2020; Steffen et al., 2018; Yang & Zhu, 2011). Both irreversible and dynamic hysteresis occur in terrestrial (Drüke et al., 2021) and marine ecosystems under climate disturbances, where they are often termed regime shifts, sometimes due to “tipping points” in the system response to forcing (Brierley & Kingsford, 2009; Cooper et al., 2020; Cowan et al., 2008; deYoung et al., 2008; Drüke et al., 2021). Here, we investigate the hysteresis of the ocean physical, biogeochem-ical, and lower trophic level ecosystem response to nuclear cooling events.

In the Earth's past, abrupt global cooling driven by volcanic eruptions has triggered atmospheric perturbations that persist for several decades to hundreds of years or longer (Otto-Bliesner et al., 2015; Sigl et al., 2015), with recorded impacts on human civilization including massive famine and fall of empires (Oppenheimer, 2011; White, 2011). Despite the ocean's large role in climate (Rahmstorf, 2002; Sarmiento & Gruber, 2006) and food security (FAO, 2018; Kent, 1997), the global ocean impacts of these cooling events, and in particular the ocean biogeochemical and ecosystem response, remain poorly understood. Like volcanic eruptions (Robock, 2000) and large forest fires (Khaykin et al., 2020; Peterson et al., 2021; Yu et al., 2019, 2021), urban firestorms generated during nuclear war using modern arsenals are expected to loft particles into the upper troposphere and lower strat-osphere. However, the smoke would have at least a three times longer residence time than volcanic aerosols, lead-ing to more extended radiation anomalies (Coupe et al., 2019; Mills et al., 2008, 2014; Otto-Bliesner et al., 2015; Robock et al., 2007; Sigl et al., 2015; Toon et al., 2019). This long atmospheric residence time of soot is due to its ability to self-loft to high altitude due to solar heating, as observed in recent forest fires (Khaykin et al., 2020; Peterson et al., 2021; Yu et al., 2019).

In recent work (Toon et al., 2019), we simulated a series of nuclear conflicts between India and Pakistan of vary-ing sizes and impacts on global climate and compared them to a larger war between the US and Russia (Coupe et al., 2019; Robock et al., 2007). As with volcanic-driven events, the reduction of sunlight after nuclear war would lead to global cooling, in turn driving a wide range of global changes, altering the living conditions on Earth. Examples include decreased agricultural and fisheries productivity, with large implications for global food security (Jägermeyr et al., 2020; Scherrer et al., 2020; Toon et al., 2019; Xia et al., 2015); increased surface ocean pH and decreased aragonite saturation (Lovenduski et al., 2020); a 7 year El Niño like event (Coupe et al., 2021); reduced ozone and increased UV radiation at the surface (Bardeen et al., 2021; Mills et al., 2008) and temporary expansion of sea ice (Mills et al., 2014). In simulations, global ocean surface cooling penetrated to depth over decades, indicating the potential for long-term impacts from relatively small global cooling events on the physical ocean state (Mills et al., 2014). Further, in the largest war scenario between the US and Russia, we found that after an initial decline in marine net primary production (NPP), NPP eventually became significantly elevated above pre-war levels long after the solar radi returned to normal. These findings suggest that the extreme cooling caused by a nuclear war might have the ability to trigger changes in the ocean system that persist well beyond the initial perturbation.

#### Nuclear war would collapse global ecosystems – especially oceans

Harrison et al., Louisiana State Department of Ocean and Coastal Science professor, 22

[Cheryl S., Tyler Rohr (Australian Antarctic Partnership Program), Alice DuVivier (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Elizabeth A. Maroon (University of Wisconsin–Madison Department of Atmospheric and Oceanic Sciences), Scott Bachman (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Charles G. Bardeen (National Center for Atmospheric Research Atmospheric Chemistry Observations and Modeling Laboratory), Joshua Coupe (Rutgers University Department of Environmental Sciences), Victoria Garza (Louisiana State Department of Ocean and Coastal Science), Ryan Heneghan (Queensland University of Technology School of Mathematical Sciences), Nicole S. Lovenduski (University of Colorado Boulder Department of Atmospheric and Oceanic Sciences, & Institute of Arctic and Alpine Research), Philipp Neubauer (Dragonfly Data Science), Victor Rangel (Texas A&M University Aerospace Engineering Department), Alan Robock (Rutgers University Department of Environmental Sciences), Kim Scherrer (University of Bergen Department of Biological Sciences, & UC Santa Barbara Bren School of Environmental Science and Management), Samantha Stevenson (UC Santa Barbara Bren School of Environmental Science and Management), & Owen B. Toon (University of Colorado Boulder Laboratory for Atmospheric and Space Physics & Department of Atmospheric and Oceanic Sciences), August 2022, AGU Advances, Volume 3, Issue 4, “A New Ocean State After Nuclear War,” <https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2021AV000610>, p. 1, accessed 7-9-22, AFB]

Abstract Nuclear war would produce dire global consequences for humans and our environment. We simulated climate impacts of US-Russia and India-Pakistan nuclear wars in an Earth System Model, here, we report on the ocean impacts. Like volcanic eruptions and large forest fires, firestorms from nuclear war would transport light-blocking aerosols to the stratosphere, resulting in global cooling. The ocean responds over two timescales: a rapid cooling event and a long recovery, indicating a hysteresis response of the ocean to global cooling. Surface cooling drives sea ice expansion, enhanced meridional overturning, and intensified ocean vertical mixing that is expanded, deeper, and longer lasting. Phytoplankton production and community structure are highly modified by perturbations to light, temperature, and nutrients, resulting in initial decimation of production, especially at high latitudes. A new physical and biogeochemical ocean state results, characterized by shallower pycnoclines, thermoclines, and nutriclines, ventilated deep water masses, and thicker Arctic sea ice. Persistent changes in nutrient limitation drive a shift in phytoplankton community structure, resulting in increased diatom populations, which in turn increase iron scavenging and iron limitation, especially at high latitudes. In the largest US-Russia scenario (150 Tg), ocean recovery is likely on the order of decades at the surface and hundreds of years at depth, while changes to Arctic sea-ice will likely last thousands of years, effectively a “Nuclear Little Ice Age.” Marine ecosystems would be highly disrupted by both the initial perturbation and in the new ocean state, resulting in long-term, global impacts to ecosystem services such as fisheries.

#### Nuclear war would have catastrophic impacts on ecosystems across the globe

Harrison et al., Louisiana State Department of Ocean and Coastal Science professor, 22

[Cheryl S., Tyler Rohr (Australian Antarctic Partnership Program), Alice DuVivier (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Elizabeth A. Maroon (University of Wisconsin–Madison Department of Atmospheric and Oceanic Sciences), Scott Bachman (National Center for Atmospheric Research Climate and Global Dynamics Laboratory), Charles G. Bardeen (National Center for Atmospheric Research Atmospheric Chemistry Observations and Modeling Laboratory), Joshua Coupe (Rutgers University Department of Environmental Sciences), Victoria Garza (Louisiana State Department of Ocean and Coastal Science), Ryan Heneghan (Queensland University of Technology School of Mathematical Sciences), Nicole S. Lovenduski (University of Colorado Boulder Department of Atmospheric and Oceanic Sciences, & Institute of Arctic and Alpine Research), Philipp Neubauer (Dragonfly Data Science), Victor Rangel (Texas A&M University Aerospace Engineering Department), Alan Robock (Rutgers University Department of Environmental Sciences), Kim Scherrer (University of Bergen Department of Biological Sciences, & UC Santa Barbara Bren School of Environmental Science and Management), Samantha Stevenson (UC Santa Barbara Bren School of Environmental Science and Management), & Owen B. Toon (University of Colorado Boulder Laboratory for Atmospheric and Space Physics & Department of Atmospheric and Oceanic Sciences), August 2022, AGU Advances, Volume 3, Issue 4, “A New Ocean State After Nuclear War,” <https://agupubs.onlinelibrary.wiley.com/doi/10.1029/2021AV000610>, p. 1, accessed 7-9-22, AFB]

Plain Language Summary If nuclear arsenals were used accidentally or intentionally, they would produce dire consequences for all life on Earth. We simulated climate impacts of nuclear wars in a global Earth system model, focusing on marine impacts. We simulated a US-Russia war and several India-Pakistan wars. In all scenarios, firestorms from nuclear war would deliver soot to the upper atmosphere, blocking out the sun and causing global cooling. Impacts of the nuclear cooling event include expansion of sea ice into populated coastal areas and decimation of ocean marine life. In all scenarios, the ocean cools rapidly but does not return to the pre-war state when the smoke clears. Instead, the ocean takes many decades to return to normal, and some parts of the ocean would likely stay in the new state for hundreds of years or longer. When the cooling event ends, Arctic sea ice is left in a new state, a sort of “Nuclear Little Ice Age.” Marine ecosystems would be highly disrupted by both the initial perturbation and the resulting new ocean state, resulting in impacts to ecosystem services worldwide, lasting for decades. This study underscores the danger of nuclear war and the long-term impacts to humans and our environment.

### AT – No One Fooled by Disinfo

#### Deep fakes have a lot of potential, several mayors were tricked in a call with a deepfake Kyiv mayor

Associated Press, 22

(Associated Press “European mayors duped into calls with fake Kyiv mayor,” 4-29-2022, https://www.cnbc.com/2022/06/25/european-mayors-duped-into-calls-with-fake-kyiv-mayor.html, accessed 7-1-2022) jh

The mayor of the Ukrainian capital of Kyiv warned Saturday that an imposter is posing as him and communicating with other officials, including three European mayors who were duped into believing they were having a video call with the real Vitali Klitschko.

“Several mayors in Europe have been contacted by a fake mayor of Kyiv who has been saying absurd things,” Klitschko told German daily newspaper Bild. “This is criminal energy. It must be urgently investigated who is behind it.”

The office of Berlin Mayor Franziska Giffey tweeted Friday night that she cut short a call with the reputed Kyiv mayor after his comments and questions made her suspicious. “The course of the conversation and the setting of topics” made Giffey wary, her office said without elaborating.

The office published a photo that showed both the German capital’s mayor and the fake Klitschko on a big screen. It said that initially, “there was no evidence that the video conference was not conducted with a real person. To all appearances, it is deep fake.”

Police were investigating the incident, Giffey’s office said.

Madrid Mayor José Luis Martínez-Almeida also interrupted a video call with someone claiming to be Klitschko on Friday. The mayor of Spain’s capital suspected he wasn’t speaking with his Kyiv counterpart and has filed a complaint with police.

Vienna Mayor Michael Ludwig did not end his call with the imposter earlier this week because he didn’t notice any suspicious behavior, Austrian public broadcaster ORF reported.

“Since no tricky topics were discussed in the conversation, this is certainly annoying in the specific occasion but not a big problem,” Ludwig said.

It was not clear who was behind the calls or what means were used to try to make the mayors think they were communicating with Klitschko.

On Saturday, Berlin’s mayor said her encounter with the fraudster means that “in the future, we will have to be even more scrutinizing, even more suspicious.”

She called the use of a phony Klitschko “a means of modern warfare,” referring to Russia’s four-month war on Ukraine.

Kyiv’s actual mayor also made a link to Russia’s war in Ukraine.

“Friends! The enemy does not let up and is waging war on all fronts - in particular by disinformation, by discrediting Ukrainian politicians,” Klitschko said in a post on the Telegram messaging app. “In order to quarrel with European partners, so that Ukraine would not be helped.”

In his remarks to Bild, he warned other European officials to be careful if they are contacted by someone claiming to represent his office. “Please be careful in the future how appointments are arranged by me. Official conversations only come through official channels,” he said.

### AT – No One Fooled by Russian Disinfo

#### Disinformation has lasting impact – Russia HIV propaganda proves

Poster, State Department historian, 18

(Alexander, Office of the Historian, Predoctoral Fellow at Yale, PHD and MA at The Ohio State University, BA at University of Michigan, 3-12-18, Washington Post, “The Russian ‘fake news’ campaign that damaged the United States — in the 1980s”, https://www.washingtonpost.com/news/made-by-history/wp/2018/03/12/the-russian-fake-news-campaign-that-damaged-the-united-states-in-the-1980s/, accessed 7-6-2022) jiu

Imagine a covert plan to weaken the United States, not through military sabotage or stealing state secrets, but simply through the manipulation of the news media. The plan involves foreign agents who write and disseminate false news articles with the aim of destabilizing American society and driving a wedge between the United States and its allies.

No, this isn’t a story about the 2016 election, but rather about how the Soviet Union capitalized on perceived American indifference toward the AIDS epidemic in the 1980s and began disseminating “fake news” as part of a disinformation campaign that had major ramifications for American foreign policy — and may well still be influencing Russian-American relations .

To be fair, the Reagan administration was slow to act when it came to HIV/AIDS. In a news conference on Oct. 15, 1982, journalist Lester Kinsolving [asked](https://www.youtube.com/watch?v=yAzDn7tE1lU) White House press secretary Larry Speakes whether President Ronald Reagan had any reaction given that “AIDS is now an epidemic.” Speakes provided a terrifyingly ignorant response: “What’s AIDS?”

When Kinsolving tried to explain the nature of the illness, noting that it was informally known as the “gay plague,” Speakes responded in jest, saying, “I don’t have it. Do you?” The fact that the Centers for Disease Control and Prevention had been reporting on AIDS for more than a year apparently was not known in the White House. “There has been no personal experience here,” Speakes concluded.

The spread of AIDS within the United States and the negligence of the Reagan administration provided the Soviets with an opportunity at a moment when Cold War tensions were high. Noting that many Americans were distrustful of their government after the Vietnam War, and observing that HIV/AIDS was more prevalent in groups that were critical of Reagan’s policies, the Soviets decided that beginning a disinformation campaign about the origins of the disease could sow dissent within the nation and among U.S. allies.

Historian Thomas Boghardt said the campaign started on July 17, 1983, when a newspaper in India, the Patriot, published an anonymous letter from an “American scientist.” The scientist claimed that AIDS was an American biological weapon created at Fort Detrick, Md. A former Soviet bloc intelligence officer who corresponded with Boghardt noted that the disinformation campaign “virtually conceptualized itself” because of the controversy about AIDS within the United States.

The Patriot had a circulation of only 35,000, so the placement of the anonymous letter did not create the panic that Soviet agents had hoped for, but persistence paid off. Throughout the next three years, embassies across the world reported on newspaper articles that accused the United States of creating AIDS as a biological weapon. In November 1985, embassy officials in Nicaragua [noted](https://history.state.gov/historicaldocuments/frus1981-88v41/d9) that pro-Sandinista publications were participating in the disinformation campaign and had run stories that Americans had tested AIDS on Haitians as well as “certain groups in North America.”

As HIV/AIDS spread rapidly in Africa, U.S. embassies complained to the State Department that the Soviets had blanketed the continent with disinformation. By 1986, newspapers in Nairobi; Lagos, Nigeria and Dakar, Senegal, had run stories that claimed that Americans had created the AIDS virus, that blood supplies from the United States were contaminated and [that](https://history.state.gov/historicaldocuments/frus1981-88v41/d19) “the citation of Africa as the disease’s point of origin is some sort of Western conspiracy.”

Because up to one-third of urban-dwelling adults in Central and East Africa were infected by 1987, these articles generated reasonable consternation among African leaders. The State Department sent a telegram to all African diplomatic posts in August 1986 with talking points that rebutted these allegations and emphasized that blood originating from the United States was not infected.

The department sent a similar telegram to all of its diplomatic posts worldwide in December 1986 as disinformation continued to spread. The telegram asked posts to [suggest](https://history.state.gov/historicaldocuments/frus1981-88v41/d21) means of “developing a counter strategy” as disinformation had become global and pernicious, and American officials seemed powerless to stop it.

By 1987, the narrative that Americans were carriers, if not creators, of a dangerous disease had taken hold to such an extent that officials in the Philippines expressed concern about U.S. servicemen at military bases in their nation. Central to their distress was the notion that Americans were spreading HIV/AIDS in the Philippines and that the epidemic “[was](https://history.state.gov/historicaldocuments/frus1981-88v41/d32) not merely a public health problem” but a social problem, with Americans identified as agents of contagion. This conception posed political problems: The Filipino government proceeded to demand more funding for an anti-AIDS campaign from the United States as a result.

Despite the success of their disinformation campaign, the Soviet leaders began to change course in 1987, the same year they first acknowledged publicly that AIDS had spread to their nation. In a July 1987 meeting with Assistant Secretary of State for African Affairs Chet Crocker, Soviet Deputy Foreign Minister Anatoly Adamishin admitted privately that the Soviets had “only begun to understand the magnitude of the AIDS problem” and [stated](https://history.state.gov/historicaldocuments/frus1981-88v41/d30) that he had “no difficulty” in admitting elements of the Soviet disinformation campaign were “foolish.”

In a meeting at the Soviet Embassy, State Department officials remarked that they welcomed newfound Soviet efforts to combat AIDS, but urged the Soviets to cease their “[blatantly false allegations first](https://history.state.gov/historicaldocuments/frus1981-88v41/d23).”

As a result of the changing Soviet posture, American policymakers were finally able to limit the damage of the Soviet disinformation campaign — but only because the Soviets sought to trade the campaign for scientific collaboration — a testament to how effective “fake news” can be.

In the years that followed, presidential administrations proved more responsive to the AIDS epidemic. President George W. Bush’s PEPFAR initiative targeted AIDS in Africa and has since provided antiretroviral treatment to 7.7 million people and saved about 11 million lives.

Despite the American commitment to address the HIV/AIDS epidemic, conspiracy theories remain. A quick search on the Internet will reveal numerous websites that assert that AIDS was, in fact, a biological weapon created at Fort Detrick. Although the Soviet Union no longer exists, its propaganda remains, as people worldwide — including Americans — still believe elements of its disinformation campaign about AIDS more than 30 years after it began.

One person who does not need to be convinced about the effectiveness of a disinformation campaign is Russian President Vladimir Putin, who was a member of the KGB from 1975 to 1990, and was able to see firsthand the outbreak of the AIDS epidemic as well as Soviet efforts to indict the United States. Americans may never know for certain whether the success of the AIDS disinformation campaign has influenced Putin’s foreign policy, but at the very least, it is worth considering. And it is a reminder of the lasting effects disinformation campaigns can have, particularly when they play off existing divisions in the United States.

### AT – NATO engages in Disinfo

#### Absent deterrence mechanisms the information battlefield is anarchic and inevitable - preemptive strikes are necessary.

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 8-9, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

The core puzzle of disinformation is therefore that although it has short-term strategic advantages, it has more significant reputational and communicative costs to the Attacker in the medium-to-long term, yet Attackers nonetheless rely on disinformation knowing that they will suffer from these costs. To that end, the focus of this chapter is this ex-post inefficiency of disinformation: why do countries engage in disinformation even though they know that their ex-ante gains from it often dwarf in contrast to their ex-post reputational costs? In Fearonian fashion, an IR-Realist explanation of disinformation would fit into three broad categories: anarchy, preventive action and positive expected utility.33 In terms of anarchy, the absence of a deterrence mechanism or a supranational authority creates an international disinformation environment that favours the Attacker. Similar to cybersecurity debates where the Attacker has a distinct advantage due to attribution problems and mediocre chance of reprisals,34 disinformation too, is a domain where the Attacker has a distinct timing and first-mover’s advantage against the Defender. Quite often, a successful disinformation campaign generates substantial shortterm benefit around important time-sensitive events, even if such campaigns are debunked and a counter disinformation offensive begins. To that end, the world of global disinformation is a significantly anarchic domain.

In a system dominated by anarchy and first-mover advantages, preventative action becomes the norm. Attacker in an information war finds initiating a campaign more preferable if it perceives that information war unavoidable. Since the disinformation domain is anarchic and information war is perceived as inevitable, a government will find the payoff of initiating a campaign greater than the risk of not initiating, in order not to suffer from the penalties of becoming a Defender by moving in late. To that end preemption becomes a form of prevention: not of the information war, but of the costs of suffering from the initial salvo.

## Democracy

### Disinformation Undermines Trust

#### Disinformation undermines trust in government – it is the greatest threat to liberal democracies

**Boudreau, Veritas Strategic Communications Principal Consultant, 22**

[Brett, 2022, Canadian Global Affairs Institute,The Rise and Fall of Military Strategic Communications at National Defence 2015-2021: A Cautionary Tale for Canada and NATO, and a Roadmap for Reform, Retrieved from <https://policycommons.net/artifacts/2460847/the-rise-and-fall-of-military-strategic-communications-at-national-defence-2015-2021/> on 01 Jul 2022. CID: 20.500.12592/527c47. HC)

Executive Summary

On November 2, 2020, the Ottawa Citizen ran the front-page headline “Canadian Military Wants to Establish New Organization to Use Propaganda and Other Techniques to Influence Canadians.” This seemed an unbelievable story, and one initially denied by a spokesperson for the minister of National Defense. Just three days later, though, then-chief of the Defense Staff (CDS) Gen. Jonathan Vance shuttered the group in question, terminating an initiative more than five years in the making that called into question the Department of National Defense’s (DND) commitment to objective and appropriate public communication, at a time when truth decay, misinformation and disinformation have gained much traction around the world and in Canada. In June 2021, the day Parliament adjourned for the summer, DND acknowledged to select media that acting CDS Lt.-Gen. Wayne Eyre and then-deputy minister Jody Thomas had determined the initiative was “incompatible” with government communications policy and the vision, mission and principles of DND Public Affairs. In a surprising self-indictment, the leaders also admitted a lack of “institution-wide strategic level direction and guidance,” to build information-related capabilities that were “governed by appropriate authorities and oversight.” Deliberate influence campaigns by malign state, non-state and increasingly by domestic actors to disturb, disrupt and create disorder in democratic societies have become widespread and commonplace. The volume of vitriol is increasing. This is fast eroding citizen faith, trust and confidence in government and public institutions and may be the greatest contemporary threat liberal democracies face – arresting this trend and then restoring trust, the ultimate challenge. National Defense’s entire program – to be successful on operations; secure sufficient funding; recruit, train and retain; effect culture change; reconstitute the force post-pandemic and procure the equipment needed to contest, confront and defeat adversaries – will largely depend on whether the institution can modernize its approach to strategic communications to maneuver more agilely and to better effect in a complex, frenetic and hostile information environment. Recently, National Defense has suffered a significant self-inflicted setback in that regard.

