# Disinformation Supplement-GDI22-SCHOLARS

**Contents**

[Disinformation Supplement-GDI22-SCHOLARS 1](#_Toc109033254)

[Disinformation Aff 1](#_Toc109033255)

[Information Credibility Advantage 1](#_Toc109033256)

[Trust Collapse Undermines Democracy 1](#_Toc109033257)

[Trust Collapse Bolsters Partisanship 1](#_Toc109033258)

[Alliances Advantage 1](#_Toc109033259)

[NATO Cooperation Key to Cyber Defense 1](#_Toc109033260)

[Alliance Coop Key to Liberation International Order 1](#_Toc109033261)

[Prebunking Solvency 1](#_Toc109033262)

[Prebunking Solves Disinformation Narrative 1](#_Toc109033263)

[AT – Prebunking Ineffective 1](#_Toc109033264)

[Solvency – AT – Say No/Internal Disinformation 1](#_Toc109033265)

[Topicality 1](#_Toc109033266)

[Security Cooperation Is Not Excusively Military-to-Military 1](#_Toc109033267)

[Disinfo Meets Cyber 1](#_Toc109033268)

[Cyber Includes Protecting Info Systems 1](#_Toc109033269)

[CP Answers 1](#_Toc109033270)

[US Key to Solve 1](#_Toc109033271)

[EU CP – UK Solvency Deficit 1](#_Toc109033272)

[Canada Gets the DA Links 1](#_Toc109033273)

[K Answers 1](#_Toc109033274)

[Scenario Planning Good 1](#_Toc109033275)

[Disad Answers 1](#_Toc109033276)

[Politics – Countering Disinformation Politically Popular 1](#_Toc109033277)

[Neg 1](#_Toc109033278)

[AT – Russian Escalation Risk 1](#_Toc109033279)

# Disinformation Aff

## Information Credibility Advantage

### Trust Collapse Undermines Democracy

Collapse of trust risks instability and threatens democracy

Thomson-Deveaux, FiveThirtyEight senior writer & Qamar, ABC News Fellow, 7-8-22

(Amelia Thomson-Deveaux and Zoha Qamar [former New York Times Senior analyst of Market and Growth Analytics], 7-8-22, FiveThirtyEight, "What Happens When Americans Don’t Trust Institutions?," https://fivethirtyeight.com/features/what-happens-when-americans-dont-trust-institutions/, accessed 7-9-2022) jiu

Americans are feeling uneasy, and it’s hard to blame them. The things they want to change — [inflation](https://www.nytimes.com/2022/06/17/business/economy/inflation-economy-recession.html), [COVID-19 case numbers](https://www.cnbc.com/2022/06/11/this-covid-wave-might-be-the-start-of-our-new-normal-experts-say.html), [rising violent crime](https://www.nytimes.com/2022/06/03/us/democrats-crime-gun-violence.html) in some cities — seem more and more intractable. There was one big, abrupt shift in American life at the end of June, when the Supreme Court [overturned the constitutional right to abortion](https://fivethirtyeight.com/features/roe-v-wade-defined-an-era-the-supreme-court-just-started-a-new-one/). But that wasn’t a change [most Americans wanted](https://www.pewresearch.org/politics/2022/07/06/majority-of-public-disapproves-of-supreme-courts-decision-to-overturn-roe-v-wade/).

This sense of dissatisfaction showed up in [a recent poll from Gallup](https://news.gallup.com/poll/394283/confidence-institutions-down-average-new-low.aspx), which asked Americans how much confidence they have in various institutions. The survey found that since last June, when Gallup last asked this set of questions, Americans’ confidence in almost every institution has dropped. In the poll, which was conducted before the justices released their decision on abortion but after [a draft of the opinion leaked](https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473), the biggest shifts were for the presidency, which saw a 15-percentage-point drop, and the Supreme Court, which saw an 11-point drop. But overall, the national mood is sour. Americans’ average confidence in 14 of the institutions that Gallup asked about was only at 27 percent — the lowest point since Gallup began the survey in 1979.