### Disinformation Undermines Democratic Values

#### Russian disinformation undermines essential values of democracy in the U.S. as partisan divides grow

Gu, Universal Rights Group NYC Research Analyst 21 - [Amanda, 3-16-2021, Universal Rights Group, "Recent US report of Russian election interference reveals how disinformation can exploit existing divides to erode trust in democracy,", https://www.universal-rights.org/universal-rights-group-nyc-2/recent-us-report-of-russian-election-interference-reveals-how-disinformation-can-exploit-existing-divides-to-erode-trust-in-democracy/, Accessed 7-6-2022, LASA-LR]

The effectiveness of these disinformation campaigns can be attributed to the pre-existing partisan divides and growing distrust in expertise in the US, which have only worsened after these attacks. According to the report, Russia’s Internet Research Agency (IRA) used its familiarity with US history, culture, and politics to exploit existing political divisions by targeting individuals who feel strongly about social issues ranging from racial and religious to party political, to ‘issue political’ such as feminist culture, gun rights, and trust in media. Disinformation campaigns were then used to activate or demobilise individuals who consider an issue personally important, creating an ‘us’ vs. ‘them’ discourse.

Disinformation tactics have become significantly more widespread and sophisticated as these online campaigns have come to rely on an assortment of bots, propaganda producers, and fake news outlets to exploit social media algorithms in order to propagate their message and ensure that it is seamlessly integrated with trusted content. These often rely on pre-existing paths of microtargeting created by advertisers and political campaigners through the use and abuse of personal data. Social media is presently an indispensable part of modern political campaigning, and there is a strong incentive for political campaigns to rely on microtargeting techniques to reach constituents. And because this targeted messaging only reaches select audiences, they are likely to bypass journalistic scrutiny and deliver disinformation to individuals unchallenged. Quantity is valued over quality, as the disinformation strategy relies on sheer mass to drown out real news.

Politicians are becoming increasingly reliant on social media to win elections, and often use the same microtargeting techniques allegedly used by Russia – feeding fear and playing off partisan divides – in order to mudsling their way to victory. Disinformation tactics have also benefited from the fact that those at the top in the US peddled outlandish theories to their constituents, normalising and facilitating the spread of fake news. Take for example the issues of mail-in voting or election illegitimacy that were pushed by Trump himself; Russian bots did not have to create new rhetoric, but only had to spread pre-existing content.

These attacks on voters’ rights to information and faith in the electoral system have worsened the existing partisan divide in America. The world of ‘alternative facts’ produced by online disinformation have created what appears to be two different realities for the two American parties, a dangerous position that puts political compromise, and hence the functioning of democracy, at risk.

Dangers to democracy

Disinformation campaigns are especially dangerous to democracies because a well-informed electorate is a prerequisite to a stable democracy. When information becomes manipulated, it damages citizens’ ability to choose their leaders based on factual news and authentic debate. This right to information is essential for voters who need to assess the performance of an elected official and exercise their democratic rights effectively, such as through timely protests.

Disinformation campaigns like the ones presented in the ICA report, are not only able to manipulate the vital information individuals rely on to participate in a democracy, but also can undermine the integrity of the electoral system itself. Unsubstantiated claims of voter fraud or a stolen election propagates a fatalistic view that the individual vote is powerless, discourages democratic participation, and breeds a culture of mistrust. When the right to information is hindered, this begins to chip away at public trust, eventually causing the foundations of democracy to buckle.

### Democracy Good – Prevents Conflict

#### The survival of democracy is key to maintaining peace

Lmai, Harvard Political Science Professor & Lo, University of Southern California Political Science Professor, 21

[Kosuke Imai and James Lo, 7-29-21, ,Harvard University, Page 16, <https://imai.fas.harvard.edu/research/files/dempeace.pdf>, p/. 916 Accessed 7-8-2022, LASA-LR]

In this research note, we apply a nonparametric sensitivity analysis to the democratic peace debate in international relations. We find that the positive association between democracy and peace is at least five times as robust as that between smoking and lung cancer. To explain away the democratic peace, researchers would have to find confounders that are many times more strongly associated with democracy and conflicts than the confounders that have been identified until now. Since such confounders have yet to be found, for now we conclude that the existing empirical evidence overwhelmingly supports the democratic peace.

#### Democracies are less likely to engage in conflict

Reiter, Harvard National Security post-doctoral fellow, 17

[Dan, 1-25-2017, Oxford Research Encyclopedia of Politics, "Is Democracy a Cause of Peace?,", https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-287#acrefore-9780190228637-e-287-div1-2, 7-2-2022, LASA-LR]

Though democracies sometimes become embroiled in conflicts with non-democracies, they almost never fight each other (Russett & Oneal, 2001). Since the emergence of modern democracy in the early 19th century, two mature democracies have never experienced intense violent conflict with each other, incurring at least 1,000 battle dead. The Correlates of War project and other data sets have long classified a conflict as a war if it experiences at least 1,000 battle dead (Reiter et al., 2016). On the rare occasions when two democracies have entered militarized disputes with each other, as in the 1898 Fashoda Crisis or the 1970s “Cod Wars” between Britain and Iceland, they essentially always settle the conflict short of war.

There have been close calls of democracies nearly fighting wars against each other. Mature democracies have sometimes fought repressive states with some democratic elements, such as the United States fighting Spain in the 1898 Spanish-American War (Ray, 1995). Democracies sometimes end up as members of opposing coalitions, though in those cases the opposing democracies avoid fighting each other. Democratic Finland fought alongside the Axis in World War II, but experienced no combat with any democratic members of the Allies. In the 1948 War of Israeli Independence, a somewhat democratic Lebanon found itself allied with Arab states against the new Israeli democracy, but Lebanon carefully avoided direct clashes with Israel (Morris, 2008, pp. 344, 348). In the 2006 Israel-Hezbollah conflict, though Israel launched strikes against Hezbollah forces based in Lebanese territory, Israel did not declare war on democratic Lebanon and generally avoided attacking Lebanese forces directly. Lebanon also mostly avoided attacking Israel forces. Probably the closest instance of two democracies going to war with each other was the 1999 Kargil War between India and Pakistan, though that conflict experienced less than 1,000 battle dead (Reiter et al., 2016). More systematic studies have also found that pairs of democratic states are less likely to experience less intense violent, international conflicts than other pairs of states (Russett & Oneal, 2001; Rousseau et al., 1996), though there is debate over whether jointly democratic pairs of states are less likely to experience non-war disputes as compared with all other pairs of states, or just with pairs of states that include a democracy and a non-democracy (Bennett & Stam, 2004).

Though there is strong consensus about the “dyadic” democratic peace, that democracies do not fight each other, there is more debate about the existence of other possible patterns of democratic peace. Many dispute the existence of the “monadic” democratic peace, that democracies are more likely to be peaceful in their relations with all states (Russett & Oneal, 2001; for an early statement of the monadic democratic peace, see Rummel, 1979). There is also debate over the existence of a “systemic” democratic peace, whether making the international system or even a region more democratic will make the system or region more peaceful (Gleditsch, 2002; Mitchell et al., 1999).

### Russia-China Spreading Authoritarianism

#### Russian and Chinese disinformation operations are converging to undermine liberal democratic order

Kendall-Taylor, New American Security Transatlantic Security Program fellow & Shullman, International Republican Institute senior advisor, 20

[Andrea Kendall-Taylor and David Shullman, 5-26-20, National Forum For Democratic Studies, "Converging Chinese and Russian Disinformation Compounds Threat to Democracy", <https://www.power3point0.org/2020/05/26/converging-chinese-and-russian-disinformation-compounds-threat-to-democracy/>, accessed on 7-9-2022, MG]

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.

#### China and Russia cyber-attacks are not mutually exclusive, and both undermine democracies that have previously sustained peace throughout Europe

Janda, Czechia Chamber of Disputes Member, 20

[Jakub, 6-17-2020, Just Security, "Beware a China-Russia Nexus in Central Europe Amid US-EU Neglect,", https://www.justsecurity.org/70822/beware-a-china-russia-nexus-in-central-europe-amid-us-eu-neglect/, 7-2-2022, LASA-LR]

Until recently, Russian and Chinese influence across Europe generally reflected their distinct strategic aims. But their interests increasingly converge. Common to both Vladimir Putin’s and Xi Jinping’s strategies is the decoupling of the United States and Europe. Leaders on both sides of the Atlantic will have to act in concert – and fast – to forestall an even greater corrosion of the democratic norms that have kept the peace – or helped restore it, in the case of the wars in the former Yugoslavia – for three-quarters of a century.

Russia and China have made particular inroads in Central and Southeastern Europe in recent years. Putin’s government identifies dissatisfied segments of the public and the political class and maliciously exploits vulnerabilities via disinformation and related propaganda to exacerbate divisions, hinder democratic institutions, and generally neutralize the European space, particularly in the Balkans and the “Visegrad Four” countries of the Czech Republic, Hungary, Poland and Slovakia. Xi’s multiple and insidious charm offensives, on the other hand, have been comparatively apolitical, being less concerned about democratic or authoritarian governance and more aimed at bolstering the Chinese Communist Party’s global legitimacy, especially among political, business, and intellectual elites.

Neither Moscow’s nor Beijing’s approaches and tactics are mutually exclusive. Russian state, military, and religious leadership affirmatively engage aligned or sympathetic elites, while China uses media proxies to steer public discourse in its favor on its priority issues — Hong Kong’s autonomy, Taiwan’s de facto independence, and the human rights of China’s Uyghur and Tibetan communities.

To the delight of both Russia and China, the gradual weakening of U.S.-European ties over the last two decades is accelerating due to mutual neglect, miscommunication, and diminished policy coordination in a post-Cold War world. It hasn’t helped that the Trump administration’s approach to resolving inequities in NATO member defense-spending commitments or aspects of transatlantic trade relations has been nearly all vinegar and little wine. The result is rapidly diminishing support for partnership with America in key ally states such as Germany. According to a Pew Research poll in April, almost as many Germans prioritized their country’s relationship with China – 36 percent – as with the United States (37 percent). That was a significant change from a year earlier, when 50 percent of Germans preferred a closer partnership with the United States, compared with 24 percent favoring better ties with China.

Washington’s unhelpful bellicosity understandably alienates many Europeans, making it all the more difficult for their elected leaders to work jointly even on common interests. This reciprocal disengagement between Washington and key European capitals leaves room, in turn, for adversarial interventions by Russia and China.

### China Threat Now

#### China is fraying the international order and threatening international security now

Beckley, Harvard international security fellow, 22

[Michael Beckley, 4/2022, Foreign Affairs, “Enemies of My Enemy: How Fear of China Is Forging a New World Order.”, <https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-my-enemy>, Accessed 7-8-2022, LASA-LR]

The international order is falling apart, and everyone seems to know how to fix it. According to some, the United States just needs to rededicate itself to leading the liberal order it helped found some 75 years ago. Others argue that the world's great powers should form a concert to guide the international community into a new age of multipolar cooperation. Still others call for a grand bargain that divides the globe into stable spheres of influence. What these and other visions of international order have in common is an assumption that global governance can be designed and imposed from the top down. With wise statesmanship and ample summitry, the international jungle can be tamed and cultivated. Conflicts of interest and historical hatreds can be negotiated away and replaced with win-win cooperation.

The history of international order, however, provides little reason for confidence in top-down, cooperative solutions. The strongest orders in modern history--from Westphalia in the seventeenth century to the liberal international order in the twentieth--were not inclusive organizations working for the greater good of humanity. Rather, they were alliances built by great powers to wage security competition against their main rivals. Fear and loathing of a shared enemy, not enlightened calls to make the world a better place, brought these orders together. Progress on transnational issues, when achieved, emerged largely as a byproduct of hardheaded security cooperation. That cooperation usually lasted only as long as a common threat remained both present and manageable. When that threat dissipated or grew too large, the orders collapsed. Today, the liberal order is fraying for many reasons, but the underlying cause is that the threat it was originally designed to defeat--Soviet communism--disappeared three decades ago. None of the proposed replacements to the current order have stuck because there hasn't been a threat scary or vivid enough to compel sustained cooperation among the key players.

Until now. Through a surge of repression and aggression, China has frightened countries near and far. It is acting belligerently in East Asia, trying to carve out exclusive economic zones in the global economy, and exporting digital systems that make authoritarianism more effective than ever. For the first time since the Cold War, a critical mass of countries face serious threats to their security, welfare, and ways of life--all emanating from a single source.

This moment of clarity has triggered a flurry of responses. China's neighbors are arming themselves and aligning with outside powers to secure their territory and sea-lanes. Many of the world's largest economies are collectively developing new trade, investment, and technology standards that implicitly discriminate against China. Democracies are gathering to devise strategies for combating authoritarianism at home and abroad, and new international organizations are popping up to coordinate the battle. Seen in real time, these efforts look scattershot. Step back from the day-to-day commotion, however, and a fuller picture emerges: for better or worse, competition with China is forging a new international order.

#### China must be checked to avoid escalating conflict, in recent years it has gone on the complete offensive with updated defense and economic exploitation

Beckley, Harvard international security fellow, 22

[Michael Beckley, 4/2022, Foreign Affairs, “Enemies of My Enemy: How Fear of China Is Forging a New World Order.” https://www.foreignaffairs.com/articles/2021-02-14/china-new-world-order-enemies-my-enemy, Accessed 7-8-2022, LASA-LR]

This threat is most apparent in maritime East Asia, where China is moving aggressively to cement its vast territorial claims. Beijing is churning out warships faster than any country has since World War II, and it has flooded Asian sea-lanes with Chinese coast guard and fishing vessels. It has strung military outposts across the South China Sea and dramatically increased its use of ship ramming and aerial interceptions to shove neighbors out of disputed areas. In the Taiwan Strait, Chinese military patrols, some involving a dozen warships and more than 50 combat aircraft, prowl the sea almost daily and simulate attacks on Taiwanese and U.S. targets. Chinese officials have told Western analysts that calls for an invasion of Taiwan are proliferating within the CCP. Pentagon officials worry that such an assault could be imminent.

China has gone on the economic offensive, too. Its latest five-year plan calls for dominating what Chinese officials call "chokepoints"--goods and services that other countries can't live without--and then using that dominance, plus the lure of China's domestic market, to browbeat countries into concessions. Toward that end, China has become the dominant dispenser of overseas loans, loading up more than 150 countries with over $1 trillion of debt. It has massively subsidized strategic industries to gain a monopoly on hundreds of vital products, and it has installed the hardware for digital networks in dozens of countries. Armed with economic leverage, it has used coercion against more than a dozen countries over the last few years. In many cases, the punishment has been disproportionate to the supposed crime--for example, slapping tariffs on many of Australia's exports after that country requested an international investigation into the origins of covid-19.

China has also become a potent antidemocratic force, selling advanced tools of tyranny around the world. By combining surveillance cameras with social media monitoring, artificial intelligence, biometrics, and speech and facial recognition technologies, the Chinese government has pioneered a system that allows dictators to watch citizens constantly and punish them instantly by blocking their access to fnance, education, employment, telecommunications, or travel. The apparatus is a despot's dream, and Chinese companies are already selling and operating aspects of it in more than 80 countries.

### Democratic Counter-Disinfo Key

#### Democracies are key to outcompeting a China/Russia alliance

**Brands, Johns Hopkins University School of Advanced International Studies Henry A. Kissinger Distinguished Professor, 22**

(Hal, 5-21-2022, ASHARQ AL-AWSAT, "Hal Brands - Democracies Can Out-Compete the China-Russia Alliance", https://english.aawsat.com/home/article/3657196/hal-brands/democracies-can-out-compete-china-russia-alliance, accessed on 7-8-2022, SR)

The economic trauma of the Ukraine War is only beginning: Energy shocks, food-supply disruption and commodity shortages will have growing impact as the conflict persists. The war, moreover, is just part of an accelerating geo-economic realignment.

**The golden age of globalization, when countries pursued interdependence with minimal fear of insecurity, is over.** The global economy is now being reshaped by competition and conflict. **That will create some opportunities for the US to strengthen its position** — as well as a whole lot of worldwide turmoil.

A remarkable aspect of the post-Cold War era was that calculations of economic efficiency so often trumped calculations of geopolitical risk. An era that began with the fall of the Berlin Wall was dominated by the pursuit of integration across traditional strategic divides.

A web of trade, financial and technological ties developed between China and the world’s democracies. European countries became highly reliant on Russian energy (notably Germany) and investment (the UK). The pursuit of profit was accompanied by a diplomatic rationale — that economic entanglement would create a common interest in global stability, mitigating whatever dangers might otherwise result from trading with a prospective enemy.

That rationale proved faulty. Globalization increased Chinese and Russian capabilities without meaningfully decreasing their ambitions. By the mid-2010s, global tensions were increasing and interdependence came to be seen as a source of vulnerability.

Worried that Beijing might translate technological primacy into geopolitical primacy, President Donald Trump’s administration urged other nations to wall off their 5G telecommunications networks against Chinese influence. t sought to forestall completion of the Nord Stream pipeline between Russia and Germany, lest Europe become diplomatically paralyzed by dependence on Moscow’s energy.

When Beijing then threatened to withhold critical pharmaceutical components amid the Covid-19 pandemic, it showed how complex supply chains could be wielded as strategic weapons.

In this context, the war in Ukraine has thrown global integration into reverse. Western companies that pushed into Russia after the Cold War are being forced to flee, with McDonald’s Corp. being the latest (and perhaps most symbolic). US export controls have severed Russia’s access to advanced semiconductors; Germany and other European democracies are rapidly undoing decades of economic engagement. This conflict-driven decoupling may simply be a preview of what comes next.

President Xi Jinping’s China was already pursuing what Matthew Pottinger, deputy national security adviser in the Trump administration, calls an “offensive decoupling” strategy — a program meant to insulate the country from Western pressure and give it tremendous coercive power by dominating critical technologies. Xi’s “dual circulation” program is meant to develop China’s internal market and make the country less reliant on external markets that might slam shut in a crisis.

It seems inevitable that this campaign will accelerate. China, whose relations with Washington are in a nosedive, can hardly leave itself susceptible to the sort of punishment the US and its allies have imposed on Moscow.

Similar processes are underway across the democratic world. Europe is moving to wean itself off Russian oil and natural gas. The US is considering sharper curbs on investment in China; Treasury Secretary Janet Yellen is pushing “friend-shoring,” or relocating production to countries aligned with Washington.

The administration of President Joe Biden is also working with allies, such as Japan, to create technological supply chains and innovation ecosystems that leave China on the outside.

#### Focus on democratic values key to preventing Russia-China authoritarian axis

Becker, US Military Academy International Relations professor, et al., 6-28-22

(LTC Jordan, Douglas,Former North Atlantic Council Permanent United States Representative, and Simon, Staffordshire University Defense Studies Editor-In-Chief Associate Professor, 6-28-2022, War on the Rocks, "Don’t Let Russia Dominate the Strategic Concept - War on the Rocks", https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed on 7-6-2022, SR)

As the trans-Atlantic community focuses on the Russo-Ukrainian war, rivalry with China continues apace. Scholars and policymakers differ on conceptual approaches to this dual dynamic, with some arguing for a geographic division of labor both within Europe and across the Atlantic, and others maintaining that, because Europe is less than the sum of its parts, U.S. military leadership remains indispensable.

Identifying a role for NATO in the Indo-Pacific is exceptionally challenging. Whether by Europeanizing NATO to enable the United States to focus on the Indo-Pacific, contending with Chinese commercial investment in European critical infrastructure, or encouraging allies to engage in Asia themselves (individually or collectively), the new strategic concept must address the relationship between the trans-Atlantic community and China. At an absolute minimum, the strategic concept should position NATO to support the current global order and “demonstrate its commitment to security and democratic values as well as to the peaceful resolution of disputes.” Such a concerted approach to China is certainly attainable: Chinese behavior may even have “brought NATO together” in ways analogous to Russian behavior, and there may be more room for economic convergence between China and the West than sometimes imagined.

A significant strategic concern for NATO allies is to avoid precipitating a Russian-Chinese authoritarian alignment. While Russia and China face distinct strategic challenges of their own and their “unlimited partnership” has appeared to stumble upon some limits, their continued pursuit of emerging, disruptive technologies and their authoritarian models of governance present significant risks to NATO allies. These models, coupled with Russia and China’s shared willingness to undermine national and international institutions in the trans-Atlantic community, mean that the most daunting threat NATO faces may be to its foundational values. Incorporating these core values into strategy and policy will be a key task for the 2022 Strategic Concept.

### Democracy Good – Climate

#### Democracies and their free flow of information are key to averting climate change-related existential threats

Carayannis, George Washington University School of Business Science, Technology, Innovation and Entrepreneurship professor & European Union Research Center director, 21

[Elias G. Carayannis, 5-15-2021, MDPI, "Democracy and the Environment: How Political Freedom Is Linked with Environmental Sustainability,", [https://www.mdpi.com/2071-1050/13/10/5522, p.](https://www.mdpi.com/2071-1050/13/10/5522,%20p.) 10 – 11, Accessed 7-8-2022, LASA-LR]

Global warming, including other negative environmental developments, has several implications and ramifications. It is related to the survival of human civilization. However, there is apparently also a direct nexus of global warming to democracy. The tensions that global warming is creating also pose a direct threat to democracy, as poor (or decreasing) environmental performance may constrain freedom by favoring authoritarian tendencies. Therefore, the prevalence of democracy in the world will also require the implementation of solutions and problem-solving regarding important ecological themes. The prospering of democracy is also tied to the environmental challenge of sustainability.

Future research efforts should examine additional data that can better explain factors related to climate change and global warming, such as rising temperatures, extreme weather events, rising sea levels, and etc. in the context of socio-political, socio-economic, and socio-technical dynamics. Furthermore, mitigation and adaptation policies to climate change may also explain the relation between democracy and environment. Climate change is a global issue that requires global cooperation and long-term commitments; the quality of democracy, therefore, is a key factor. As noted by several scholars, democracies are characterized by the free flow of information regarding problems and solutions, increased administrative capacities, lower levels of corruption, improved scientific and technical capacity, and dynamic, innovative economies [90,91]. In this context, under a Quadruple and Quintuple Helix approach (Quadruple and Quintuple Innovation Helix Frameworks), it will be interesting to examine the role of civil society and innovation in a more holistic environment-democracy-innovation nexus.

### Democracy Good – Environment

#### Democracies are essential to developing effective, sustainable environmental programs

Carayannis, George Washington University School of Business Science, Technology, Innovation and Entrepreneurship professor & European Union Research Center director, 21

[Elias G. Carayannis, 5-15-2021, MDPI, "Democracy and the Environment: How Political Freedom Is Linked with Environmental Sustainability,", [https://www.mdpi.com/2071-1050/13/10/5522, p.](https://www.mdpi.com/2071-1050/13/10/5522,%20p.) 10 – 11, Accessed 7-8-2022, LASA-LR]

What this correlation tells us is that, simply: The higher the political freedom in a country, the more likely it is to have a higher environmental performance. Similarly, the lower the political freedom in a country the more likely it is to have a lower environmental performance. Of course, since Pearson’s correlation coefficient is not able to identify cause and effect, the previous findings need further analysis, validation, and justification in order to understand the aforementioned interrelations.

However, it should be stressed that correlation is not causation. We should consider that it is almost impossible to suggest that results show causal determinism, which might imply that lower environmental performances are automatically interlinked with authoritarianism or lead to authoritarianism. Moreover, the presented results may indicate a spurious correlation, despite the existence of studies that justify the interrelations between democracy and the environment. Therefore, in order to confirm that aforementioned correlations are sound, additional variables should be considered in order to model an integrated dynamic environment-democracy system (see also [89]). Consequently, the democracy-environment nexus. Simultaneously, it should be emphasized that such early-stage correlative work can help in the preparation of later work with more advanced statistical means.

#### Democracy promotes the sharing of citizen’s ideas, and allows for more climate action to transpire due to the value they place on listening to their populace

Akalin, Kutahya Dumlupınar University Economics professor & Sakarya, Hatay Mustafa Kemal University Economics professor, 20

[Guray Akalin and Sinan Erdogan, 10-7-20, Environmental Science and Pollution Research, “Does democracy help reduce environmental degradation?”, https://doi.org/10.1007/s11356-020-11096-1, https://rdcu.be/cRg6d, accessed 7-8-2022, LASA-LR]

Adams and Acheampong (2019) emphasized that democracy promotes civic competence and gives awareness to citizens for differentiating public and individual interests. Democracy gives freedom of choice to individuals; therefore, citizens could freely choose the environmental policies by the voting mechanism. Moreover, autocratic regimes fail to provide public goods; hence, the provision of a clean and sustainable environment may not be achieved in autocracies (Olson 1996). According to Payne (1995), individuals are free to learn about the environment and ecological policies and can express their opinions, priorities, and putting political pressure on the government through voting (Acemoglu and Robinson 2006). Moreover, in democratic systems, individuals have greater access to information about environmental issues through freedom of the press. They also have the right to organize and lobby for environmental protection at both national and international levels (Kinda 2011). Pande (2003) points out that “a basic premise of representative democracy is that all those subject to policy should have a voice in its making.” Therefore, individuals living in democratic societies have more influence than those living in autocratic systems in which people are not allowed to express opinions on socioeconomic or ecological issues. Thus, demands for better environmental quality can be easily transmitted in the decision-making process and can force leaders to raise environmental standards. McCloskey (1983) and Payne (1995) assert that democratic governments are more sensitive to individual demands on ecological issues, which could encourage them to fulfill responsibilities and commitments under international treaties. Moreover, they emphasize that in autocratic systems individuals are not allowed to freely express their opinion on socio-economic issues, as well as ecological ones, they are not allowed to organize, and access to information without no cost is almost impossible.

### AT – Plan Censors/Hurts Democracy

#### Regulating social media companies is key to protecting democratic engagement in the public sphere.

Mckay and Tenove, The University of British Columbia Vancouver; Centre for the Study of Democratic Institutions Research Associate and Political Science Postdoctoral Research Fellow, 20

(Spencer Mckay, The University Of British Columbia Vancouver Centre for the Study of Democratic Institutions Research Associate, Chris Tenove, Chris Tenove, University of British Columbia Political Science Postdoctoral Research Fellow. SAGE Journals, 7-4-2020, "Disinformation as a Threat to Deliberative Democracy," Political Research Quarterly 2021, Vol. 74. No. 3, p. 706, https://journals.sagepub.com/doi/full/10.1177/1065912920938143, accessed 7-1-2022) SS:/

Online communication has introduced new means to disguise or misrepresent the authors and amplifiers of communication. The impact of these developments is complex as anonymity promotes inclusion or exclusion in different contexts (Asenbaum 2018). Anonymity or pseudonymity can enable people to speak their minds without fearing repercussions for expressing views that could face social sanction or government repression. Techniques to disguise one’s identity may be important measures to counteract the increased capacities of digital media systems for state and corporate surveillance. Among other benefits for deliberative systems, this can enhance inclusion and expose a “false impression of conformity” of opinion on issues (Moore 2018, 182).

However, the possibility for social media users to disguise their identity can also enable manipulative and unaccountable communication. Disinformation actors regularly misrepresent their identities through the use of “sock puppets” (fake accounts operated by humans) or “political bots” (“algorithms that operate over social media, written to learn from and mimic real people,” Woolley and Howard 2016, 4885). As Moore (2018, 182) puts it, the misrepresentation of identity “leaves the listener unable to judge the interests, agendas, and biases of the speaker, and thereby creates opportunities for strategic and deceptive communication.” A similar problem applies to fake news organizations, think tanks, and government agencies. Because all sources of content tend to look the same on social media, users often suffer “source blindness” and do not apply the interpretive shortcuts they would otherwise use to assess source credibility (Pearson 2020).

The ability to misrepresent identities on social media is one of many means by which social media can reduce accountability. Most basically, some individuals can push false and insulting messages online, even using a real name, knowing that violations of social norms are unlikely to lead to sanctions in their off-line lives. Disinformation actors can micro-target messages to audiences in ways that avoid detection by more critical publics and they can engage in transnational operations, knowing that it is difficult or impossible for state authorities to enforce their laws outside their jurisdiction.

Democracies must protect citizens’ opportunities to contribute to public discussion, especially in the wild public sphere; prevent communication from being overwhelmed by coercive, economic, or other forms of dominating power; and support transmission mechanisms that facilitate accountability and responsiveness of empowered sites of discourse. Media regulation is fraught due to threats of capture by the state, political factions, and economic actors, and all democracies regulate mass media in ways that grapple with these tensions. However, social media companies have evaded many forms of accountability and public oversight that apply to other mass media companies.

## Alliance Cohesion

### Now Key Time

#### Must act now to prevent disinformation – Disinformation magnifies all impacts – it is a force magnifier, spoiler and entangler – undermining democratic institutions, deterrence, and NATO cohesion

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 289-90, accessed 6-22-22, AFB]

Disinformation, fake news and—since the COVID-19 pandemic erupted in 2020—“infodemics” have been added to the vocabulary of societies across the world. Often conflated with other terms including misinformation, tainted leaks, and propaganda, disinformation is the use of false or manipulated information to distort the truth, weaken trust, and undermine democratic discourse and practices. It has become a catch-all for information manipulation operations and has fundamentally altered the way we view geopolitical competition, warfare, and security.

For NATO, a defensive military alliance based on collective defense—“an attack against one is an attack against all”—disinformation has until recently been rarely discussed, much less considered. Article 2 of the North Atlantic Treaty, however, underscores that “peaceful and friendly international relations” come not from military strength alone, but strong and free member state institutions and an understanding of the principles behind them.1 Disinformation, which is part of broader malign influence operations, directly threatens these principles and institutions. Its acceleration in recent years has brought disinformation onto the transatlantic agenda.

In the coming decade, NATO is likely to face an increasingly complex and contested strategic environment. Disinformation will lurk as a force-multiplier, spoiler, and entangler. Russia and China have demonstrated willingness to deploy non-military means against NATO and could intensify the use of disinformation with the benefit of emerging technologies. At the operational level, disinformation could increasingly probe and erode NATO’s defense and deterrence. At the strategic level, long-term information operations and narratives skeptical of NATO’s enduring purpose could weaken solidarity and cohesion. To protect its political center-of-gravity, NATO should crystallize where disinformation fits among the multiplicity of threats likely facing the Alliance in the emerging security environment and then further evolve its approach to countering disinformation.

#### Disinformation fuels authoritarianism and poses an existential threat to the alliance, undermining democratic models, principles, and decision-making that are key to the alliance

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 290-292, accessed 6-22-22, AFB]

The Threat of Disinformation

Disinformation is used strategically to challenge the very foundations of liberal democracy and of transatlantic relations by affecting political decision-making, societies, and the very functioning of democratic institutions. Political warfare and disinformation allow authoritarian regimes to present the authoritarian governance model—and during COVID-19 its crisis management—as a superior alternative to democracy.2 Given the magnitude and resources of their state-owned media operations and global ambitions, Russia and increasingly China are the most prominent authoritarian adversaries for the transatlantic Alliance.3 But the use of disinformation is proliferating among a multitude of state and nonstate actors, including most notoriously the Islamic State (ISIS). US law enforcement agencies noted in a report about foreign interference in the 2020 elections that Iran, Venezuela, and Cuba are also present in this space, as well as other nonstate actors like Hizballah.4 Worryingly, various actors within democratic societies and NATO members are also turning to disinformation and information suppression to advance their political goals domestically.5 A prominent tool of political warfare during the Cold War—Soviet campaigns of “active measures” and dezinformatsiya6—propaganda and disinformation went under the radar for the better part of the past 30 years in the West. The Kremlin’s military aggression in Ukraine and illegal annexation of Crimea in 2014 revealed Russia’s use of information as a weapon, amplified and strengthened by modern technologies, social media, and a revamped state-media apparatus. Disinformation campaigns became a central tool for denying, justifying, and supporting its actions in Ukraine. It created an alternate reality meant not only to obscure Russia’s involvement, but also to completely discredit theidea of factuality, truth, and trust in the possibility or mere existence of facts (“implausible deniability”).7 This became a core tactic for the Kremlin’s power projection in Europe and particularly in former Soviet or satellite states. The attempt by pro-Kremlin actors to influence the 2016 US election was another turning point. It revealed the vulnerability of consolidated democracies and the irrelevance of geography when it comes to new modes of political warfare. Disinformation and other means of malign influence build over time, prey on local conditions, prime audiences for future attacks and are mobilized at crucial moments such as elections, requiring significant resources to investigate and uncover them. Disinformation is deployed as a force multiplier, part of a toolkit of malign influence tactics to ensure the success of broader strategic aims.8 These can be military operations, such as Russia’s war against Georgia and Ukraine or its intervention in Syria, or intelligence operations, such as the Skripal poisoning case in the United Kingdom, whereby the Kremlin sought to provide a cover for its unlawful incursion on UK territory in a cloud of disinformation and competing narratives. During the first peak of the COVID-19 crisis, the use of disinformation, propaganda, and coordinated digital deception by both Russia and China went hand in hand with so-called ‘mask diplomacy,’ a media strategy accompanying the delivery of medical supplies by Russia and China to Europe.9 These information operations were meant to highlight the European Union (EU) and NATO’s lack of solidarity with their members and incapacity to act swiftly and effectively. China also branded a new, more aggressive approach to engaging with Western counterparts—so-called ‘wolf-warrior diplomacy’—both in official communication and by leveraging its state media and an increased social media presence.10

Disinformation has become a weapon to undermine and potentially distort the outcomes of democratic elections, introduce wedges in the transatlantic alliance, deepen public health crises, and change the nature of conflict. Thus, the salience of disinformation has grown exponentially among researchers, civil society, and policy makers in civilian and military structures alike. Increasingly, military structures are starting to incorporate countering disinformation in their strategies11 because ambiguity and masked intentions could negate readiness and delay reinforcement.12 Supranational structures like the EU, NATO, and G-7 also have dedicated programming on tackling disinformation. With this, it has become a pressing national and transatlantic security threat and poses a long-term existential challenge to the values and principles underpinning the North Atlantic Treaty.

#### Ukraine is undermining alliance China strategy

Becker, US Military Academy International Relations professor, et al., 6-28-22

(LTC Jordan, Douglas, Former North Atlantic Council Permanent United States Representative, and Simon, Staffordshire University Defense Studies Editor-In-Chief Associate Professor, 6-28-2022, War on the Rocks, "Don’t Let Russia Dominate the Strategic Concept - War on the Rocks", https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed on 7-6-2022, SR)

When NATO members agree on a new Strategic Concept at their summit in Madrid, Russia’s invasion of Ukraine will dominate the discussion. **But with this existential crisis rightfully taking center stage, other threats have not gone away.** The challenge for NATO is to situate Russia’s invasion in a wider strategic context, addressing other key issues before they create new existential crises in the future.

What does this mean in practice? We contend that despite the current centrality of the Russo-Ukrainian war, Sino-American rivalry is likely to drive U.S. national security thinking in the coming decades. NATO’s 2022 Strategic Concept should address this reality. Among the many challenges in Asia and the broader Indo-Pacific, **China’s designs on Taiwan figure most prominently. China is watching the Russo-Ukrainian war closely, seeking to draw strategic lessons.** This dynamic need not be catastrophic for European and trans-Atlantic security. It creates opportunities for E.U.-NATO cooperation and greater European strategic autonomy (or strategic responsibility) in the context of an enduring trans-Atlantic bond. Europe and Asia are increasingly linked as two theaters in a global system hinging on the United States and anchored in its alliances in both regions. The strategic concept should thus lay out a vision for how NATO can simultaneously compete with both China and Russia.

### Internal Link – Disinformation Undermines Alliance

#### Erosion of truth breaks down alliances

Grimes, Committee for Skeptical Inquiry post-doctoral fellow, 2**2**

(David Robert, 3-28-2022, Scientific American, "Russian Misinformation Seeks to Confound, Not Convince", https://www.scientificamerican.com/article/russian-misinformation-seeks-to-confound-not-convince/, accessed on 7-6-2022, SR)

Rather than take a side, these campaigns create decision paralysis that leads to inaction

As war envelops Ukraine, Russian sources have strived to create a miasma of disinformation about the invasion. Among ample efforts to distort reality, the Russian Ministry of Defense asserted recently that U.S.-backed labs in Ukraine have been developing bioweapons. Outlandish as this falsehood may be, Fox’s Tucker Carlson gave it credence by arguing that the U.S. government’s response was a “cover-up.”

As the Russia-Ukraine war intensifies, so too will the flow of disinformation. This is an age-old strategy Russia has long history of employing, and a playbook that others, most notably anti-vaccine activists, have borrowed from liberally. Yet, rather than focusing effort on convincing people of a falsehood, the Russian strategy takes a tack reminiscent of a strategy long employed by the tobacco industry: to sow so much doubt about what is true that it sends people into decision paralysis. Faced with a cacophony of wild and conflicting claims, people do nothing, unsure of what is right.

Despite constituting only a small part of our media diet, disinformation campaigns, in our digital world, can be devastatingly effective. We are intrinsically biased towards information that is emotionally visceral. We afford more weight to content that frightens or outrages us, with the ability to induce anger serving as the single greatest predictor of whether content goes viral. This propels the most visceral, divisive narratives to the forefront of discourse, creating a sound and fury of passionately debated claims and counter claims. In that atmosphere, it becomes increasingly difficult to ascertain what to believe, and easy to abandon the task of discerning the truth.

If we are not to fall victim to such rank dishonesty, it is crucial now that we question our sources more carefully than ever before.

Indecision and distraction have long been central to Russia’s dezinformatsiya (disinformation) policy, a term Stalin himself is credited with coining. While an ancient concept, Russia had by the imperial age mastered dark obfuscation techniques refined for the era of mass communication. By the dawn of the Soviet empire, they realized this potential on an industrial scale, establishing the world's first office dedicated to disinformation in 1923. In the 1960s, the KGB covertly sponsored American fringe groups, amplifying conspiratorial narratives about everything from the assassination of president John F. Kennedy to water fluoridation.

The goal, as KGB Major General Oleg Kalugin elucidated in 1998, **was “not intelligence collection, but subversion: active measures to weaken the West, to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people of Europe, Asia, Africa, Latin America....”**. Operation INFEKTION, a mid-1980s clandestine effort to spread the myth that AIDS was a CIA-designed bioweapon, was but one infamous exemplar. While utterly fictious, it resonated with communities ravaged by HIV and neglected by the callous indifference of the Reagan administration. Despite Russian intelligence taking responsibility for this lie in 1992, the legacy of AIDS denialism persists to this day worldwide.

During the Cold War, the doctrine of “active measures” was the beating heart of Soviet intelligence. This philosophy of political and information warfare had wide remit, including front groups, media manipulation, counterfeiting, infiltrating peace groups and even the occasional assassination.

And in our media-saturated era, Russia has been, by far, disinformation’s most enthusiastic user. Take the 2016 U.S. presidential election and the contentious Brexit referendum; Russia appears to have influenced both via lies and distortions.

But disinformation is not solely confined to geopolitics. By summer 2020, the European Commission identified a concerted Russian drive to propagate COVID disinformation worldwide. From the outset of the pandemic, Kremlin-backed troll farms pushed the narrative that COVID was an engineered bioweapon, peddling the explosive fiction that 5G radio frequencies caused the virus—a lie that resulted in dozens of arson attacks on cell towers worldwide.

There is a dark irony in the observation that conspiracy-minded people can be weaponized in plots to which they’re entirely oblivious. The enduring popularity of the virus-as-a-bioweapon mantra is a stark reminder that in the age of social media, such manipulation has become ever easier and more effective. Perhaps the most odious example of this is the cynical rise of anti-vaccine propaganda.

The sheer efficacy of vaccination is scientifically incontrovertible, and after clean water, immunization is the most life-saving intervention in human history. Despite this, the last decade has witnessed precipitous drops in vaccine confidence worldwide. The renaissance of once-virtually-conquered diseases prompted the WHO to declare vaccine hesitancy a top-10 threat to public health in 2019.

Sign up for Scientific American’s free newsletters.

Vaccine hesitancy is a spectrum rather than a simple binary, and exposure to anti-vaccine conspiracy theories nudges recipients towards rejection. But critically, many who decline vaccination are not dyed-in-the-wool anti-vaccine zealots, but simply scared by what they have heard, unsure what to believe. Our tendency towards the illusory truth effect exacerbates this inertia, as the mere repetition of a fiction is enough to prime us to accept it, even if we know it to be false on an intellectual level. While Russia has often amplified anti-vaccine conspiracy theories to increase tensions, the anti-vaccine movements exist independently of these efforts, and are masters at sowing the seeds of doubt with torrents of conflicting and emotive claims.

This illustrates the grim reality that disinformation has no need for consistency and zero commitment to objective reality; claims are frequently contradictory, arguing both sides of the coin in exaggerated and divisive ways. This “Russian firehose” model of propaganda is high-output, contradictory and multichannel. The stream encourages us to sleepwalk into apathy, distrustful of everything. This renders us supremely malleable, and dangerously disengaged.

When it comes to vaccination, concerned parents often opt to stay with the devil they know, delaying or even rejecting vaccination rather than sifting through the symphony of conflicting claims to which they’re subjected. Similarly, the outpouring of fictions about Ukraine, its president, Volodymyr Zelensky, and the war is designed to overwhelm our capacity to analyze, inducing us to implicitly accept uncertainty over aggressor and aggrieved—a manufactured doubt benefitting Russia and other nations.

**Conviction is not the chief goal of disinformation; instilling doubt is.** This is why anti-vaccine activists have been so successful online, and why Russian troll-farms push ample resources into hawking lies virtually everywhere. The ubiquity of these fictions gives them an implicit veneer of legitimacy, fueling polarization and distrust.

This is the strategy Putin continues to pursue; already Russian propaganda has tried to paint Ukraine (or NATO / America) as aggressors with staged disinformation. This has been rendered less effective by the Biden administration’s creative approach of releasing intelligence prior to the operation. Across social media, Russian front organizations still try to induce doubt, efforts that will only intensify as the war wages on. Truth, the old adage insists, is the first casualty of war.

#### Russian disinformation campaigns break down alliances and democratic norms

**Evans, George Washington University Elliot School of International Affairs M.A. candidate 4/12/22** [Jacqueline, 4-12-22, Russian Analytical Digest, "Russian Information Warfare", [https://doi.org/10.3929/ethz-b-000541999 page 10, accessed on 7-6-22](https://doi.org/10.3929/ethz-b-000541999%20accessed%20on%207-6-2022) hooch//cs]

**Even though Russian information warfare is not a new concept, it still poses a massive risk to U.S. democracy and its ability to act on the international stage**. To better understand the threat, it is important to understand why Russia is using informational warfare against the US, what Russia’s goals are, and what the Kremlin is targeting

All actions taken by the Kremlin are carried out to achieve Russia’s geopolitical goals, including preserving its zone of influence in the countries of the former Soviet Union, attaining desirable opportunities to extend Russian sway internationally, expanding the Russian economy, and protecting Russian culture and society from information interference and psychological attacks (Gurganus and Rumer, 2019**). To achieve many of these goals, Putin believes that Russia must undermine the standing of the US domestically, in Europe, and around the world, as the Kremlin sees the US as pursuing policies to maintain American hegemony and isolate Russia** (Wojnowski, 2021).

At its core, **Russia seeks to use information to exert psychological influence over individuals, societal groups, nations, and multilateral institutions (Saradzhyan, 2021). Therefore, Russia’s information warfare targets U.S.democracy to create internal divisions, increase political polarization, influence elections, and discredit democratic institutions, as well as strain relations between the US and its allies/partners through misinformation campaigns within and outside the US that exacerbate tensions and undermine coalitions** (Wojnowski, 2021).

Essentially, Russia’s goal in the US is to create so much polarization and division that Americans come to doubt the legitimacy of democracy and their government**. Internationally, Russia hopes to weaken Western coalitions by promoting information that makes allies and partners question each other.**

Solvency – Cohesion

Diverse threats against NATO poise an opportunity to bring the alliance to harmony

Becker, US Military Academy International Relations professor, et al., 6-28-22

(LTC Jordan, Douglas,Former North Atlantic Council Permanent United States Representative, and Simon, Staffordshire University Defense Studies Editor-In-Chief Associate Professor, 6-28-2022, War on the Rocks, "Don’t Let Russia Dominate the Strategic Concept - War on the Rocks", https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed on 7-6-2022, SR)

There are also several specific threats and challenges that the 2022 Strategic Concept should address. First, allies should tackle the effects of emerging and emerged disruptive technologies on strategic, defense, and force planning. Second, adversaries are increasingly using high- and low-tech approaches short of armed conflict to disrupt national politics and daily life in Western democracies. Enhancing and coordinating resilience across the alliance should be a goal of the strategic concept. Third, money remains the sinew of war. Whether it is investment in national and common-funded capabilities, or transfers to partners like Ukraine, ample and efficient spending is a requirement for a successful strategy. Fourth, NATO should continue to grapple with the distinct but related challenges of terrorism and irregular warfare.