Americans aren’t just cynical about their political institutions. In [Gallup’s trends](https://news.gallup.com/poll/1597/confidence-institutions.aspx), you can see more and more disillusionment with pretty much every major institution. Some of these shifts are hard to blame on politics — confidence in banks, for instance, fell dramatically during the Great Recession. But experts told me that they’re also the result of increasing partisan polarization and a [decades-long effort](https://www.washingtonpost.com/outlook/2021/10/12/conservatives-have-long-stoked-distrust-government-now-were-paying-it/) by the Republican Party to sow distrust in a wide range of government institutions. The COVID-19 pandemic may have also reinforced Americans’ sense that the government won’t be there for them in times of crisis: According to [a Monmouth University poll](https://www.monmouth.edu/polling-institute/reports/monmouthpoll_US_070522/) conducted from June 23-27, 57 percent of Americans said that the actions of the federal government over the past six months have hurt their family regarding the issue most important to them, up from 34 percent in July 2021 and 46 percent in December.

This broad loss of faith in the institutions that organize our society is dangerous, experts say — and it may be hard to reverse. “Despite the political polarization, both sides feel like they’re losing,” said [Daniel Drezner](https://fletcher.tufts.edu/people/faculty/daniel-drezner), a professor of international politics at Tufts University. “And populaces and countries that are pessimistic about the future often end up doing really bad things.”

The idea that the government doesn’t work for people — and therefore, we should have less of it — can be traced back decades, to the political campaigns of former presidents Richard Nixon and Ronald Reagan. Those messages fed a sense of cynicism that was already growing, according to [Amy Fried](https://umaine.edu/polisci/faculty-and-staff/amy-fried/), a political science professor at the University of Maine who has studied the history of political mistrust. “Throughout the 1960s and 1970s, there are all of these upheavals — Watergate, the Vietnam War, riots, assassinations,” she said. But politicians — mostly Republicans — have since amplified Americans’ doubts by continuing to talk about government overreach and corruption. Former President Donald Trump dialed up these messages, attacking [banks](https://www.washingtonpost.com/politics/trumps-convention-further-alienates-wall-street-and-its-money-players/2016/07/19/5872ade8-4dd2-11e6-a7d8-13d06b37f256_story.html), the [country’s](https://www.theguardian.com/us-news/2018/aug/18/why-is-donald-trump-attacking-the-us-intelligence-community) [intelligence agencies](https://www.bbc.com/news/av/world-us-canada-42360540) and [its election system](https://abcnews.go.com/Politics/trump-longstanding-history-calling-elections-rigged-doesnt-results/story?id=74126926) during his campaigns and presidency.

Political allegiances increasingly shape the way Americans view all kinds of institutions, too. [There are the obvious ones](https://www.pewresearch.org/politics/2022/06/06/public-trust-in-government-1958-2022/) — Democrats have more confidence in the presidency when a Democrat is in the White House, Republicans have more confidence in Congress when the GOP is in control — but trust in the medical system, organized religion and public schools are all shaped by partisanship too. According to Gallup, between 2021 and 2022, Republicans’ confidence in the military fell from 81 percent to 71 percent — a shift that Drezner said could be due to the [botched withdrawal from Afghanistan last summer](https://www.pewresearch.org/fact-tank/2021/08/31/majority-of-u-s-public-favors-afghanistan-troop-withdrawal-biden-criticized-for-his-handling-of-situation/), or to a general sense among some conservative voters that even the military can’t be trusted under a Democratic president. “The culture wars have become so heavily partisan that they now spill over into institutions that previously were thought of as not partisan at all,” he said.

The [economic](https://fivethirtyeight.com/features/were-the-stimulus-checks-a-mistake/) and [public health](https://fivethirtyeight.com/features/the-u-s-still-doesnt-know-how-to-track-a-pandemic/) responses to the COVID-19 pandemic, meanwhile, may have convinced more Americans that the government simply doesn’t know what it’s doing. [Katherine Carman](https://www.rand.org/about/people/c/carman_katherine_grace.html), a senior economist at the RAND Corporation, was one of the authors of [a 2020 report](https://www.rand.org/pubs/research_reports/RRA112-7.html) that examined why Americans trust institutions in the first place. “Competence and honesty — these are really important factors that contribute to trust,” she said. “We ask the government to make and enforce laws and policy for us. So we need them to be truthful about the information they’re providing. And we want them to have the skills and knowledge to actually do those things.”