While it seems clear that Russian aggression has mitigated some centrifugal tendencies in the alliance, NATO will remain more like an orchestra requiring a conductor to avoid strategic cacophony, rather than a self-organizing jazz band. The strategic concept represents an opportunity to better bring the members of the alliance into harmony. To do so, it should address the dual challenge posed by Russia and China, while better balancing NATO’s core commitments with a diverse set of new and growing threats.

#### Solvency – NATO can solve impacts of disinformation by modeling existing infrastructure

Smalley, Journalist Northwestern University MA Journalism, 22

(Suzanne, Northwestern University MA Journalism, 6-29-2022, CyberScoop, "NATO to create cyber rapid response force, increase cyber defense aid to Ukraine", https://www.cyberscoop.com/nato-madrid-summit-cyber-ukraine/, accessed on 7-6-2022, SR)

NATO announced plans Wednesday for a commitment to create a rapid response cyber force and to bolster military partnerships with civil society and industry to respond to cyber threats.

Coming on the heels of a meeting that included leaders from all 30 allied countries, the Madrid summit declaration also said NATO will do more to support Ukraine’s cyber resilience and defense against Russia while also focusing on China as a long-term and mounting cyberthreat.

“We are confronted by cyber, space, and hybrid and other asymmetric threats, and by the malicious use of emerging and disruptive technologies,” the declaration said. “We face systemic competition from those, including the People’s Republic of China, who challenge our interests, security, and values and seek to undermine the rules-based international order.”

The declaration’s mention of more military collaboration with industry is critical, said Jim Lewis, who directs the Strategic Technologies Program at the Center for Strategic and International Studies.

“Paragraph 10 is the key, since it announces more civil-military cooperation and a rapid reaction force – these were the crucial elements of Ukraine’s successful cyber defense,” said Lewis, who was previously rapporteur and senior adviser for four U.N. Groups of Governmental Experts on Information Security.

Cooperation is a regular theme of the document.

“We will significantly strengthen our cyber defenses through enhanced civil-military cooperation,” the declaration says. “We will also expand partnership with industry. Allies have decided, on a voluntary basis and using national assets, to build and exercise a virtual rapid response cyber capability to respond to significant malicious cyber activities.”

The declaration is a departure from past iterations which have tended to rely on “routine ‘we are concerned about cyber’ add on statements” instead of the substantive focus in the declaration released Wednesday, said Mark Montgomery, senior director of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies and the former executive director of the Cyberspace Solarium Commission.

“Cyber is now part and parcel of both the threat and the response that NATO looking at — it’s no longer some foreign object. It is something that they have been building steadily since [the] Lisbon [NATO summit] many years ago, and it’s become more and more prominent as time goes on. And that’s appropriate.”

## Russian Hegemony – DRAFT

### 1AC – Russian Hegemony – DRAFT

#### Russian disinformation is used to bolster Russia’s geopolitical influence – including in Africa

**Goldenziel**, **U.S. Marine Corps University Associate Professor of International Relations, 22**

[Jill, 03-30-2022, Forbes.com, "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=33f0b74c25a0, accessed on 7-5-2022, hooch//cs]

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.

#### Russia uses disinformation to legitimize its policies in a zero-sum competition with the US

**Szabó, security engineer & International Centre for Migration Policy Development research intern, 22**

[Réka Szabó, works for the International Team for the Study of Security Verona in the International Centre for Migration Policy Development as a research intern, 6-18-2022, International Team for the Study of Security Verona, "Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?", <https://www.itssverona.it/wp-content/uploads/2022/06/Reka-Szabo.pdf>, p. 3-4, accessed on 7-2-2022, MG]

There are differences between the Western and Russian attitudes to warfare in cyberspace. The Russian interpretation of cyber warfare — as it is called in the West — is a kind of warfare that is part of the so-called information confrontation. 3 This has to be observed through the lens of a geopolitical zero-sum game, in which the national interest is achieved or protected with the involvement of information infrastructures. Cybersecurity as a term does not appear in Russian usage. Documents from the Ministry of Defense and other authorities refer to it as information security instead. This encompasses more than cybersecurity: it is not solely about “the protection of critical digital networks, but society’s cognitive integrity as well.”4 This points out that maintaining narratives about certain events among populations is considered crucial by Russia. By using operations that focus on the cognitive spheres, Russian actors are able to spread disinformation and misinformation. As the narratives become entrenched in the population, Russia is able to use them as justification for their foreign policy and claim their strategic aims are legitimate.

#### Strong US engagement with African countries key to African growth and stability

**Signé,** Thunderbird School of Global Management Executive Director **21** [Landry, 7-28-2021, Brookings, "US trade and investment in Africa", <https://www.brookings.edu/testimonies/us-trade-and-investment-in-africa/> accessed on 7-8-2022 hooch//cs]

Advancing trade, investment, and technology in Africa offers enormous economic growth and increased prosperity for both regions and is best realized through value-based foreign policy and a market-based model of development, education, and accountability. There is no better time to accelerate U.S. trade and investment in Africa than now. Despite Africa’s tremendous economic potential, the U.S. has lost substantial ground to traditional and emerging partners, especially China. Indeed, while recent trends indicate that the U.S. engagement with the region has fallen, it has not and should not cede its relationship with the region to other powers.

Importantly, the U.S. can build on new regional momentum to revive and strengthen its partnership with Africa for mutual prosperity, including building on the recent launch of the African Continental Free Trade Area (AfCFTA), and given the promise of the initiatives of the DFC, Prosper Africa, and the post-AGOA 2025 options. To do so means a shift in emphasis in the relationship to one more focused on value-based foreign policy,[1] and also building upon the areas of strength and convergence with African citizens’ preferences;[2] such as trade, investment, technology, education, accountability, and a market-based model of development

Trade and investment are not just about money and prosperity. They also bring and support peace, stability, and security. In my book Unlocking Africa’s Business Potential,[3] I explore key trade and investment trends, opportunities, challenges and strategies, that illustrate the tremendous potential of Africa, and explain the complex competition between emerging and established powers on the continent. The following key trends are critical for policymaking given their implications for trade investment, economic transformation, inclusive prosperity, geopolitical dynamics, and mutual U.S.-Africa interests.

Africa’s economic transformation and business potential are more substantial than most people think: the world’s next growth market. Considered a hopeless continent in 2000 by The Economist, Africa has seen the two best cumulative successive decades of its existence in the 21st century. Trade in and with Africa has grown 300 percent in the last decade, outperforming global averages (196 percent).[4] It has become home to many of the world’s fastest-growing economies, offering unique opportunities for U.S. trade and investment. Moreover, Africa has tremendous economic potential and offers rewarding opportunities for local and global partners looking for new markets and long-term investments with some of the highest returns, but also the potential to foster economic growth, diversification, job creation, including for women and youth, and improved general welfare.

The fast population growth on the continent could be turned into demographic dividends, or threats to global prosperity and stability. Africa was home to 17 percent of the world population in 2020, and is expected to have 26 percent of the global population in 2050 (2.53 billion people).[5] If Africa is not successfully integrated into the global economy, there could be a major threat to global prosperity and stability. Citizens could be further subject to extreme poverty, fragility, violent extremism, illegal immigration, health challenges, among others—challenges that many already face on the continent. If our goal is a prosperous and safe world, Africa must not be left behind.

The growth of household consumption and business spending: a unique opportunity for U.S. trade and investment. By 2050, Africa will be home to an estimated USD 16.12 trillion of combined consumer and business spending.[6][7] And Africa’s prosperity can be good for the U.S.: Such growth will offer tremendous opportunities for U.S. businesses in household consumption (USD 8 trillion) in areas such as food and beverages, housing, hospitality and recreation, health care, financial services, education and transport, and consumer goods, but also business to business spending (construction, utility, and transportation, agriculture and agri-processing, wholesale and retail, etc.).

4. The rise of global partnerships and the competition between traditional and new players: an opportunity for the U.S. to build on its sustainable competitive advantage. In 2009, China became the region’s prime trading partner. In fact, between 2006 and 2016, China’s trade with Africa surged, with imports increasing by 233 percent and exports increasing 53 percent, as they did for several other global players as well.[8] During the same period, the U.S. lost ground in exports to Africa (-66 percent).[9]

China’s influence goes beyond the trade relationship: It is also the top investor in infrastructure, and now is the first destination of English-speaking African students, outperforming the U.S. and the U.K But the U.S. remains a critical player on the continent, as I mentioned in a recent article: “Successes in the past decades—initiatives such as the African Growth and Opportunity Act (AGOA), the President’s Malaria Initiative, the President’s Emergency Plan for AIDS Relief, the Millennium Challenge Corporation, and U.S. trade and investment hubs—have generated tremendous opportunities for millions of Africans and Americans. But the current era—and competition from other global powers—will require new ideas and a new approach to several key issues.”[12] In fact, African countries would often prefer to work with the U.S. given local content regulation rules, more investment in on-the-ground resources, and standards about hiring/training locals. In other words, the U.S. is less extractive and more transparent than numerous other partners.

5. Fast urbanization but also fast rural population growth: By 2030, Africa will be home to 5 cities of more than 10 million inhabitants and 12 other cities of more than 5 million inhabitants.[13] Cities in Africa are becoming powerful economic centers, and a city-based approach to foreign policy, but also trade and investment, will be critical to outperform competitors and build mutual prosperity. Contributing to the prosperity of African cities will also make a difference in addressing security challenges.

6. Africa has made tremendous progress in mobilizing resources for infrastructure development, working hard to bridge gaps in ICT, energy, water and sanitation, and transportation. Despite the remaining deficits, the Infrastructure Consortium for Africa (ICA) reported that between 2013 and 2017 the annual funding for infrastructure development in the region was USD 77 billion, about twice as much as the annual funding average of the first six years of the 2000s.[14] However, many of these gaps persist. In 2018 the African Development Bank (AfDB) found that Africa’s infrastructure requirements are between USD 130 and 170 billion a year, leaving a financing gap of USD 68 to108 billion.[15] China has played a key role in financing, and has become the largest bilateral infrastructure financer in Africa (Chinese FDI grew 40 percent annually from 2010 to 2020).[16] However, the U.S. has the chance to make a monumental difference when it comes to investing in infrastructure development in Africa.

In fact, Africa has one of the fastest-growing, and is the second-largest, mobile phone market in the world.[17][18] In sub-Saharan Africa alone, there were 477 million mobile subscribers in 2019; by 2025, the region will host 614 million cell phone subscribers, and 475 million mobile internet users.[19] The internet is also expected to contribute to at least 5 to 6 percent of Africa’s total GDP by 2025.[20] While the Information and Communication Technology sector is making incredible advancements, water and sanitation, transportation, and energy infrastructure development still needs significant investment. However, this is indicative of positive and extensive investment opportunities that can be undertaken on the African continent.

7. Fast digitalization, increased technological innovation, and an accelerated Fourth Industrial Revolution (4IR): The Fourth Industrial Revolution is characterized by the fusion of the digital, biological, and technological world, and technologies such as artificial intelligence, big data, 5G, drones and automated vehicles, and cloud computing.[21] As a world leader in technological innovation, digital transformation, and the Fourth Industrial Revolution, the United States is well-positioned to play a leading role in the African digital space and contribute to Africa’s pursuit of now-vital technologies.

Indeed, advanced technology can have beneficial spillover effects: For example, in health, countries such as Rwanda and Ghana are using an American drone company Zipline to deliver, in record time, medication, blood, and medical supplies to remote rural areas with limited road accessibility.[22] In agriculture, African farmers now have access to affordable precision farming tools that use sensors, satellites, smart devices, and big data technologies to inform every decision. The lending, insurance, and e-commerce opportunities provided by the fintech industry are transforming the lives of all Africans, and not just those in urban centers. These advancements are just the beginning too, as African entrepreneurs are increasingly seeking partners to bring transformative businesses to life. African tech startup funding increased over 40 percent in 2020 to over USD 700 million, a fraction of tech startup funding outside of Africa. Despite such progress, the digital divide remains important and must be bridged to allow inclusive development. During the pandemic, for example, access to school and business on the continent was more complex given the level of internet connectivity, among other limitations. Bridging the digital divide represents an opportunity to both advance U.S. trade and investment in Africa while addressing some of Africa’s key priorities.

8. Fast regional integration and the African Continental Free Trade Areas: opportunities for a continental engagement. With the signing of the African Continental Free Trade Area (AfCFTA) in 2018, ratification in 2019, and an official launch in January 2021, African growth prospects and business opportunities have been magnified. The continent is giving the world just one more reason to invest in it with the creation of the largest new free-trade zone per number of countries in world, since the creation of the WTO. The AfCFTA will accelerate Africa’s industrialization as well as incomes, which will lead to the increase of both household consumption and business spending, generating unique opportunities for U.S. trade and investment. Per a World Bank study, the AfCFTA has the potential to lift 30 million people out of extreme poverty, increase the income of 68 million Africans, increase Africa’s exports by USD 560 billion, and generate USD 450 billion of potential gains for African economies by 2035.[23]

9. The sustained demand for accountability, democracy, and stability of African citizens, and policy priorities aligned with U.S. core values. Per Afrobarometer surveys, 7 out of 10 Africans support democracy and accountable governance, and approximately two-thirds are opposed to a single party or military government.[24] Importantly, areas in which the U.S. has a sustained competitive advantage, given its global leadership in democracy and human rights, and its support for such issues as health and education, are priorities for Africans too.[25] Given China’s leadership in infrastructure, the U.S. could grow its footprint in this area but by partnering with other players such as the G7 and the European Union countries. This approach will be welcomed by African citizens, who prefer the U.S. model of development (32 percent) over the Chinse one (23 percent).[26]

### Internal Link – Russian Disinfo Globalized

#### Russian disinfo has multiple audiences – even if debunked in some places, it may still be confusing others

**Tucker,** New York University Jordan Center for Advanced Study of Russia director**, 22**

[Joshua A, 4-12-22, Slate, "The People Who Believe Russia’s Disinformation", [https://slate.com/technology/2022/04/russia-disinformation-china-africa-latin-america.html accessed on 6-27-22](https://slate.com/technology/2022/04/russia-disinformation-china-africa-latin-america.html%20accessed%20on%206-27-2022) hooch//cs]

Every day we wake up to new Russian atrocities—and new Russian lies about those atrocities—in Ukraine. The latest example is in Bucha, a Kyiv suburb where retreating Russian forces “left behind dead civilians lining the streets—some with their hands bound, some with gunshot wounds to the head.” The Kremlin quickly issued denials and claimed the evidence was fabricated.

After weeks of war, much has been written about the success and failures of Russia’s disinformation and propaganda. These tactics, of course, are not new. Russia has been running propaganda campaigns since the Cold War. What does feel new is the preponderance of true information available—and perhaps equally importantly, the speed at which it spreads. Social media, satellite imagery, and 24/7 reporting are directly refuting Russian disinformation in real time.

That news is only reaching some people, however. It’s worth stepping back to consider the various audiences for Russia’s disinformation campaigns and examine where they’re working and where they’re not.

First, where it’s not: Ukraine and the West. Russia and Putin have spread a long line of falsehoods about Ukraine. They claimed that Russian language speakers in Ukraine would welcome a Russian invasion. They’ve denied Ukrainian statehood, claiming Ukraine has always been part of Russia. They said this “special military operation” was necessary to “liberate” Ukrainians from their “Nazi leaders.” And with the war underway, government officials now claim Ukrainians, not the Russians, are shooting and bombing their own people.

None of this is true, of course. These falsehoods fell apart immediately, both in Ukraine and in the West, largely because true information won out. The Biden administration released intelligence that was remarkably accurate in predicting Putin’s next moves. Social media users in Ukraine have posted videos documenting the brutal invasion from Russian forces. Journalists have used that evidence, along with satellite imagery and other tools, to debunk false claims. As a result, foreign audiences can not only see for themselves what’s really happening in Ukraine, but also read the heart-wrenching stories of citizens caught in the crossfire and fleeing for their lives.

That leads us to where the disinformation campaigns may be working, at least for now: Russia, China, and the world beyond NATO, the EU, and their allies.

As with Soviet-era propaganda campaigns, Putin is trying to seal off his population from information to control the narrative. Authorities have shut down independent media and blocked most Western social media. For many, the only viable option left is state-controlled media, which pushes Putin’s false narratives.

Reports indicate this is working—at least to some extent. We read stories of Ukrainians with family members in Russia who don’t believe the war is real. “Every day I send them the necessary information, but the response is that ‘This is some kind of fake information, that this cannot be the case at all, that no one can or will shoot at civilians,’” said one Ukrainian woman, speaking about her sister and cousins who don’t believe what’s happening.

Likewise, a recent poll found Russians’ support for Putin has actually increased from 71 to 83 percent since the war started, although the more repressive a regime, the harder it can be to know what people are truly thinking. Indeed, a recent study using a more sophisticated methodology designed to elicit opinions on sensitive topics found actual support for the war to be 15 percentage points—53 percent vs. 68 percent—lower than reported using traditional survey methods. On the one hand, it is interesting that even in the current climate close to one-third of Russians were willing to explicitly tell pollsters that they oppose the war. On the other, even with the more sophisticated methods, more than half of Russians still expressed support for the war, so the fact that many Russians genuinely support the war should not be discounted – the phenomenon of “rallying round the flag” in times of war is a real one. Either way, true information will be critical to topple this digital iron curtain and pressure Vladimir Putin to end the war.

We also see evidence of Russia’s disinformation narratives spreading outside of Europe and the Western world. One recent New York Times story, for example, revealed how China’s Communist Party is using university classes, the media, and videos to push “a campaign that paints Russia as a long-suffering victim rather than an aggressor and defends China’s strong ties with Moscow as vital.” Another piece in the New York Times reports on research showing how Chinese state media is directly parroting Russian propaganda talking points. Beyond China, one study discovered a coordinated network of new, fake, and hacked Twitter accounts in Africa and Asia sharing pro-Putin messages. Another study found more than 170 websites in various languages pushing war disinformation, and NBC recently reported on Russian disinformation in Latin American media. The extent to which these messages will resonate outside of the NATO countries and their allies that are directly supporting Ukraine remains to be seen, but recent votes at the United Nations show that governments in the Global South remain much more conflicted about withdrawing support for Russia, suggesting such campaigns remain important.

#### Information space is exploited by Russia to continue to spread disinformation

**Hakala, NATO Strategic Communications Centre of Excellence researcher and Melnychuk, Canadian Department of National Defence Communications Officer, 21**

[Janne & Jazlyn, 6-15-21, NATO Strategic Communications Centre of Excellence, "RUSSIA’S STRATEGY IN CYBERSPACE", <https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf>, p. 5-7, accessed on 7-2-22, MG]

Russia’s conceptualization of ‘information confrontation’ and the role of cyberspace within it is outlined in strategic policy documents, such as National Security Strategy (2015), Foreign Policy Concept (2016), Information Security Doctrine (2016), Military doctrine (2014), Conceptual Views on the Activity of the Armed Forces in the Information Space (2016), as well as works and publications by Russian military thinkers.

From the Russian perspective, cyber warfare or the Russian equivalent ‘informationtechnological warfare,’1 is only a part of the overarching concept of “information confrontation” (informatsionnoe protivoborstvo). The Russian Ministry of Defence describes the information confrontation as the clash of national interests and ideas, where superiority is sought by targeting the adversary’s information infrastructure while protecting its own objects from similar influence.2 The translation of the term informatsionnoe protivoborstvo into English has proven difficult, and has often incorrectly been translated as ‘information warfare’3 (‘informacionnaja vojna’), despite the fact that protivoborstvo refers to ‘counterstruggle’, ‘countermeasure’ or ‘counteraction’ rather than ‘warfare’.4 This paper uses the term ‘information confrontation’ due to its established status in discussions regarding hostile Russian informational activities.

The confrontation includes a significant psychological remit, whereby an actor attempts to affect informational resources (documents in information systems) as well as the minds of the adversary’s military personnel and population at large.5 Ultimately, cyber operations (or informationtechnical means) are one of many methods used to gain superiority in the information confrontation. Russia, and particularly Russian President Putin’s regime, sees the information confrontation as a constant geopolitical zero-sum competition between great powers, political and economic systems, and civilizations.6

Protecting ‘Information’: Cognitive and Technical Publicly available Russian doctrines and policy documents do not explicitly reference cyber operations. Furthermore, Russian documents do not use the term ‘cybersecurity’, but refer instead to ‘information security.’ This term differs from the Western notion of ‘information security’ (or in short: infosec) in that it encompasses not only the protection of critical digital networks, but society’s cognitive integrity as well.7 There are several reasons why Russian military thinkers apply the term ‘cyber’ when talking about Western threats and activities, but are reluctant to link the term to Russia’s own capabilities and actions. Some authors argue that this deliberate choice is related to negative connotations around Soviet-era ‘cybernetics,’ as well as the importance the term ‘information security’ holds for Russia’s own domestic politics 8.

When discussing the operational environment, Russia uses the term ‘information space’ (informatsionnoe prostranstvo), or ‘information sphere’ (informatsionnaya sfera), which again is more comprehensive than the Western concept of ‘cyberspace’ or ‘cyber domain.’ The 2016 Russian Doctrine of Information Security defines the information sphere as: “a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet […], communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating social relations in the sphere”.9

The information space refers to activities to form, transform, and store information, as well as ‘influencing individual and public consciousness, information infrastructure and information itself.’10

According to Ofer Fridman, Russia conceptualizes cyberspace as the intersection between hardware, software, infrastructure, and content11. In this framework, the information-technological layer includes hardware, software and infrastructure, while the informationpsychological layer includes hardware, software and content.’ Irrespective of the means used – technological (for example, destroying digital infrastructure) or psychological (manipulating a message on social media) – activities in cyberspace are understood in terms of their effect in the information space.12 Importantly, Russia perceives the information space in very geopolitical terms, with their domestic information space representing a continuation of territorial state borders, which they view as constantly being violated by foreign intrusions.13

NATO doctrine understands cyberspace as an operational domain and considers it as part of the information environment. This environment is ‘[…] comprised of the information itself, the individuals, organizations and systems that receive, process and convey the information’. The information processed through this environment provides the base for cognitive processes that affect individual decision-making and subsequently, behaviour. Those processes happen in three dimensions – physical, virtual and cognitive – and cyberspace involves all three of them. In this respect, NATO’s concept of the information environment is not that different from Russia’s understanding of ‘information space’ and the role of cyberspace within it. Similarly, the Russian concept of ‘information weapons’ (practically absent in Western parlance) includes more than just digital measures.14 Although the Russian Armed Forces vaguely defines them as “information technologies, means and methods used for the purposes of waging information war,” in practice the concept covers a wide array of activities (often with an emphasis on affecting the human mind); this includes the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.15

Contrary to the Western view of interstate conflict that is based on the international legal order outlined in international treaty and customary law (specifically the UN Charter and the Geneva Conventions) that makes a clear distinction between war and peace, Russia’s ‘information confrontation’ is constant and ongoing. This view is exploited by Russia to undertake activities beneath the threshold of armed conflict, allowing it to remain unpredictable and pursue strategic objectives short of causing kinetic conflict.16

A key goal of Western democracies is to maintain a free, stable and open Internet, where fundamental rights and freedoms are ensured. In this regard, ‘information security’ is perceived as the protection of data and systems, but not imposing control over the attitudes and beliefs that the users of those systems are expressing. At the same time, the principles of openness and freedom of speech upheld in Western democracies might be exploited by information and cyberattacks. Russia seeks to exploit this openness to gain ‘information superiority,’ notwithstanding whether it is in a conventional conflict with its opponents or not.

### Internal Link – Regional Instability

#### Russian disinformation leads to destabilization throughout neighboring states

Commission on Security and Cooperation in Europe, 17

[Cory, 9-14-2017, Commission on Security and Cooperation in Europe, "The Scourge of Russian Disinformation,", https://www.csce.gov/international-impact/events/scourge-russian-disinformation, Accessed 7-6-22, LASA-LR]

Russian disinformation is a grave transnational threat, facilitating unacceptable aggression by Russia both at home and across the 57-nation OSCE [Organization for Security and Co-operation in Europe] region. Russian disinformation helps support rampant violations of OSCE norms by the Putin regime, ranging from internal human rights abuses to military intervention in neighboring states to interference in elections in several countries.

On Thursday, September 14, 2017, the U.S. Helsinki Commission held a hearing on Russian disinformation in the OSCE region. Sen. Cory Gardner (CO) presided over the hearing on behalf of Commission Chairman Sen. Robert Wicker (MS). Witnesses included Mr. John F. Lansing, CEO and Director of the Broadcasting Board of Governors; Ms. Molly McKew, CEO of Fianna Strategies; and Ms. Melissa Hooper, Director of Human Rights and Civil Society Programs at Human Rights First.

In his opening statement, Sen. Gardner described the serious threat that Russian disinformation poses to the liberal international order, and underscored “how it undermines the security and human rights of people in the OSCE region.” Russia’s goal, he said, is “to sow fear, discord, and paralysis that undermines democratic institutions and weakens critical Western alliances such as NATO and the EU.”

Ranking Member Sen. Ben Cardin (MD) highlighted the impact of Russian disinformation campaigns in Ukraine in conjunction with the recent invasions of Crimea and the Donbas. He also noted the extent of Russian efforts to influence the 2016 presidential election in the United States, and observed that such disinformation campaigns take advantage of our democratic institutions to advance Russia’s strategic agenda.

Helsinki Commission Co-Chairman Rep. Chris Smith (NJ-04) characterized Russia’s disinformation efforts as a part of a strategy of “hybrid war,” and emphasized the need for the United States and its allies to develop counter-disinformation strategies as part of a “hybrid defense.”

### Internal Link – Balkans

#### Russia is using disinformation campaign to destabilize Balkans

**UK Prime Minister’s Office, 6-30-22**

(Prime Minister's Office, 6-30-2022, GOV.UK, "UK deploys military experts to counter Russian malign influence in Bosnia and Herzegovina", [https://www.gov.uk/government/news/uk-deploys-military-experts-to-counter-russian-malign-influence-in-bosnia-and-herzegovina accessed on 7-1-2022](https://www.gov.uk/government/news/uk-deploys-military-experts-to-counter-russian-malign-influence-in-bosnia-and-herzegovina%20accessed%20on%207-1-2022), HC)

Two experts in counter-disinformation and defence reform will work with the Bosnian Armed Forces and NATO to uphold peace and security in the country

UK will also provide funding to strengthen cyber security in Bosnia and Herzegovina, making the country more resilient to attacks

Russia is stirring violence and secessionism in the country to undermine the hard-won peace and destabilise the European continent

UK military specialists will be sent to Bosnia and Herzegovina to reinforce the NATO Mission and promote stability and security in the country, the Prime Minister has announced today (Thursday 30th June).

Bosnia and Herzegovina is currently facing the greatest existential threat in its post-war period, with secessionist leaders actively working to create further division and conflict. These plans are backed by Moscow as part of Putin’s drive to undermine both Bosnia’s Euro-Atlantic integration and its stability.

At the request of NATO Headquarters Sarajevo, a UK military counter-disinformation expert and a civilian strategic defence adviser will be deployed to support and train the Bosnia and Herzegovinian Armed Forces.

The counter-disinformation expert will bolster the NATO HQ and Bosnia and Herzegovina’s ability to resist malign influences – helping block Russian and other efforts to sow mistrust and undermine democracy in the country and region.

The new strategic defence adviser will support defence reform in the country, helping them to develop a modern, representative Armed Forces brought up to NATO standard.

In addition, the UK will provide £750,000 to establish a cyber-security centre of excellent within the University of Sarajevo. This will bolster Bosnia and Herzegovina’s defences against cyber attacks – which can hurt people both within and beyond the country. The UK will work closely with media outlets and Bosnian institutions to equip them with the tools to identify and mitigate the effects of lies and disinformation.

The Ministry of Defence is currently working with its Bosnian counterpart to keep the country rooted on a Euro-Atlantic trajectory, developing the capability and resilience the Bosnian Armed Forces need to tackle the security challenges they face.

The assistance recognises the UK’s leadership in countering malign influence and fostering security and stability. The UK has a longstanding commitment to peace and security in the region, starting in the 1990s when British soldiers formed an integral part of humanitarian efforts during the Bosnian War. UK troops have continuously served it the country ever since, helping it to rebuild and protecting and promoting peace.

The Prime Minister said:

We cannot allow the Western Balkans to become another playground for Putin’s pernicious pursuits. By fanning the flames of secessionism and sectarianism Russia seeks to reverse the gains of the last three decades in Bosnia and Herzegovina, gains that have brought more stability to our whole continent.

That is why we are stepping up support to Bosnia and Herzegovina, answering the call from our friends to help protect the peace they so rightfully deserve to enjoy.

In addition to military support to the Bosnian Armed Forces and NATO, the UK is working politically to uphold the historic Dayton Peace Accords. We have sanctioned those working to undermine rule of law in the country and last year the Prime Minister appointed a new Special Envoy to the Western Balkans to tackle serious and organised crime and other joint security challenges.

#### Russian and Chinese propaganda undermine democracies that have previously sustained peace throughout Europe

Janda, Czechia Chamber of Disputes Member, 20

[Jakub, 6-17-2020, Just Security, "Beware a China-Russia Nexus in Central Europe Amid US-EU Neglect,", https://www.justsecurity.org/70822/beware-a-china-russia-nexus-in-central-europe-amid-us-eu-neglect/, 7-2-2022, LASA-LR]

Until recently, Russian and Chinese influence across Europe generally reflected their distinct strategic aims. But their interests increasingly converge. Common to both Vladimir Putin’s and Xi Jinping’s strategies is the decoupling of the United States and Europe. Leaders on both sides of the Atlantic will have to act in concert – and fast – to forestall an even greater corrosion of the democratic norms that have kept the peace – or helped restore it, in the case of the wars in the former Yugoslavia – for three-quarters of a century.

Russia and China have made particular inroads in Central and Southeastern Europe in recent years. Putin’s government identifies dissatisfied segments of the public and the political class and maliciously exploits vulnerabilities via disinformation and related propaganda to exacerbate divisions, hinder democratic institutions, and generally neutralize the European space, particularly in the Balkans and the “Visegrad Four” countries of the Czech Republic, Hungary, Poland and Slovakia. Xi’s multiple and insidious charm offensives, on the other hand, have been comparatively apolitical, being less concerned about democratic or authoritarian governance and more aimed at bolstering the Chinese Communist Party’s global legitimacy, especially among political, business, and intellectual elites.

Neither Moscow’s nor Beijing’s approaches and tactics are mutually exclusive. Russian state, military, and religious leadership affirmatively engage aligned or sympathetic elites, while China uses media proxies to steer public discourse in its favor on its priority issues — Hong Kong’s autonomy, Taiwan’s de facto independence, and the human rights of China’s Uyghur and Tibetan communities.

To the delight of both Russia and China, the gradual weakening of U.S.-European ties over the last two decades is accelerating due to mutual neglect, miscommunication, and diminished policy coordination in a post-Cold War world. It hasn’t helped that the Trump administration’s approach to resolving inequities in NATO member defense-spending commitments or aspects of transatlantic trade relations has been nearly all vinegar and little wine. The result is rapidly diminishing support for partnership with America in key ally states such as Germany. According to a Pew Research poll in April, almost as many Germans prioritized their country’s relationship with China – 36 percent – as with the United States (37 percent). That was a significant change from a year earlier, when 50 percent of Germans preferred a closer partnership with the United States, compared with 24 percent favoring better ties with China.

Washington’s unhelpful bellicosity understandably alienates many Europeans, making it all the more difficult for their elected leaders to work jointly even on common interests. This reciprocal disengagement between Washington and key European capitals leaves room, in turn, for adversarial interventions by Russia and China.

## Plan Ideas

### Plan Concepts

#### Plan Concepts

* Alliance disinformation policy
* Security cooperation on disinformation
* Proactive
* Systemic – i.e. all levels
* Coordination
* Harmonization
* Intel sharing
* Broaden the mandate – coordination ev – to include internal coordination
* Preventive

#### Resolution

The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in one or more of the following areas: artificial intelligence, biotechnology, cybersecurity.

#### Coordinated, Proactive, System-Wide

The United States federal government should substantially increase coordinated cooperation with the North Atlantic Treaty Organization on proactive and system-wide counter-disinformation cyberspace initiatives.

### Student Ideas

#### Standards

The United States Federal Government should substantially increase its security cooperation with the North Atlantic Treaty Organization by proposing a set of standards for disinformation.

#### Vague

The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization by countering disinformation

#### Little more specific

The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization by integrating countermeasures to both domestic and foreign disinformation.

#### All levels

Resolved: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of cybersecurity by addressing disinformation at all levels.

#### Specs internal

Resolved: The United States federal government should substantially increase its security cooperation with the North Atlantic Treaty Organization in the area of cybersecurity by:

* ending internal disinformation campaigns
* developing a system-wide approach to debunking disinformation

#### Clark Evidence Idea

Plan: The United States federal government and the North Atlantic Treaty Organization, in an effort to substantially combat disinformation should implement

* Transparency policies
* Preemptive Information sharing
* Media literacy campaigns
* Increased private sector engagement and regulation
* Multilateral cooperation

## Solvency

### Proactive Solvency

#### Shift to proactive systemwide approach key to readiness

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 300, accessed 6-22-22, AFB]

Policy Recommendations

Update NATO’s Strategic Concept to incorporate a forward-looking approach to emerging security challenges including disinformation.

Disinformation changes shape, force-multiplies conventional capabilities and presents a threat to NATO’s foundational value system on an indefinite timescale. The challenge is anticipating and managing disinformation rather than eliminating it entirely, without overstating the threat.64 Disinformation also mirrors adversary thinking and offers a window into the goals and means of malign actors. NATO should develop a more holistic understanding of security that encapsulates shifts in information technologies and use of strategic narratives. NATO currently responds ex post to discrete, finite disinformation campaigns at the operational and strategic levels rather than preparing for the inherently unpredictable nature of threats in the emerging security environment. Recognizing that unconventional means could pose an existential threat to the Alliance, NATO’s updated Strategic Concept should remove the distinction between conventional and unconventional threats and emphasize that future threats will occur across the spectrum of peace to war. In other words, the Alliance should unambiguously recognize the security implications of non-military means. Effecting such a shift in NATO’s strategic thinking would improve overall readiness moving forward.

### Systemic Solvency

#### System-wide coordinated approach key to managing disinformation crises

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 304-305, accessed 6-22-22, AFB]

Develop a networked approach to security and resilience.

Collective security and the appropriateness of full-scale NATO responses came under deliberation as cyber aggression became a prominent tool of below-threshold warfare (on cyber challenges, see Blessing in this volume). Like cyberattacks, disinformation campaigns can be launched from anywhere by state and non-state actors, have little or no command structure, can be syndicated or promoted by entrepreneurial patriots, operate in networks, and are difficult to attribute. As the information sphere becomes the critical operational domain for hybrid warfare,83 the side that masters the network will almost certainly gain an advantage.84 Greater connectivity in NATO’s Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems also makes them higher value targets for disinformation, cyber, and physical attacks.85 For the first time in its history, the Alliance is facing challenges that require partnership with a variety of (private and civil society) actors to increase learning and situational awareness—including, most importantly, an understanding of the role that disinformation plays within an ensemble of influence tools and operations—but also establish a support system that can be mobilized in response to emerging security challenges.86 This will enhance NATO’s anticipatory thinking and its ability to quickly react as crises emerge.

NATO should also use its political dialogue mechanisms to create a coherent methodology across member nations. The Finnish and Swedish total defense and civil preparedness concepts are good models to draw upon at the national and multinational level.87 This could include the creation of institutional networks, society-oriented activities, infrastructure building, research, education, and training—tools that go beyond mere debunking and strategic communications. The Swedish model of psychological defense also includes crisis modelling drills for a variety of civil actors including media outlets.88

#### Comprehensive approach key to solving disinformation – systemic engagement and cooperation key to preventing the worst impacts of disinformation

**Clark et al. George Washington University Elliot School of International Affairs MA candidates, 04/12/22**

[Jesse Evans, Jessiica Brzeski, and Nash Miller, 04-12-2022, Russian Analytical Digest, "Russian Information Warfare", <https://doi.org/10.3929/ethz-b-000541999>, pages 17-19, accessed on 7-6-2022, hooch//cs]

This final article on Russian information warfare presents policy recommendations that can be adopted to combat and respond to information warfare. Each case study exhibits unique circumstances that illuminate potential policy options for counteracting Russian disinformation campaigns. After analyzing both the successes and failures in each case study, the **following policy recommendations emerged: transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation. These policy recommendations provide a broad framework for all countries facing a similar threat.**

1. **Transparency**

**The first policy that all governments, institutions, and agencies should adopt is transparency**. One of Russia’s goals is to weaken society by creating division and doubt about what is true and what is false. This is particularly evident when you examine how Russia has used information warfare to make average citizens question the legitimacy of their own governments and the information that they receive from them. Although a vital part of democracy is the freedom to question the information of a government**, Russia has exploited this to foment division and make people doubt the very legitimacy of their own governments** and whether they truly support the rule of law

**The best way to combat these efforts is by being transparent with the public, providing factual evidence that backs up an official government claim.** The United States has attempted this strategy through its intelligence community’s bid to shine a light on Russian disinformation campaigns in advance of the February 2022 invasion of Ukraine, sometimes before the events had even happened. Although met with uncertainty at first, **when many of these events eventually transpired, this strategy proved itself an effective tool for transparency.**

The European Union also seeks to be transparent with its populace by tracking and exposing examples of Russian disinformation on its website EUvsDisinfo, which currently has a database of over 13,000 cases. The EU emphasizes the explanatory rather than inflammatory nature of EuvsDisinfo, which is run by the body’s East StratCom Task Force. The EU values transparency and public awareness of disinformation above all else, and the organization publicly states on its website that no counter-information operations are conducted. **Information warfare is inherently based on lies, deception, and misdirection. For this reason, policy intended to counter it should focus on being as transparent as possible with the public in order to cut through the fog and build trust among citizens.**

1. **Preemptive Information-Sharing**

Another policy option that has thus far shown promising results in combating Russian information warfare is the use of preemptive information-sharing. **This policy option calls upon members of the government and intelligence community to preemptively release information to the public once the intelligence agencies are warned of a particular misinformation or disinformation campaign that Russia is planning to implement**. Preemptively warning about an upcoming Russian information operation alerts both the general public and foreign countries ahead of time, thus enabling them to prepare for and weaken Russia’s operation.

Currently, this strategy is successfully being implemented by the US in regard to Russia’s invasion and the Kremlin’s response to the global sanctions. **Two key examples that demonstrate its overall success include the US releasing intelligence that Russia was planning to use a false flag operation to justify the invasion and President Biden’s warning to American corporations that Russia was going to disrupt the US via a hacking campaign.** In both cases, **the policy of preemptive information-sharing informed the relevant parties and the public of the Kremlin’s antics, thus reducing the attack’s likelihood of success and giving actors time to steel themselves against it.**

**Other countries and multilateral organizations should employ this policy, as it essentially beats Russia at its own game.** By releasing reports that Russia intends to carry out a misinformation or disinformation attack, it makes the public aware of the threat, thereby making information warfare less effective because individuals in society are less likely to fall victim to the false narrative and propaganda slogans.

1. **Media Literacy Education**

Campaigns to promote media literacy can be a potent force in inoculating audiences against information warfare. **If given the proper intellectual tools, audiences can be taught to identify misinformation, independently fact-check, and compile trustworthy verified sources**.

**Latvia, which has been on the front line of Russian information warfare for years, has successfully used media literacy education at schools and universities**. Similarly, since the annexation of Crimea and invasion of the Donbass in 2014, Ukrainian civil society groups have successfully implemented a number of programs aimed at improving media literacy.

Universities, schools, and other organizations can conduct short courses or workshops for students, journalists, and political activists to effectively recognize misinformation. Civil society groups and journalist organizations have also found success in exposing and disproving Russian misinformation using verifiable facts. **Openly exposing misinformation narratives can drown out and delegitimize information warfare campaigns, and can be an effective alternative to censorship, which raises civil liberties concerns.**

As governments scramble to protect their populations from information warfare, media literacy education campaigns—**starting from an early age and conducted by balanced and trusted organizations—can have a major impact**.

1. **Private-Sector Engagement**

**Engagement with the private sector has shown itself to be a crucial aspect of countering Russian information warfare**. **Since many covert disinformation campaigns are conducted via social media, the corporations that run these websites and apps necessarily have a role to play in coordinating responses to this threat.** There are many schools of thought on how the public and private sector should interact within this space, with some arguing that the public sector should simply dictate policy to corporations and others advocating for allowing companies to self-regulate their content.

The European Union has opted for something in between, called co-regulation, and this model serves as a useful example for how states may approach policy to counter information warfare in a pragmatic way. The coregulation model seeks to find areas of potential cooperation with social media companies in a way that aims to foster goodwill and keep them on the side of governments in the fight against disinformation. The EU has attempted to implement this through its Code of Practice, which serves as a guide for how private companies should regulate disinformation in key areas such as political advertising and general integrity of services.

The Code of Practice is far from perfect: critics have noted that the progress companies make in tracking disinformation areas is largely self-reported and is not subject to strict enforcement. However, **it provides a helpful framework for how states and international actors can orient policy against disinformation in a way that includes the private sector. Large social media companies must be considered in any attempt to counter Russian information warfare due to how heavily the Kremlin relies on these media to conduct its information operations**. Many of these companies have a vested interest in regulating disinformation, but their concerns are primarily financial and are not inherently opposed to the idea of Russian-originated accounts stoking divisive topics on their platforms. **Policies that bring the private sector into the fold as a collaborator against disinformation, like the EU’s Code of Practice, are preferable to allowing corporations to be the sole arbiters of what should and should not be allowed on their platforms**.

1. **Multilateral Cooperation**

The scope of information warfare has evolved beyond the borders of one country, with impacts spreading globally. Therefore, **for a country to effectively combat information warfare of any type, a multilateral effort must be considered**. This entails countries coming together in creating effective solutions to combat information warfare by implementing standards and structures through shared experiences. **Not only does multilateral cooperation to combat information warfare strengthen efforts, but it also holds countries accountable in their own domestic processes.** Overall, **countries should make multilateral cooperation one of their key solutions to combating information warfare**

**In the case of Poland, binding obligations to multilateral security measures within the EU and NATO have strengthened domestic information security structures.** These include physical and legal implementations that help combat impending threats and destruction caused by Russian information warfare. **A desire to measure up to the legal standards of the EU and NATO has not only impelled the initiatives taken by Poland in the security realm, but also inspired domestic enterprise. In addition, as a member state of both organizations, Poland has also contributed to their information security**. Therefore, **a multilateral approach to Russian information warfare fosters greater accountability and ingenuity in combating the various associated threats**

**Multilateral cooperation in the face of information warfare will resolve a variety of issues when it comes to combating this evolving threat**. As globalization has spread, so too have the platforms and techniques of information warfare evolved to impact a series of actors ranging from online citizens to government institutions. The case study of Poland perfectly exemplifies why multilateral cooperation would benefit countries as they attempt to counteract the various derivative threats of information warfare. **An approach that seeks multilateral cooperation would strengthen the legal and physical structures of countries while implementing domestic accountability**. Of course, multilateral cooperation is not a perfect solution, **but it offers a pre-established platform that would provide the basis for further problem solving.**

**Conclusion**

As demonstrated in this series of articles, Russian **information warfare poses a massive threat to the future of democracy**. The danger lies in the Kremlin’s ability to use various methods and tools that target each nation differently, thus making a global response more difficult. That said, as laid out in the previous sections, the successes and failures of democracies around the world show which countermeasures work and, therefore, what policies should be adopted to limit Putin’s ability to further divide the democratic world**. By adopting transparency, preemptive information-sharing, media literacy campaigns, private-sector engagement, and multilateral cooperation, countries can combat information warfare while protecting vital civil liberties. Information warfare is here to stay and will continue to evolve as social media and the internet continue to change. Thus, states must develop strong responses now and prepare for future threats.**

#### Disinformation is the most common and one of the most dangerous forms of hybrid threats—NATO coordination and proactive approach key to solve threat escalation

**Center for European Policy Analysis, 21**

[7-28-2021, Center for European Policy Analysis, "Hybrid Warfare of the Future ", <https://cepa.org/hybrid-warfare-of-the-future-sharpening-natos-competitive-edge/>, accessed on 7-2-2022, MG]

Hybrid warfare combines military and nonmilitary as well as covert and overt means, such as disinformation, cyberattacks, economic coercion, lawfare, corruption, and irregular and regular forces. Hybrid methods are used to blur the lines between war and peace. They attempt to undermine target institutions and populations to achieve strategic aims. While these threats are not new, technological advancements and increasing global connectivity have recently expanded their speed, intensity, and scope. To more effectively tackle future hybrid threats from Russia, China, and non-state actors, the transatlantic community and NATO should improve in the following key areas.