[At the beginning of the COVID-19 pandemic](https://fivethirtyeight.com/features/americans-trust-the-cdc-on-covid-19-trump-not-so-much/), Americans said they generally trusted the government to handle the crisis and share accurate information about it. Their confidence in Trump’s response to the pandemic [eroded over the remaining year](https://www.reuters.com/article/us-usa-election-trump-coronavirus/trumps-handling-of-coronavirus-pandemic-hits-record-low-approval-reuters-ipsos-poll-idUSKBN26T3OF), but when Biden came into office, approval of his handling of the pandemic was pretty high. Now, though, according to [FiveThirtyEight’s approval tracker for presidents' COVID-19 response](https://projects.fivethirtyeight.com/coronavirus-polls/), 49 percent of Americans approve of Biden’s handling of the pandemic and 43 percent disapprove.[1](https://fivethirtyeight.com/features/what-happens-when-americans-dont-trust-institutions/#fn-1) And [a Pew Research Center poll](https://www.pewresearch.org/politics/2022/01/25/biden-starts-year-two-with-diminished-public-support-and-a-daunting-list-of-challenges/) from earlier this year found that a declining share of Americans are confident that Biden is able to handle the public health effects of the COVID-19 pandemic and that he has good judgment on economic policy, reflecting widespread public concern about rising inflation and a possible recession.

These shifts are happening among Americans of all political stripes, although to different degrees. The Gallup poll found that Democrats’ confidence in the institution of the presidency fell from 69 percent in 2021 to 51 percent this year — an alarming drop among members of Biden’s own party. That tracks, overall, with [a broader erosion in Biden’s support](https://fivethirtyeight.com/features/democrats-have-been-souring-on-biden-since-last-summer/) among Democrats, many of whom are disappointed about his administration’s lack of policy achievements and increasingly frustrated about rising costs.

The danger, Carman said, is that Americans’ trust in institutions doesn’t just decline — mistrust starts to grow. Her report found that there was already active mistrust of the government and media. “I think that’s particularly worrisome,” she said. “Active distrust means not only do you think they’re not always honest — maybe they lie to you. Maybe they’re trying to hurt you.”

Widespread distrust can be dangerous. If people don’t trust government institutions, they’ll be more likely to believe that elections are untrustworthy too. Drezner said that as distrust increases, people are more likely to act in disruptive or even violent ways, like with the Jan. 6 insurrection. If Americans believe the institutions around them are failing, he said, they “might be tempted to take a risky gamble that puts you back to where you used to be.”

That’s a bleak outlook. But Americans are in a bleak mood. Drezner said that if some of the trends that are sowing deeper distrust turn around — say, the pandemic fades into the background and inflation begins to abate — people might start to feel better about the government too. But for now, they’re not feeling happy about most of the institutions that order society — and that could be bad for democracy.

### Trust Collapse Bolsters Partisanship

#### Weakening trust bolsters partisan extremes and risks crises

Bump, Washington Post National Correspondent, 7-11-22

(Philip Bump, National correspondent, Washington Post, 7-11-2022, "Analysis," https://www.washingtonpost.com/politics/2022/07/11/sarah-palin-offers-perilous-framing-election-good-vs-evil/, accessed 7-11-2022) SS:/

American politics is predicated on the idea that power is transitory. Citizens are asked to go to the polls every two years and decide on national leadership, with all involved theoretically recognizing that this might mean a change of direction. If you’re a Democrat wanting to see a Democrat represent you, you vote for the Democrat and hope she wins. If she doesn’t — well, there’s always two years from now.

You already recognize a way in which this idea has been polluted. Partisan redistricting and the pattern of Americans moving into politically homogeneous communities have meant that there are fewer places where there are actual transitions between parties. If you are a Republican in California or a Democrat in Mississippi, you hold out little hope for being represented in the Senate by a member of your party.

This is a problem we don’t often acknowledge. I interviewed Princeton University’s Corrine McConnaughy last year, and she expressed concern about the lack of institutions that let “people feel represented enough, feel their voice heard enough.” Essential to democracy is that people “understand that losing today is not losing tomorrow.” That there is recourse for changing direction. If people feel as though electoral politics can’t effect change, they look for other mechanisms to do so.

Now we layer onto this another danger, one exemplified by former Alaska governor Sarah Palin at a rally last week. Palin is running for Alaska’s safely Republican House seat and appeared at a rally with former president Donald Trump. She cast the election in stark terms, which in broad strokes isn’t atypical for a candidate. But the phrasing Palin uses was a moral, existential one.

“This is life-changing what’s coming up here in the midterms, the changes that are needed,” Palin told the cheering audience. “And it’s no longer Democrat versus Republican. This is all about control versus freedom.”

Then, a starker contrast: “It’s good versus evil. It is a spiritual battle.”

This is on-brand for Palin. Her arrival on the national political scene in 2008 was as John McCain’s vice-presidential running mate, a selection made because McCain’s team believed she could provide an invigorating jolt of energy — and lure further-right, often evangelical voters to cast a ballot. In the Trump era, evangelical voters became a driving part of the party’s success. Palin, of course, already spoke the language.