Raise public awareness of hybrid threats. To counter hybrid threats, the transatlantic community must first understand what they are. Participants in the digital campaign considered disinformation and cyberwarfare to be the most common and pressing hybrid threats of today. On the other hand, there was less awareness of economic coercion, political subversion, and lawfare. Experts noted that while the existence of these threats is acknowledged individually, their use in conjunction makes them increasingly disruptive and their interconnectivity is underexplored. There is an urgent need to understand the impact of these threats on transatlantic societies and institutions and which hybrid actions are most likely to succeed or cause damage to allies in the future. Future hybrid threats that require more attention include weaponized corruption, automated armies, and biowarfare. 80% of respondents to a campaign poll believed NATO’s 2021 Brussels Summit Communiqué adequately prioritized hybrid threats.

Increase NATO’s speed of recognizing hybrid threats. Looking to the future, participants agreed the Alliance must be able to more quickly recognize and respond to hybrid campaigns before they can fully unfold and achieve their aims. This requires investing more in intelligence, surveillance, and reconnaissance capabilities; leveraging open-source information; and utilizing human-machine teaming to compete with adversaries that have more centralized, rapid decision-making than NATO. These capabilities can aid in the attribution of hybrid actions to their perpetrators, which are purposefully difficult to detect. To help the Alliance better recognize, conceptualize, and plan for hybrid threats, campaign participants suggested NATO consider a sixth “cognitive” or “human” domain of future warfare.

Get comfortable operating more proactively below the threshold of conflict. Hybrid threats often fall below NATO’s Article 5 threshold of armed attack laid out in its founding treaty. This makes it difficult for NATO member states to respond swiftly and appropriately in collective defense. NATO has already acknowledged that a serious cyberattack can trigger Article 5. But rather than waiting for today’s ongoing cyberattacks to escalate to that level, 93% of survey respondents agreed NATO must play a more proactive role in addressing below-threshold hybrid threats. For example, NATO could help coordinate more active and persistent cyber defense capabilities from nations, such as “hunt forward” teams. Under Article 3 of its founding treaty, NATO can also help nations mitigate the effects of hybrid threats by setting resilience standards and capability targets.

Build trust between governments, institutions, and publics. Survey respondents overwhelmingly agreed that national governments bear the most responsibility for countering hybrid threats. But their trust in officials and institutions to take such action varied greatly, with nearly 50% of respondents rating their trust levels at three on a five-point scale. This lack of confidence plays directly into the aims of adversaries’ hybrid campaigns, inhibits societal resilience, and undermines government response. NATO ally and partner publics should engage in more civil education campaigns and trust-building exercises to strengthen democracies against hybrid threats.

### Coordinated Solvency

#### Solvency – Strong, coordinated democracies are key to deterring the spread of disinformation

Polyakova, Center for European Policy Analysis President, 20

[Alina, 12-2-20, Center for European Policy Analysis President, , "Democratic Offense Against Disinformation,", https://cepa.org/democratic-offense-against-disinformation/, 7-2-2022, LASA-LR]

The intentional use of misleading information to influence societies, or disinformation, presents a serious threat to the integrity of democratic systems. Authoritarian states regularly use it to exploit democracies’ open information systems, presenting a significant national security threat that demands a purposeful and concerted response. This paper is the third in a series of papers that deals with how democracies can build resilience against disinformation. The first installment, Democratic Defense Against Disinformation,1 and its follow-up, Democratic Defense Against Disinformation 2.0,2 unpacked the challenge of foreign-origin disinformation and suggested practical steps to deal with it, including actions by governments, social media companies, and civil society. The core argument was that defense against disinformation has to be rooted in democratic principles and values: transparency, accountability, and respect for freedom of expression. We must not become them to fight them.

While domestic-origin disinformation is a more widespread (and growing) challenge, the tools to deal with foreign state-sponsored disinformation are broader. The Russian government was the first mover and innovator in exploiting the digital information environment to carry out influence operations against democracies, targeting the United States, Europe, and countries beyond.3

But while Russian interference in the 2016 U.S. elections awoke Americans and Europeans to the threat of disinformation, the response has not deterred the Kremlin, which has extended its efforts globally. Moreover, Russia is no longer the sole threat in the foreign influence game. The Chinese Communist Party (CCP) has far greater resources than Russia and a long track record of information manipulation and aggressive intervention in Taiwan and Hong Kong. With the Covid-19 pandemic, China entered the global disinformation space, targeting Europe, NATO, and the United States, working from the Kremlin’s playbook. There is now growing evidence that Russia and China are working together to amplify anti-democratic narratives.4

Democracies have aimed to identify, expose, and build greater public awareness of state-sponsored disinformation with the goal of building up greater long-term resilience to information influence operations.5 But the adversaries adapt and evolve their strategies and tactics to circumvent exposure and attribution. Companies, researchers, and governments are playing whack-a-mole — responding to each disinformation campaign as it arises while trying (and failing) to keep up with new threats. To get ahead of foreign disinformation, democracies must develop a proactive strategy to prevent state-sponsored information operations in the first place.6 That means getting off our back foot and getting on the offensive. This paper, written principally for the United States but hopefully applicable in adapted form to other countries, is a road map for how countries can get ahead of foreign disinformation. The new U.S. administration should lead the democratic community in this effort.

Alina Polyakova

Daniel Fried

icon-pdf

EXECUTIVE SUMMARY

The United States and other democratic countries have made progress defending against foreign and domestic disinformation. Unevenly, but steadily, a structure for democratic defense against disinformation is emerging, consistent with the principles of transparency, accountability, and respect for freedom of expression. It includes:

a growing network of disinformation detectors (led by civil society sometimes informed by government agencies);

social media companies (responsive to public and legislative pressure) that constrict disinformation on their platforms;

an informed media that exposes disinformation; and,

potentially at a next stage, a regulatory framework that seeks to filter out inauthentic and deceptive behavior.

While defensive measures cannot block all disinformation, they can limit disinformation as more people learn to filter it out on their own (“social resilience”).

But defense is working against a moving target. Purveyors of disinformation have grown more sophisticated and their tactics continue to advance. The line between domestic and foreign disinformation has blurred, with Russian agents using local actors as proxies to carry out disinformation operations. “Deepfakes” are progressing beyond the ability to detect such content in real time. China and other foreign players (Iran, for example) have also entered the disinformation game.

Defensive tactics based on democratic values can mitigate the impact of disinformation, but there remains a mismatch between the fast-evolving threat and the slow implementation of efforts to manage it.

We, therefore, recommend supplementing defense with offense. Our recommendations are designed for the United States; some may be adaptable by European governments and the European Union (EU) as well. Offense does not mean spreading disinformation (that would not be consistent with democratic values and democracies aren’t good at it anyway). It does mean building up:

Cyber tools to identify and disrupt foreign disinformation operations. The U.S. Cyber Command (USCYBERCOM) has already launched this option — the U.S. military terms it “hunt, surveil, expose and disable.” It has the appeal of immediacy and directness, but at its harder-edged end it has drawbacks. The “disable” option needs to be implemented with care.

Sanctions (and other financial) tools against disinformation actors and their sources of funding, and development of contingent retaliatory sanctions as a deterrent. Use of the sanctions tool requires persistence to apply well and its impact will be moderate rather than decisive. It will be more effective if carried out in parallel by the United States, the EU, and the United Kingdom.

Support for free media in the broad sense, including journalists, activists, and independent investigators, can be the most effective tool of counter-disinformation. It is asymmetric — it does not directly counter disinformation — but plays to the greatest strengths of free societies dealing with authoritarian adversaries: the inherent attraction, over the long run, of truth. This was a key lesson of the Cold War, when 20th century methods, e.g., support for independent radio broadcasting at Radio Free Europe/Radio Liberty (RFE/RL), proved effective in reaching societies inside the Soviet Union and Soviet Bloc. Today, updated technologies, including direct, although unofficial, support for activist journalists working both inside and outside Russia (and China) may become a 21st century equivalent. China’s media and internet landscape is more restrictive than Russia’s but options exist there as well. These activities can be slow to yield measurable results but can have strategic impact over time, if applied with creativity and determination.

The United States and, to some degree, the EU, NATO, and some European national governments, are already applying versions of these tools, but often haphazardly, without integrating them into a policy framework and with only spotty coordination. For the first two levels of tools, governments will have the lead; for the third, civil society groups will be critical and, in some cases, leading actors.

The new U.S. administration under President-elect Joseph R. Biden Jr. is likely to be more committed to developing a strategic response to disinformation, and be more effective generally, in crafting and implementing policies. U.S. President Donald J. Trump’s mixed signals with respect to Russian disinformation, attacks on free media, and distracting fights with European allies prevented a coordinated response and set the United States back.7 Recovering from these setbacks will not be easy, but the new Biden administration will have a roadmap for what to do.

#### With increasing tech innovation and disinformation it is NATO’s responsibility to invest in the protecting their democracies in the face of aggressive disinformation attacks

NATO Reflection Group 20

[NATO reflection group, 11-25-2020, NATO, https://www.nato.int/nato\_static\_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, Page 48, 7-2-2022, LASA-LR]

Strategic communications are a critical tool of deterrence and defence. Effective deterrence rests on clear projection of the ability and resolve to act if necessary. For some adversaries and challengers, information is now a domain of contest. The information environment is contorted by misinformation, disinformation, and deception from these actors. These techniques aim to disseminate manipulated information with the intent of undermining trust in democratic institutions. Disinformation, propaganda, and misinformation are especially dangerous in times of rapid technological advancements and when generational changes continue to alter perceptions of NATO among Allied publics.

The rapid pace of digitisation across all walks of life poses a particular challenge to NATO Strategic Communications. NATO and Allied audiences are increasingly drawing their information from, and are influenced by, information delivered via digital means. Strategic competitors continue to demonstrate their growing capability and will to deploy the latest digital technologies against NATO and Allies, particularly in the information environment. Building resilience across Allied populations is the primary responsibility of Allies themselves. However, across the board, Allies have not invested sufficiently in the human, technical, and financial resources required to engage in a consistent and sustained manner on issues related to security and defence. Neither have they prioritised proactive and consistent communications in support of Alliance aims and objectives. Recognising the threat posed by state and non-state actors who deploy aggressive tactics below the threshold of conventional force to challenge and undermine Alliance values and cohesion, NATO must ensure that it is aware and able to prevent and respond with objective and factual information.

### Resilience Solvency

#### Foregrounding disinformation and proactive threat management key to disinfo resilience

**Dolan, Lebanon Valley College political science professor & Intelligence and Security Studies Master’s program director, 6-8-22**

[Chris J., two-time Fulbright U.S. Scholar in international security in North Macedonia (2022) and Kosovo (2020), 6-8-2022, Just Security, "NATO’s 2022 Strategic Concept Must Enhance Digital Access and Capacities", <https://www.justsecurity.org/81839/natos-2022-strategic-concept-must-enhance-digital-access-and-capacities/>, accessed on 7-2-2022, MG]

This month in Madrid, the North Atlantic Treaty Organization (NATO) will update its Strategic Concept, the principal document that guides the alliance’s political-military strategy and collective defense operations. The war in Ukraine has put resilience in the face of Russian aggression front and center, especially in the cyber and information operation domains. Over the years, NATO has digitized and enhanced its security platforms, emphasizing interoperability of systems among its now 30 current member states. If NATO is to become more resilient against advanced persistent threats, hackers, and the maligned states that sponsor them, then the 2022 Strategic Concept must infuse multinational warfighting and deterrence against hybrid threats with methods that facilitate access to data and information sharing on its platforms and across multiple domains, namely in air, cyber, information, land, maritime, and space operations.

The Strategic Concept is among NATO’s most important documents as it informs alliance planning, resource allocation, and programming based on changes in the threat environment. But the document has not been updated since 2010. The 2010 Strategic Concept, entitled “Active engagement, Modern Defense,” contained just one brief sentence about cyber attacks and did not even mention China. It also stated that “Today, the Euro-Atlantic area is at peace,” even though Russia had invaded Georgia two years before and the threat of a return to great power competition loomed.

To argue that a lot has happened between 2010 and 2022 would be an understatement. Russia’s annexation of Crimea and intervention in the Donbas in 2014 and the invasion of Ukraine in 2022 shattered any illusions of a lasting peace with Russia. China’s territorial ambitions, economic assertiveness, threats against Taiwan, and military modernization threaten the rules-based order. Emerging technologies – in the form of hypersonic weapons, artificial intelligence, quantum computing, and machine learning – have intensified great power competition.

The 2022 Strategic Concept should highlight the essential role of technology in collective defense. To build greater digital capacity while also emphasizing resilience, NATO must adopt a new technological orientation on the military strategic level of command, especially within the Allied Command Transformation (ACT) in Norfolk, Virginia and the Allied Command Operations (ACO) in Mons, Belgium. ACT leverages advanced technologies for security and defense in capabilities, procedures, public-private partnerships, civil-military relations, and at NATO’s Centers of Excellence. Led by the Supreme Allied Commander Europe, ACO is responsible for collective defense through direction, requirements, planning, and execution at the strategic level.

However, the Strategic Concept 2022 should focus less on the emergence of new technologies and more on how NATO’s military and civilian personnel use them. ACO and ACT must emphasize greater accessibility to information and data for its multinational warfighters, cyber operators, and civilian professionals. NATO must reach out to experts in the private sector, academia, and non-governmental organizations to harness ways to expand access and emphasize flexibility in multi-domain operations. NATO can do this by providing more grants to private sector partners and establish a new center of excellence on data and information sharing.

ACO and ACT should also enable personnel and partners to readily access data and information in DIMEL domains: diplomatic, information/cyber, military, economic, and legal. This would expand the range of measures needed by ACT and ACO to connect and correlate deterrence with evolving hybrid threats. To deter hybrid threats across multiple domains, with enhanced access on different digital platforms, NATO members should develop smarter and lethal capabilities to confront threats from state and non-state actors. This would allow ACT and ACO to prepare for any contingency and respond to adversaries in battlefields and battlespaces.

The 2022 Strategic Concept encourages collaboration in the implementation of guidelines and procedures through a “plug-and-play” concept, in which platforms and systems are optimized for readiness and response at lightning speed. Plug-and-play is based on approaches used in commercial software that allow for innovation and easy access to networks and systems through secure platforms. The NATO School Oberammergau should offer platform training and education courses programs in mobile access for ACT and ACO personnel with appropriate security clearances. This would allow them to access the appropriate platform and utilize data and information necessary for their tasks and responsibilities.

For example, NATO’s Small Arms and Light Weapons (SALW) and Mine Action (MA) Information Sharing Platform contains rich and publicly available datasets on the roles played by the alliance in mitigating the illicit trade in small arms, tanks, aircraft, and naval vessels. It reports and updates NATO-funded projects to prevent adversaries from acquiring these weapons. However, the SALW-MA platform is outdated and not user friendly, impeding its functionality in practice.

Put simply, NATO’s ACT and ACO should focus as much on easing access to information as it does on advanced technologies and conventional weaponry. This would provide NATO with useful tools to access data and intelligence on the strategic, operational, and tactical levels and in land, sea, air, space, and cyber domains using devices and platforms that can seamlessly connect in different locations. But NATO Commands cannot simply expect its existing personnel to adapt. They must be trained and educated on a regular basis to use digital infrastructures in ways that make their jobs easier.

On the strategic level, the 2022 Strategic Concept must provide NATO’s political and military leaders with flexibility and resources to discern the diversity of hybrid threats in the environment. NATO’s strategic planners, cyber operators, and warfighters should be trained and educated in relevant digital platforms, access, and sharing data and information in ways that improve collaborative decision-making and collective defense. On the operations level, personnel must be given enough space to share data and intelligence as well as to train tactical level personnel on software that enables them to collect, analyze, process, and disseminate information quickly and easily across multiple domains.

Addressing these challenges is difficult for just one nation-state, let alone for all 30 NATO members. Therefore, the 2022 Strategic Concept should emphasize connectivity between member states in multi-domain operations and in collaboration with the private sector and academia. Accessibility to information and data sharing among NATO members should be securitized and harmonized.

The challenge for NATO is not necessarily adopting and investing in emerging and disrupting technologies for collective defense. Rather, the question is whether ACT and ACO can enhance accessibility to digital platforms and ease communications between platforms. Here, artificial intelligence (AI) can play a role in overcoming critical obstacles.

AI is now occupying a greater space in NATO’s collective defense orientation. The challenge in the 2022 Strategic Concept will be delineating the degree to which AI will enhance the ability of the alliance to analyze information and assess data. Moreover, AI is only as good as the data it relies on. To maintain its technological edge, in 2021 NATO released an Artificial Intelligence Strategy, a good step toward maximizing interoperability of weapons systems, improving infrastructure, and building resilient hybrid defenses. While it emphasizes collaboration with the private sector and academia, the strategy needs further refinement as AI would help NATO’s military and civilian personnel interlink devices on different platforms, perform rigorous data analytics, and quicken response time in response to a conventional or hybrid attack.

One innovation is the Defence Innovation Accelerator for the North Atlantic (DIANA). DIANA leverages partnerships among academics, technology companies, start-up firms to address the full spectrum of threats in the security environment. Private sector firms utilizing DIANA can access innovation sites and test centers that focus on artificial intelligence, machine learning, quantum computing, autonomous machines, and biotechnology. In the past, alliance members supported the creation and development of a venture capital Innovation Fund for technology companies and start-ups. The Strategic Concept should support the initiative with sustained public funds in ways that allow for strategic-level planning at ACO and ATO to communicate more effectively at the operational and tactical levels. DIANA and the Innovation Fund are models for the alliance.

An existing partnership that is proving effective is NATO’s collaboration with Klarrio, a firm that provides the alliance with innovative real-time data analytics and streaming services to combat disinformation and fake news. Klarrio has partnered with NATO’s Strategic Communications Center (StratCom) to assist the alliance in the information domain by streaming data analysis, processing, and applications analytics to identify and eradicate disinformation for NATO’s strategic-level planners. It supports and updates dashboard services to track suspicious activities in social media platforms, maintains an interactive user interface, generates analytical reports, and uses machine learning to analyze data and information.

The 2022 Strategic Concept must value partnerships and collaboration with the private sector to develop solutions to pressing collective defense challenges. Technology companies, academics, and start-ups can work with NATO military and civilian personnel to push solutions to multinational warfighters and cyber operators entrusted with protecting alliance members from both conventional military threats and hybrid attacks across multiple domains. This should not be difficult since the world’s most advanced capabilities, cutting-edge technology firms, and experts are in NATO member states.

NATO still will need advanced stealth F-35s, aircraft carriers, and tanks to wage war on the battlefield. However, NATO also needs digital tools that enable its fighters to readily access information and data in contemporary battlespaces. Whereas “battlefields” highlight land-based operations over others, “battlespaces” are not concerned with a specific arena. Access to data and information is a requirement for multi-domain situational awareness.

While it is difficult to predict how future geopolitical events will play out, NATO almost certainly will continue to have to manage threats from an aggressive and revisionist Russia, as well as a rising China. NATO should leverage the Strategic Concept in ways that emphasize access and flexibility against hybrid threats across multiple domains – this is contemporary resilience. Deterring hybrid attacks, whether in the form of cyber intrusions, disinformation through social media platforms, or maligned influence operations, demands that NATO protect its digital infrastructure and allow for greater accessibility to information and data necessary to operate in the gray zone of multi-domain spaces. A “whole-of-alliance” approach grounded on multinational collaboration and coordination, and centered on digital accessibility, will strengthen NATO resilience. Artificial Intelligence, China, Cybersecurity, Digital Access, NATO, Russia, Strategic Concept All-source, public repository of congressional hearing transcripts, government agency documents, digital forensics, social media analysis, public opinion surveys, empirical research, more.

### Tech Solvency

#### Technology is part of the solution – AI can help detect and track disinformation

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 298, accessed 6-22-22, AFB]

Technology is not only a tool in the hands of bad actors. AI and NLP have so far largely been utilized to detect fake news and disinformation and to support research into how disinformation spreads, what type of communities it reaches and map out rhetorical battlefields.55 Transatlantic militaries are also beginning to take an interest in how these tools might help with strategy and planning.

[Note – AI = artificial intelligence, NLP = natural language processing]

#### Old tactics are becoming obsolete, the digitization of disinformation makes new tactics necessary

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 2-3 https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

Propaganda, manipulation and misdirection have been long-standing tactics of diplomacy and international competition. In the last decade, and especially around the 2016 US Presidential election, ‘fake news’ and disinformation became buzzwords of sorts that led to a rediscovery of the role of information in political competition. The biggest difference between the traditional and more recent debates on the matter is the digitalization of information warfare and the subsequent scale, volume and speed advantages brought by this digitalization. The advent of Information and Communications Technologies (ICTs) brought about a faster information exchange medium where traditional gatekeepers like editors, censors or curators are of secondary importance and often irrelevant. While in more traditional media forms, broadcast is dependent on the approval of an intermediary individual or a group, with ICTs and social media, this approval is often hard to enforce with the sheer scale of information poured into such media venues. Although automated content moderation works in most cases, it can easily be circumvented.7 With information gatekeepers out of the way, information becomes disintermediated (reduction in the use of intermediaries), with information suppliers (citizen journalists or anyone with access to social media) directly able to reach information consumers around the world, in real time.8 The disintermediated nature of modern information exchange has rendered ICTs a conducive ground for misinformation (unintended spread of false information), disinformation (purposeful creation and dissemination of false information) and malinformation (deliberate use of accurate or inaccurate information with the purpose of harming an individual or people).9

### Democracy Solvency

#### Solvency - A full system approach solves for the suppression of dissenting opinions and marginalized voices.

Mckay and Tenove, The University Of British Columbia Vancouver; Centre for the Study of Democratic Institutions Research Associate and Political Science Postdoctoral Research Fellow, 20

(Spencer Mckay, The University of British Columbia Vancouver Centre for the Study of Democratic Institutions Research Associate, Chris Tenove, Chris Tenove, University of British Columbia Political Science Postdoctoral Research Fellow. SAGE Journals, 7-4-2020, "Disinformation as a Threat to Deliberative Democracy," Political Research Quarterly 2021, Vol. 74. No. 3, p. 706-707, https://journals.sagepub.com/doi/full/10.1177/1065912920938143, accessed 7-1-2022) SS:/

A systemic approach to deliberative democracy acknowledges that the quality of political communication will vary greatly in different spaces and at different times. Even the “unrestricted communication” of wild, informal public spheres is valuable because this is where “collective identities and need interpretations can be articulated with fewer compulsions than is the case in procedurally regulated public spheres” (Habermas 1996, 308). Deliberative systems can respond positively to non-deliberative activity, such as raucous protests that prompt public attention to demands from marginalized voices (Mansbridge et al. 2012, 19). However, it is possible for discourse in public spheres to be too wild, for transmission mechanisms to amplify rather than reduce deception and false claims, for failures of deliberation in empowered sites, and for other problems that undermine the quality of deliberation throughout the system. For instance, extremely “partisan and aggressive” protests can generate “a toxic atmosphere for deliberation and thus is not system enhancing over time” (Mansbridge et al. 2012, 20).

It is therefore necessary to understand when forms of communication may degrade a system. This topic has received relatively little attention from deliberative theorists.2 A systemic view suggests that communication may harm the functions of a deliberative system even if it is not obviously anti-deliberative at a micro level—that is, “manifestly disrespectful, strategic, and coercive” (Rollo 2017, 592). While intentional falsehoods and insults may be recognized as anti-deliberative by participants or observers of a conversation, other instances of anti-deliberative communication may only be detectable by looking at their effects across forums, later in time, or both.

### Deepfakes Solvency

#### Basic guardrails and ethics guidelines cooperation with services that provide deepfakes is key to limiting their malicious disinformation spreading capabilities

Fowler, Washington Post Technology columnist, 21

[Geoffrey A., 3-25-21, Washington Post, “Anyone with an iPhone can now make deepfakes. We aren’t ready for what happens next,” https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/, accessed 7-1-2022, LASA-LR]

Installing guardrails

Avatarify’s creator, Ali Aliev, a former Samsung engineer in Moscow, told me he’s also concerned that deepfakes could be misused. But he doesn’t believe his current app will cause problems. “I think the technology is not that good at this point,” he told me.

That doesn’t put me at ease. “They will become that good,” says Mutale Nkonde, CEO of the nonprofit AI For the People and a fellow at Stanford University. The way AI systems learn from being trained on new images, she says, “it’s not going to take very long for those deepfakes to be really, really convincing.”

Your smartphone photos are totally fake — and you love it

Avatarify’s terms of service say it can’t be used in hateful or obscene ways, but it doesn’t have any systems to check. Moreover, the app itself doesn’t limit what you can make people say or do. “We didn’t limit it because we are looking for use cases — and they are mainly for fun,” Aliev says. “If we are too preventive then we could miss something.”

Hany Farid, a computer science professor at the University of California at Berkeley, says he has heard that move-fast-and-break-things ethos before from companies like Facebook. “If your technology is going to lead to harm — and it’s reasonable to foresee that harm — I think you have to be held liable,” he says.

What guardrails might mitigate harm? Wombo’s CEO Ben-Zion Benkhin says deepfake app makers should be “very careful” about giving people the power to control what comes out of other people’s mouths. His app is limited to deepfake animations from a curated collection of music videos with head and lip movements recorded by actors. “You’re not able to pick something that’s super offensive or that could be misconstrued,” Benkhin says.

MyHeritage won’t let you add lip motion or voices to its videos at all — though it broke its own rule by using its tech to produce an advertisement featuring a fake Abraham Lincoln.

There are also privacy concerns about sharing faces with an app, a lesson we learned from 2019′s controversial FaceApp, a Russian service that needed access to your photos to use AI to make faces look old. Avatarify (also Russian) says it doesn’t ever receive your photos because it works entirely on the phone — but Wombo and MyHeritage do take your photos to process them in the cloud.

App stores that distribute this technology could be doing a lot more to set standards. Apple removed Avatarify from its China App Store, saying it violated unspecified Chinese law. But the app is available in the United States and elsewhere — and Apple says it doesn’t have specific rules for deepfake apps aside from general prohibitions on defamatory, discriminatory or mean-spirited content.

Labels or watermarks that make it clear when you’re looking at a deepfake could help, too. All three of these services include visible watermarks, though Avatarify removes them with a $2.50-per-week premium subscription.

Even better would be hidden watermarks in video files that might be harder to remove, and could help identify fakes. All three creators say they think that’s a good idea — but need somebody to develop the standards.

Social networks, too, will play a key role in making sure deepfakes aren’t used for ill. Their policies generally treat deepfakes like other content that misinforms or could lead to people getting hurt: Facebook and Instagram’s policy is to remove “manipulated media,” though it has an exception for parodies. TikTok’s policy is to remove “digital forgeries” that mislead and cause harm to the subject of the video or society, such as inaccurate health information. YouTube’s “deceptive practices” policy prohibits technically manipulated content that misleads and may pose a serious risk.

But it’s not clear how good of a job the social networks can do enforcing their policies when the volume of deepfakes skyrockets. What if, say, a student makes a mean joke deepfake of his math teacher — and then the principal doesn’t immediately understand it’s a fake? All the companies say they’ll continue to evaluate their approaches.

One idea: Social networks could bolster guardrails by making a practice out of automatically labeling deepfakes — a use for those hidden watermarks — even if it’s not immediately obvious they’re causing harm. Facebook and Google have been investing in technology to identify them.

“The burden here has to be on the companies and our government and our regulators,” Farid says.

### AT – Disinfo Shifts

#### Shifts in disinformation landscape are inevitable and unpredictable – nimble, proactive approach key to mitigating complex threats

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 299-300 accessed 6-22-22, AFB]

Shifts in the disinformation landscape might also come from unexpected—or underestimated—offline events such as the COVID-19 pandemic that create a global captive audience and a fertile ground for information operations. During the COVID-19 crisis, malign actors (in particular, Russia) utilized many recycled disinformation narratives combined with “traditional” propaganda.63 The emergence of new actors, in particular China as well as Iran, their resources, and their ability to deploy manipulative tactics seem to evolve faster than their actual technological prowess.

As transatlantic democratic actors are exploring the future of disinformation, the pace and scope of technological innovation will be crucial. But they will also have to grapple with more traditional tools of malign influence. It is yet unclear to what extent foreign authoritarian actors will have the ability to acquire and deploy new technologies at scale, especially as their media and digital deception machinery already seem successful. A key question is also whether deploying such technologies fits into the geopolitical strategies of malign actors and their approach to global competition. China in particular is an important actor that requires further monitoring. Its capabilities could potentially match doomsday scenarios about innovative technologies, but whether their deployment on a global scale is in China’s strategic interest is unclear. To deal with future threats, transatlantic partners and NATO specifically will have to consider disinformation in the context of the complex existing and emerging security threats in order to develop nimble and more proactive approaches.

#### Status quo approach flawed – bolstering cooperation and proactive counter-disinformation campaign key to deter authoritarian aggression and maintain the international order – collective approach key

Brown, Center for the Study of the Presidency & Congress Defense Studies senior fellow, 22

[Ethan, 11-year veteran of the U.S. Air Force as a Special Operations Joint Terminal Attack controller, contributor to the Diplomatic Courier, and has written for the Modern War Institute (West Point) and RealClearDefense, 1-25-22, The Hill, “The Cold War is over — we need a new playbook for Russia”, <https://thehill.com/opinion/international/591192-the-cold-war-is-over-we-need-a-new-playbook-for-russia/>, accessed 6-22-22, AFB]

NATO and the United States are failing to curb Russian aggression in the midst of the Ukraine crisis. By only using diplomatic forums, limited counter disinformation and continued economic aid to Ukraine while unilaterally engaging Russia, we are failing to meet the diversity of the effects of Russian aggression with our own diversity of deterrence.

NATO is a security architecture that still operates with a Cold War mentality — awkwardly sustaining hard power while ignoring the impact of hybrid methodologies despite recognizing them. The answers are already known, but not acted upon: double-down on the cooperation of liberal-minded states and fight disinformation with accurate and credible information that discredits Moscow.

Russia, of course, has been playing this game in Ukraine for some time. Hybrid warfare defies a single definition but consists of a state using multiple vectors of intelligence, information, cyber, conventional military and, at its core, political efforts to divide adversaries while avoiding open conflict. Hybrid warfare is indisputably how aggressor states subvert international stability, and states concerned with maintaining rules-based international order are not effectively responding to the threat that hybrid activities create.

What then, are the ways to deter this escalating threat and offset the capacity for instability by the future use of hybrid mechanisms? The problem lies in both the complexity of the adversary’s capabilities and the old dictum of a legitimate, rules-based body confronting a totalitarian regime: When fighting against a ruthless adversary, the arena forces one to become just as inhumane and ruthless — in which case, how are we different?

An important aspect that those abiding by rules-based order seem slow to realize and act upon is the aggressive use of exploitative information to discredit and isolate Russia. In short, credible, damning information is the inverse of disinformation. We live in a hyper-connected world where trust in legitimate institutions has wavered as a result of disinformation being used as a warfare activity. While intelligence activities have already shined a light on possible Russian false flags, to the surprise of no one concerned with the broader situation in Ukraine, it does not serve as fodder for delegitimizing Russian interference.

Military and cyber capabilities employed to highlight Moscow’s activities in the public forum are a vector of countering hybrid strategy that doesn’t fall into the aforementioned dictum of becoming like the adversary. Exploiting a figurative and literal flank in the Arctic to create an inversion of the Ukraine crisis for Moscow remains one vector that offers potential, but the West has been slow to utilize that active theater. Electronic warfare, the effects of which include collection and intelligence gathering, as well as interference against existing architecture, remains yet another medium of deterrent power in which Russia enjoys an advantage but one where the Western alliance can and should invest resources to disrupt.

While Russia moves across a variety of fronts to achieve political end-states (even if that iterative end state might simply be creating instability to justify intervention) the alliance remains reactive.

Following the Russian incursion into Crimea in 2014, the U.S. bolstered economic aid and arms exports to Kyiv. Economic sanctions have been so overused as to no longer serve as meaningful. As Moscow massed conventional power at sovereign borders — conventional military power still matters — the United States called for a summit. Even while attempting to seize the information initiative by releasing intelligence reports about Russian false flag operations pretexting an invasion, Moscow summarily denied the reports amidst declining future dialogue on defusing tensions. The situation is not advanced or improved by wavering commentary that fails to decry Moscow’s aggression.

Political solutions already exist — exemplified in the Pacific, where Japan is leading regional efforts to bolster collective security against Chinese aggression with the United States and Australia as key partners. It would be a mistake to immediately lob Beijing and Moscow into one monolith of counter-liberal power, but they should be viewed as similar, distinct problems with a common solution: unify the liberally minded states into a common front and make concerted efforts to reverse the effects of hybrid strategies.

This isn’t a new concept; it’s simply being ignored. Indeed, the very basis of hybrid warfare seeks to disaggregate collective institutions that challenge authoritarianism near its borders. This thinking is precisely why Moscow has exploited its generous authorities under the Collective Security Treaty Organization; the CSTO essentially recreates the Eastern bloc of the Soviet era, allowing Russia to insulate itself from perceived Western encroachment.

Rebuilding U.S. cohesion within the NATO and EU alliances is critical. These relations have been fractured further by the United States leading a unilateral approach to negotiations with Russia, largely excluding the rest of the alliance and Ukraine from the ineffective diplomatic process. The EU, whose presidency has recently been assumed by French leadership bent on reducing integration with the U.S., is hardly a cohesive unit capable of effectively deterring Russian aggression on the European continent.

Thus, an aggressive engagement to rebuild relationships and unity in the region — combined with actions that bolster democratic credibility, highlight unacceptable activities by aggressors and solidify the fragile status of the Atlantic alliance — are the obvious course forward. Yet it seems that the United States and NATO are failing to realize this reality before possible conflict breaks out.

#### Current approach is playing whack-a-mole – need proactive approach to counter-disinformation

Ling, investigative journalist, 22

[Justin Ling, works in journalism as an investigative journalist whose areas of interest include, misinformation, extremism and national security, 5-21-2022, Center For International Governance Innovation Online, "NATO Should Elevate Its Cyber Game, and Quickly", <https://www.cigionline.org/articles/nato-should-elevate-its-cyber-game-and-quickly/>, accessed on 7-2-2022, MG]

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.”

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. 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.

### AT – Attacker Has Advantage

#### The attacker’s advantage is not absolute if the defender can signal its debunking capacity and rally the international audience by reducing its engagement in its own disinformation campaigns.

Ünver, Özyeğin University Department of International Relations Associate Professor, and Ertan, Boğaziçi University, Department of International Trade Assistant Professor, 22

(Akin Unver, Ozyegin University Department of International Relations Associate Professor, Arhan S. Ertan, Bogazici University, Department of International Trade Assistant Professor, Social Science Research Network, 5-2-2022, "The Strategic Logic of Digital Disinformation: Offense, Defence and Deterrence in Information Warfare," p. 19-20, https://dx.doi.org/10.2139/ssrn.4098988, accessed 7-5-2022) SS:/

Our model posits that deterrence in international information war can be attainable through two venues: first, if the Defender can successfully signal its debunking capacity to the Attacker, and second, if the Defender can demonstrate its ability to rally the international audience to its cause quickly enough. The first condition is attainable through building and maintaining a robust fact-checking ecosystem either within the government ranks, or the civil society, but ideally both. If a Defender regularly demonstrates rapid and successful debunking performance in past interactions, the Attacker’s valuation of its short-term utility by deploying disinformation will likely be reduced. Since one of the core drivers of disinformation is the Attacker’s high valuation of its short-term demobilizing and distracting potential against its adversaries, those adversaries can in turn demonstrate that they can debunk and disseminate accurate news rapidly in order to reduce the Attacker’s perceived payoffs.

The second condition is attainable through diplomatic alliances, media and cultural power, and fewer reliance on fake news as a government strategy in past information interactions. If the Defender has regularly used disinformation as a conscious strategy in past interactions – more so compared to the Attacker – it will be harder for the IA to rally behind the Defender’s cause. To that end not resorting to disinformation is a cumulative resource that countries ‘save’ over time, and can ‘cash-in’ during emergencies, by rendering the IA more receptive towards its cause.

This chapter has identified two important dynamics. First, the fact that disinformation may incur reputational and suspicion costs to the Attacker suggests that there must be greater short-term gains for the Attacker so that it prefers spreading fake news. This reasoning advances the prevalent wisdom that states engage in disinformation because it is a cheap way of demobilizing an adversary and there are no repercussions against this form of action. Second, Defenders are not as completely vulnerable to disinformation campaigns as the mainstream debate suggests and the Attacker’s advantage in information warfare is no absolute. The Attacker chooses to engage in organized disinformation because it believes that the Defender will not be able to debunk these claims on time and at scale. If the Defender demonstrates the opposite reliably, then the Attacker’s decision to launch a disinformation campaign is not a given and automatic, and may be deterred from choosing this course of action. In addition, the Defender may deter the Attacker through its influence over the IA, by not regularly engaging in disinformation campaigns itself and optimizing its cultural and media power, which accumulates over time, through ‘good practices’.

We expect a number of criticisms on our model. First, we concede that the Defender may not be isolated into a single decision to automatically debunk all disinformation attempts. It can indeed choose not to take action, or spread disinformation itself to win the short-term information war. This is indeed an important point, but empirically, such cases have been so rare that modelling them within the same parameters of likelihood with the rest of our model can be misleading. Second, we anticipate that our decision to include the International Audience as a decision-making actor may incur too much agency on it, as in most cases IA’s likelihood of believing disinformation or not is very deterministic: if the Attacker is skilful and can generate sufficient emotional triggers, the IA has a likelihood of believing the disinformation. Also, pre-existing beliefs about the Attacker and the Defender matters significantly in driving the momentum of the IA. However, we believe that the IA is the actual kingmaker in this interaction and its gravitational dynamics impact the outcome of the information war. To that end, we favour retaining the agency of the IA.

### AT – Internal Disinfo Alt Cause

#### NATO itself can coordinate to upgrade national safeguards against democratic backsliding

Becker, US Military Academy International Relations professor, et al., 6-28-22

(LTC Jordan, Douglas,Former North Atlantic Council Permanent United States Representative, and Simon, Staffordshire University Defense Studies Editor-In-Chief Associate Professor, 6-28-2022, War on the Rocks, "Don’t Let Russia Dominate the Strategic Concept - War on the Rocks", https://warontherocks.com/2022/06/dont-let-russia-dominate-the-strategic-concept/, accessed on 7-6-2022, SR)

Although defending human and physical infrastructure from asymmetric threats is inherently national business, **NATO itself can serve as a platform for coordinating allied responses to these challenges.** NATO allies agreed on seven baseline requirements for national resilience at their 2016 Warsaw Summit. They have also “improve[d] their cyber resilience by introducing capability targets” into the NATO Defence Planning Process.

Recently, however, national resilience has been challenged in additional areas, which should be reflected. Specifically, NATO should address democratic backsliding, election interference, and economic and information manipulation. Specifically, **NATO’s requirements for national resilience should be upgraded to require national safeguards against democratic backsliding.** Prior to taking up her position as the senior U.S. Department of Defense official in Europe, Rachel Ellehuus highlighted the vulnerabilities laid bare by such backsliding and argued that “the trans-Atlantic alliance will only remain strong if members genuinely abide by its founding principles.” By incorporating such safeguards into NATO’s systems for monitoring allies’ defense preparations, allies can shape one another’s political, economic, and security incentives in ways that reduce these vulnerabilities.

### AT – Aff Can’t Solve without Private Sector Involvement

#### Improving NATO’s capacity to handle disinformation will improve response rate and make it more capable of utilizing private sector tools to identify and attribute disinformation

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 303-304, accessed 6-22-22, AFB]

Establish mechanisms for regular consultation with the private sector.

Attribution is inherently difficult, but enhancing NATO’s capacity will increase the Alliance’s speed of response to disinformation and mitigate risks to conventional capabilities. NATO’s newly-launched Defense Innovation Accelerator and regular talks with private-sector actors could improve NATO’s capacity to attribute sources of disinformation, encourage operational resilience, integrate innovative solutions, and design regulations and interventions to secure critical infrastructure (including in information and telecommunications) and investment screening.77 Promising new tools coming predominantly from the private sector include machine learning to remove fake social media accounts, blockchain technology for secure digital identity systems,78 24/7 disinformation monitoring systems driven by artificial intelligence,79 and software to detect deepfakes.80 Transatlantic civil society actors have also developed a variety of tools for tracking malign narratives and tactics, and have already piloted technological innovations that could help deepen NATO’s broader understanding of the threat.81 New technologies pose inherent risks but also significant opportunities to enhance security through an operational approach to innovation.82

# AFF Off-Case Answers

## Topicality

### Topicality – Cyber

#### Disinformation is a facet of cyber warfare

**Szabó, security engineer & International Centre for Migration Policy Development research intern, 22**

[Réka Szabó, works for the International Team for the Study of Security Verona in the International Centre for Migration Policy Development as a research intern, 6-18-2022, International Team for the Study of Security Verona, "Cyber Warfare in the Ukrainian Conflict — a Determinant of the Outcome of the War?", <https://www.itssverona.it/wp-content/uploads/2022/06/Reka-Szabo.pdf>, p. 4, accessed on 7-2-2022, MG]

In cyber warfare, damage can be done in both physical and cognitive spheres. To achieve such damages, cyberspace can be used in multiple ways. It embodies software, hardware, and infrastructure as well. Information war has a broader scope, and can mean “a wide array of activities […], the spreading of disinformation, electronic warfare, the degradation of navigation support, psychological pressure, and the destruction of adversary computer capabilities.”5 Overall, cyber warfare can be applied for offensive and defensive purposes.

In observing Russian cyber warfare-related practices today, experts6 claim that the legacy of the Soviet Union is still evident. There are operations in cyberspace that strive for the alteration/influence of policies of other nations, in a secret way, using illegal means. The manipulation of information is a way of doing this. Another example of operations that can be paralleled with Soviet-era methods is the one that encompasses concealment and deception so that the other party makes mistakes because of false pieces of information. Cyberattacks used in the current conflict can be classified into three main categories. One group is called wipers. Such attacks delete information from networks or block data. Another type of cyberattack is DDoS (Distributed Denial of Service) attacks. These impede the access of websites, by “overwhelming a system via an excessive number of ‘requests’ — people trying to access a website — in a short space of time.” 7 Defacement attacks, on the other hand, operate on the psychological or cognitive level: they eliminate or modify pieces of information from websites, thus facilitating the dissemination of disinformation and fake news.8

### Topicality – Disinformation

#### Disinformation refers to the digital space

Ünver, Özyeğin University Department of International Relations Associate Professor, and Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, 22

(Akın Ünver, Özyeğin University Department of International Relations Associate Professor and Ahmet Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, All Azimuth, 6/15/2022 “Securitization of Disinformation in NATO’s Lexicon: A Computational Text Analysis,” p. 4, https://doi.org/10.20991/allazimuth.1110500 https://www.allazimuth.com/wp-content/uploads/2022/06/Unver-and-Kurnaz\_SecuritizationofDisinformation.pdf, accessed 7-1-2022) SS:/

Over the last few years, defining misleading content and measuring the legitimacy of its dissemination have been at the forefront of journalistic, political, and scientific debates.24 Even before its proliferation in 2016, disinformation was a widely-used term in mainstream discourse, co-existing with other terms such as infoglut, or information overload.25 While disinformation and misinformation were first used interchangeably, today, disinformation refers to the deliberate dissemination of false information with the intention of misleading and confusing an audience. Misinformation, on the other hand, strictly refers to the unintended diffusion of false information without malintent. There are also bridge terms such as ‘malinformation’, which refers to information that is factually accurate but is deployed to damage the image of an individual or an entity, or the concept of ‘problematic information’ as defined by Caroline Jack.26 Although it is not directly mentioned, all of these concepts refer to the digital space, where information manipulation is disseminated faster and more broadly on social media and digital communication technologies as compared to other forms of media.

#### Disinformation/misinformation and hybrid war are similarly constructed threats – focusing on distinctions clouds effective discourse

Ünver, Özyeğin University Department of International Relations Associate Professor, and Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, 22

(Akın Ünver, Özyeğin University Department of International Relations Associate Professor and Ahmet Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, All Azimuth, 6/15/2022 “Securitization of Disinformation in NATO’s Lexicon: A Computational Text Analysis,” p. 4-5, https://doi.org/10.20991/allazimuth.1110500 https://www.allazimuth.com/wp-content/uploads/2022/06/Unver-and-Kurnaz\_SecuritizationofDisinformation.pdf, accessed 7-1-2022) SS:/

Over the last few years, defining misleading content and measuring the legitimacy of its dissemination have been at the forefront of journalistic, political, and scientific debates.24 Even before its proliferation in 2016, disinformation was a widely-used term in mainstream discourse, co-existing with other terms such as infoglut, or information overload.25 While disinformation and misinformation were first used interchangeably, today, disinformation refers to the deliberate dissemination of false information with the intention of misleading and confusing an audience. Misinformation, on the other hand, strictly refers to the unintended diffusion of false information without malintent. There are also bridge terms such as ‘malinformation’, which refers to information that is factually accurate but is deployed to damage the image of an individual or an entity, or the concept of ‘problematic information’ as defined by Caroline Jack.26 Although it is not directly mentioned, all of these concepts refer to the digital space, where information manipulation is disseminated faster and more broadly on social media and digital communication technologies as compared to other forms of media.

As the terms ‘disinformation/misinformation’, ‘fake news’, ‘information operation’, and ‘hybrid war’ are often used interchangeably in political discourse, there are little clear-cut differences in the strategic meaning of each word choice.27 Politicians and leaders often use these terms as a bag of buzzwords without a clear operational definition of what each term precisely means. All of these buzzwords generate roughly the same effect, the delegitimization of their target, on consumers of such messages.28 Especially problematic is the \*fact that once the discourse on disinformation is weaponized to delegitimize rivals, there is very little such rivals can do to defend themselves. Given the significant political charge of these terms, individuals or institutions that are alleged to be engaging in disinformation-related activities often have to enter into a fruitless spar of words to challenge such allegations, which usually leads to further controversy. This renders the accuser – or the side that securitizes disinformation – more advantageous compared to the accused, generating a dynamic similar to the ‘attacker’s advantage’ in cyber security, where the defender is continuously blindsided.29

#### NATO uses disinformation, misinformation, hybrid war and ‘fake news’ interchangeably.

Ünver, Özyeğin University Department of International Relations Associate Professor, and Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, 22

(Akın Ünver, Özyeğin University Department of International Relations Associate Professor and Ahmet Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, All Azimuth, 6/15/2022 “Securitization of Disinformation in NATO’s Lexicon: A Computational Text Analysis,” p. 10, https://doi.org/10.20991/allazimuth.1110500 https://www.allazimuth.com/wp-content/uploads/2022/06/Unver-and-Kurnaz\_SecuritizationofDisinformation.pdf, accessed 7-1-2022) SS:/

A longitudinal analysis of the specific keywords sorted by document type reveals a clear difference in word choice between different NATO documents. In NATO Basic Texts, the most-preferred reference keyword is ‘hybrid warfare’, whereas in press releases, reliance on the word ‘misinformation’ gradually evolves into ‘disinformation’ by 2018. NATO reviews also largely prefer ‘misinformation’, but NATO speeches and tweets are more diverse, with a heavier use of the terms ‘propaganda’, ‘disinformation’, and ‘fake news’. This difference is an interesting demonstration of how elastic these terms are and how different institutional cultures and outlets can prefer one over the other in their communication strategies.

### Topicality – Artificial Intelligence

#### AI is used to track disinformation

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 298, accessed 6-22-22, AFB]

Technology is not only a tool in the hands of bad actors. AI and NLP have so far largely been utilized to detect fake news and disinformation and to support research into how disinformation spreads, what type of communities it reaches and map out rhetorical battlefields.55 Transatlantic militaries are also beginning to take an interest in how these tools might help with strategy and planning.

[Note – AI = artificial intelligence, NLP = natural language processing]

## US Key

### US Key – Alliance Strength

#### US key – Rebuilding Atlantic alliance cooperation key to deterrence – Europe does not have the strength to deter Russia on its own

Brown, Center for the Study of the Presidency & Congress Defense Studies senior fellow, 22

[Ethan, 11-year veteran of the U.S. Air Force as a Special Operations Joint Terminal Attack controller, contributor to the Diplomatic Courier, and has written for the Modern War Institute (West Point) and RealClearDefense, 1-25-22, The Hill, “The Cold War is over — we need a new playbook for Russia”, <https://thehill.com/opinion/international/591192-the-cold-war-is-over-we-need-a-new-playbook-for-russia/>, accessed 6-22-22, AFB]

Political solutions already exist — exemplified in the Pacific, where Japan is leading regional efforts to bolster collective security against Chinese aggression with the United States and Australia as key partners. It would be a mistake to immediately lob Beijing and Moscow into one monolith of counter-liberal power, but they should be viewed as similar, distinct problems with a common solution: unify the liberally minded states into a common front and make concerted efforts to reverse the effects of hybrid strategies.

This isn’t a new concept; it’s simply being ignored. Indeed, the very basis of hybrid warfare seeks to disaggregate collective institutions that challenge authoritarianism near its borders. This thinking is precisely why Moscow has exploited its generous authorities under the Collective Security Treaty Organization; the CSTO essentially recreates the Eastern bloc of the Soviet era, allowing Russia to insulate itself from perceived Western encroachment.

Rebuilding U.S. cohesion within the NATO and EU alliances is critical. These relations have been fractured further by the United States leading a unilateral approach to negotiations with Russia, largely excluding the rest of the alliance and Ukraine from the ineffective diplomatic process. The EU, whose presidency has recently been assumed by French leadership bent on reducing integration with the U.S., is hardly a cohesive unit capable of effectively deterring Russian aggression on the European continent.

Thus, an aggressive engagement to rebuild relationships and unity in the region — combined with actions that bolster democratic credibility, highlight unacceptable activities by aggressors and solidify the fragile status of the Atlantic alliance — are the obvious course forward. Yet it seems that the United States and NATO are failing to realize this reality before possible conflict breaks out.

## US-EU Coop CP Answers

### Coop Fails

#### The U.S. and EU have fundamentally different approaches to countering disinformation, making it completely impossible to cooperate

Ignatidou, Chatham House International Security DepartmentAcademy Stavros Niarchos Foundation Fellow, 19

[Sophia, 9-19, Chatham House, " EU–US Cooperation on Tackling Disinformation", https://www.chathamhouse.org/sites/default/files/2019-10-03-EU-US-TacklingDisinformation.pdf, Page 34, Accessed 7-6-22, LASA-LR]

The EU and US diverge in terms of constitutional and human rights priorities – e.g. freedom of expression vis-à-vis privacy or surveillance and security – and the trade-offs they have settled with feed into their non-aligned approach to disinformation. Aggravating the complexity of coordinating regulatory efforts is the fact that the debate in the US revolves around freedom of expression and the framing of efforts to constrain the power of Big Tech as being anti-free market, when in the EU freedom of expression is a qualified right that has to be balanced with other rights such as privacy.169 The EU sees regulation as mainly a systemic issue and seeks to address disinformation by looking across different domains, from tech regulation to privacy frameworks and information markets, while the US institutional approach indicates an interpretation as an agent problem and allocates responsibility to federal agencies to focus on manipulation campaigns of state actors like Russia, Iran or China. Nevertheless, investigations launched this year by US Congress committees and the FTC, indicate the tide may be changing and a window of opportunity for alignment may manifest.

## EU CP Answers

### Solvency Deficit – US Key – EU Alone Won’t Solve

#### NATO cohesion key to deterrence – EU alone does not have the strength or cohesion to deter Russia

Brown, Center for the Study of the Presidency & Congress Defense Studies senior fellow, 22

[Ethan, 11-year veteran of the U.S. Air Force as a Special Operations Joint Terminal Attack controller, contributor to the Diplomatic Courier, and has written for the Modern War Institute (West Point) and RealClearDefense, 1-25-22, The Hill, “The Cold War is over — we need a new playbook for Russia”, <https://thehill.com/opinion/international/591192-the-cold-war-is-over-we-need-a-new-playbook-for-russia/>, accessed 6-22-22, AFB]

Political solutions already exist — exemplified in the Pacific, where Japan is leading regional efforts to bolster collective security against Chinese aggression with the United States and Australia as key partners. It would be a mistake to immediately lob Beijing and Moscow into one monolith of counter-liberal power, but they should be viewed as similar, distinct problems with a common solution: unify the liberally minded states into a common front and make concerted efforts to reverse the effects of hybrid strategies.

This isn’t a new concept; it’s simply being ignored. Indeed, the very basis of hybrid warfare seeks to disaggregate collective institutions that challenge authoritarianism near its borders. This thinking is precisely why Moscow has exploited its generous authorities under the Collective Security Treaty Organization; the CSTO essentially recreates the Eastern bloc of the Soviet era, allowing Russia to insulate itself from perceived Western encroachment.

Rebuilding U.S. cohesion within the NATO and EU alliances is critical. These relations have been fractured further by the United States leading a unilateral approach to negotiations with Russia, largely excluding the rest of the alliance and Ukraine from the ineffective diplomatic process. The EU, whose presidency has recently been assumed by French leadership bent on reducing integration with the U.S., is hardly a cohesive unit capable of effectively deterring Russian aggression on the European continent.

Thus, an aggressive engagement to rebuild relationships and unity in the region — combined with actions that bolster democratic credibility, highlight unacceptable activities by aggressors and solidify the fragile status of the Atlantic alliance — are the obvious course forward. Yet it seems that the United States and NATO are failing to realize this reality before possible conflict breaks out.

### Permutation Solves Best

#### Permutation solves best – both sides have unique expertise – security component means NATO involvement necessary to reduce threats

Rebegea, Center for European Policy Analysis Democratic Resilience Director & Schmiedl, Center for European Policy Analysis Senior Program Officer, 21

[Corina & Carsten, In 2020, Schmiedl served as Advisor to the U.S. representative and co-chair of the NATO Reflection Group, 2022, NATO 2030 Towards a New Strategic Concept and Beyond, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, edited by Jason Blessing, Katherine Kjellström Elgin, Nele Marianne Ewers-Peters, “Chapter 13 War by Other Means: Securing NATO Against Disinformation in the Coming Decade”, <https://www.sais.jhu.edu/kissinger/nato-2030-towards-new-strategic-concept-and-beyond>, p. 303-304, accessed 6-22-22, AFB]

Enhance cooperation with the EU and other national authorities on disinformation by creating a unique contact point.

NATO is the main force shaping European and transatlantic security. It needs to be involved in advancing thinking and planning for future threats, but also participate in setting norms and standards in cooperation with other actors. NATO and the European Union have an established format of cooperation spanning several critical domains, including hybrid threats.75 This should expand to include disinformation. With the emerging COVID-19 “infodemic” in 2020, disinformation and propaganda already became a source of increased coordination between NATO and the EU, mainly because the latter already had mechanisms in place and considerable experience in tracking Russian disinformation and propaganda. NATO should establish a unique contact point and a formal process of consultation and coordination with the EU’s counterpart which specializes in dealing with information operations. In addition, NATO should be part of the transatlantic conversation on regulations and laws (mainly spearheaded by the EU), particularly for the thriving information manipulation industry that allows malign actors to hide their tracks behind fake engagement.76

#### NATO and EU already have their own ways of checking disinformation - they can cooperate with each other in a cohesive way that allows for both organizations to solve better through cooperation

Wrobel, Emerging Europe Technology and Innovation Journalist, 20

[Andrew, 6-5-2020, Emerging Europe, "NATO and the EU: Tackling disinformation in partnership,", https://emerging-europe.com/news/nato-and-the-eu-tackling-disinformation-in-partnership/, Accessed 7-7-2022, LASA-LR]

The common challenges of disinformation and fake news have led to enhanced NATO – EU cooperation, with both organisations acknowledging that disinformation, propaganda, and fake news are challenges that put increasing pressure on the resilience of democratic systems.

This trend has increased during the pandemic, as state and non-state actors have exploited the current situation to further their own interests by trying to sow divisions and undermine liberal societies and democracies. The fight against disinformation is more important than ever as the pandemic intensifies competition between different political models, testing the strength of democratic systems and the values of human rights across the world. If left unchecked, these trends risk undermining the foundations and legitimacy of the rules-based international order.

In several instances, in the context of the pandemic, disinformation has been aimed at eroding trust in the readiness of NATO troops in Central and Eastern Europe. As such, raising awareness and strengthening collective defences against sources of disinformation and the hostile actors behind them has become critical.

In this context, the importance of enhanced NATO – EU cooperation on countering disinformation and propaganda has been highlighted by both institutions, and several measures aimed at countering these trends have already been identified and implemented.

The EU has set up a Rapid Alert System among EU institutions and member states in order to spot and tackle coordinated disinformation campaigns. The EU has also worked closely with big internet platforms to sign up to a Code of Practice on Disinformation, asking them, among other things, to disrupt the advertising revenues of those behind disinformation, take greater action against bots, and make political advertising more transparent.

NATO meanwhile is also closely monitoring disinformation and countering it with democratic values and facts. NATO is continuing to work with all of its allies as well as partners to identify, expose and counter disinformation.

Both NATO and the EU have stressed the need to support free independent media, a key building block of democratic systems. Other key pillars in the fight against disinformation are governments and international organisations, which must call out disinformation and counter it with facts, and citizens, who must learn to understand hostile information and to check that their news and information comes from reliable sources.

#### EU- NATO cooperation is already present, but further cooperation between the two organizations is necessary for long term mitigation of rising threats.

Wrobel, Emerging Europe Technology and Innovation Journalist, 20

[Andrew, 6-5-2020, Emerging Europe, "NATO and the EU: Tackling disinformation in partnership,", https://emerging-europe.com/news/nato-and-the-eu-tackling-disinformation-in-partnership/, Accessed 7-7-2022, LASA-LR]

NATO – EU cooperation and coordination has never been closer, especially when it comes to countering hybrid threats, disinformation and cyberattacks. The current crisis has further reinforced the importance of cooperation and partnership, and the necessity to access the idle potential of synergies. This makes further cooperation possible, and indeed highly likely.

Enhanced cooperation on resilience between the EU and NATO could result in the short-term in a standardising of procedures and methods, in the medium-term in a joint assessment and awareness of threats and trends emerging on the event horizon, while in the long-term, it might lead to a coordinated response to a problem that shows no signs of abating.

## Canada CP Answers

### Canada CP Answer – Perm Do Both

#### Canada should work with US to exert its power

Gecelovsky, Professor Economics, University of Windsor, 21 (Paul, “CHAPTER 4 In Search of Canada’s International Identity in an Emerging Order”, in The Palgrave Handbook of Canada in International Affairs, Edited by Robert W. Murray and Paul Gecelovsky, https://www.researchgate.net/profile/Heather-Exner-Pirot/publication/353047113\_Canada%27s\_Arctic\_Foreign\_Policy/links/60e60d300fbf460db8ed865a/Canadas-Arctic-Foreign-Policy.pdf#page=81

Canada also has to participate actively in the creation of the emerging international order, especially in fora with the US and PRC, individually or together. Clark (2014, 6) notes that “the ability to bridge conflicting identities and hostile groups, and patiently seek enough common ground to build trust and collaboration, is critically needed,” and “no one is better at it than Canada”. Canada needs to build on its reputation as a ‘helpful fixer’ or ‘mediator’ to construct coalitions of like-minded state and non-state actors on issues of importance (see Nagy, Chapter 29) even when the US and China take a contradictory position. This will be neither easy, nor without consequence, as demonstrated by China’s ‘wolf-warrior’ diplomacy and Trump’s unpredictability, each seeking to measure the depth of commitment of Canada and other states to their positions. Previously, Canada has demonstrated that when it takes the lead and works with strategic friends, it can move the international commu- nity to action, as in the case of Ottawa Convention on Landmines and the International Criminal Court both of which do not include China or the US.

### Canada CP Answer – No Middle Power/Liberal Order Solvency

#### Canada doesn’t have power to guide global order

Paikin, Research Fellow, Institute for Peace & Diplomacy, 21

(Dr. Zachary, and a Researcher at the Centre for European Policy Studies in Brussels (CEPS), “Is Canada Still a Middle Power?”, April 22, <https://peacediplomacy.org/2021/04/22/is-canada-still-a-middle-power/>, GDI, access 7/8/22)

The reality is that the core pillars that guided Canadian foreign policy throughout the second half of the 20th century are no longer present in today’s world. A special relationship with Washington and reliable access to the U.S. market can no longer be taken for granted. Multilateralism is, if not in crisis, then at least in a period of profound transition. And not only will Atlanticism lose its relative importance as the global distribution of power shifts eastward, it has also become an uncertain means of constraining American unilateralism in an era that features an increasingly zero-sum great power rivalry.

Canada will need to face up to this new world with intellectual clarity. It must soberly assess the extent to which developments in distant yet adjacent geographic theatres, such as Europe and Asia, genuinely affect its national security and prosperity. If it determines that the impact of such developments is minimal in relative terms, then Canada should abandon its outdated rhetoric of being a “leading middle power” that “punches above its weight” and content itself with the security provided by vassal status. Ottawa could retain an independent trade policy but would cease its efforts to conduct an independent foreign policy, which in many ways now differs from U.S. foreign policy more symbolically than substantively. Canada would continue to police the North American continent to the minimal extent necessary to ensure its formal independence from a southern neighbour that views continental defence and its national security as synonymous. Such a strategy would align well with a post-hegemonic world in which local actors are increasingly assuming responsibility for managing their own regional affairs.

Alternatively, if Canada’s leadership decides that its security interests do not stop at the water’s edge, then it must develop a bipartisan, long-term strategy that lays out which national resources will be developed or deployed in the name of pursuing those interests. This must be accompanied by a conceptual framework that explains how Canada’s varied interests across different regional theatres can be coalesced into a coherent national strategic posture.

Although technically a member of the G7, it is difficult to argue that Canada is as geopolitically prominent a country as France, Germany or Japan in today’s world. In part due to its underinvestment in Asia in a decade where the Sino-American rivalry will take centre stage, it may already be too late for Canada to play a substantive role in shaping global order over the medium term. But as a country with a growing population and a proud history of international engagement, Canada cannot avoid asking itself what kind of international actor it wants to be as this century unfolds. Does it genuinely want to – or even need to – work hard to regain middle power status at a time when global power is becoming increasingly diffuse, or can it be content with the real-world and psychological consequences of possessing more limited ambitions?

## K Answers

### Security K Answer - Permutation

#### Perm - Studying how NATO evolves by securitizing disinformation creates long-term insights into NATO security planning and amity-enmity threat construction.

\**raisons d’être = reason or justification for existence*

Ünver, Özyeğin University Department of International Relations Associate Professor, and Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, 22

(Akın Ünver, Özyeğin University Department of International Relations Associate Professor and Ahmet Kurnaz, Çanakkale Onsekiz Mart University Political Science and Public Administration Research Assistant, All Azimuth, 6/15/2022 “Securitization of Disinformation in NATO’s Lexicon: A Computational Text Analysis,” p. 6-7, https://doi.org/10.20991/allazimuth.1110500 https://www.allazimuth.com/wp-content/uploads/2022/06/Unver-and-Kurnaz\_SecuritizationofDisinformation.pdf, accessed 7-1-2022) SS:/

The logic of interpreting how disinformation gets securitized by relying on NATO documents is two-fold: first, NATO has been evolving to find new *raisons d’être* since the end of the Cold War and has sought to capitalize on the securitization of new threats, such as terrorism, cybersecurity, Syria, and forced migration.38 Disinformation and information war are two of the recent additions to this threat portfolio that helps us understand how NATO’s discourses on security adapt to a new-medium threat. Second, it enables us to understand how institutional security arrangements like NATO reinvent their security identities and construct their amity-enmity relations in light of newer technologies. Since identity and action are considered closely linked in constructivism, and because they are never fixed or intrinsic, but are rather fluid and constituted through social processes, studying longitudinal securitization dynamics gives us valuable insight into long-term NATO security planning.39

### Security/IR K – Alternative Fails

#### No alternative spillover – won’t change real world policymaking

Satoh, Co-Director IAFOR Research Centre, Osaka School of International Public Policy, 21

(Haruko, Osaka University “Great power relations and threats to the liberal international order”, Hiroshima Peace Research Journal, <https://www.peace.hiroshima-cu.ac.jp/wp/wp-content/uploads/2021/03/HPI-Journal-Vol-8.pdf#page=54>, GDO accessed 7/8/22)

Needless to say, the theoretical and philosophical discussions for this less state-centric definition of security are anchored in the English school and liberal internationalists. But more often than not their contribution is obscured by the disagreements within the aca- demic discipline of international relations theory, if they are not pitted against the dominant realists and neo-realists to compete for an authoritative voice. A discernable challenge is how much impact the academic, theoretical debates have on policymakers, particularly those in the foreign and security policy community of great powers. This is not to say that the theoretical world that offers a more nuanced approach to international relations has had no bearing on the real policy world and conducts of great powers. Nor do the realists, particularly prevalent in the US, only see the world in the classical balance of military power terms, if only because of the “discovery” of the utility of power of persuasion, or soft power, as an effective tool of American diplomacy in winning friends in the Cold War. But in mainstream policy discussions about geopolitical competition between the US and China, there appears little room for nuance.