Trump’s campaign and presidency were centered on widening fissures within the country, hewing closely to the demands of his base and working energetically to score political points against the hated left. Many evangelicals saw this in religious terms. In early 2019, a poll found that half of White evangelical Christians believed that God wanted Trump to be president. He was their overt, unflinching defender — not because he shared their beliefs necessarily (though many convinced themselves he did) but because he understood that rising to the religious right’s defense would bolster his own political position. He promised to defend them, and he did. In 2016, he won evangelicals by 61 points. In 2020, by 69.

That the country has become more polarized is well documented. Members of each major political party have viewed the opposition in increasingly hostile terms over the past 20 years, as measured by the American National Election Study conducted during each presidential year. As recently as 2000, the median “temperature” score granted the other party by Republicans and Democrats was above 40 out of 100, with lower numbers indicating “colder” views of the party. In 2020, both parties had medians under 20.

Again, some of this probably derives from our political isolation. We often live near those from the opposing party, but we don’t necessarily incorporate them into our lives. Pew Research Center found in the summer of 2020 that only about 1 in 5 supporters of Trump or Joe Biden had more than a few friends supporting the other candidate. Four in 10 knew no one who did.

Such a divide and such skepticism about the opposition make it easier to cast those other partisans as dangerous or evil, a framing that is facilitated by the country’s increased reliance on partisan media universes. Shortly after Biden took office, CBS News published a poll conducted by YouGov finding that about 4 in 10 Democrats viewed Republicans not as political opponents but as enemies. More than half of Republicans said they viewed Democrats as enemies.

Consider how intertwining religion with politics makes a sense of political impotence worse. If you think that you have little recourse for being heard through the electoral process and you see your side as fighting on behalf of a divinely motivated cause? Perilous.

This isn’t newly perilous, certainly. In his seminal essay “The Paranoid Style in American Politics,” Richard Hofstadter described right-wing frustration at a perceived political elite more than a half-century before the current moment.

“The situation becomes worse when the representatives of a particular social interest — perhaps because of the very unrealistic and unrealizable nature of its demands — are shut out of the political process. Having no access to political bargaining or the making of decisions, they find their original conception that the world of power is sinister and malicious fully confirmed.”

Palin was speaking to an audience about the dangers of leaders who advocated measures such as mask mandates, something for which many Americans did, in fact, have no real recourse — besides, of course, simply not complying. The mandates were, in fact, often described as sinister and malicious. In her speech, shortly after the “good versus evil” bit, Palin called the emergence of the coronavirus the “plandemic” and suggested that elites wanted to tank the economy.

The particular problem here is that there will always be a level of governance over which someone has no control. Even if you live in Oklahoma, with conservative House members, senators and state-level officials, Biden is still president. The House and Senate are still majority-Democratic. Even if Republicans regain a federal trifecta, you have little recourse over, say, the Department of Motor Vehicles. This is the utility of casting government as an enemy; the opportunities to cast some part of it as despotic are eternal. To cast it as evil.

Last summer, Pew asked Americans how they felt about leaders from their own party describing the other party’s officials as evil. Most thought this should not be considered acceptable. Just under half of Republicans thought the party should be “very” or “somewhat” accepting of such rhetoric.

If you convince people that elections are fights between two ends of the moral plane, the consequences of losing are heightened dramatically. If you then claim that the election itself was dishonest, that your side had been “shut out of the political process” (as Hofstadter put it) illicitly, you risk crisis.

## Alliances Advantage

### NATO Cooperation Key to Cyber Defense

#### NATO’s Cyber Operations Centre requires better collaboration with Allies to deter higher frequency threats.

Jacobsen, University of Southern Denmark Danish Institute for International Studies Ph.D. candidate, 21

(Jeppe T Jacobsen, University of Southern Denmark Danish Institute for International Studies Ph.D. candidate, Oxford University Press, 5-10-2021, "Cyber offense in NATO: challenges and opportunities," International Affairs, Volume 97, Issue 3, Pages 704-705, EBSCO, https://doi.org/10.1093/ia/iiab010, accessed 7-13-2022) SS:/

\*NATO Cyber Operations Centre = CYOC

The article makes three arguments in support of the overall argument that NATO will (and should) continue to play only a limited offensive role in cyberspace. First, it identifies four distinct cyber effects from the current debates on major cyber incidents presented in the cyber-conflict literature. This is done in order to assess the operational challenges and possibilities for successful integration of sovereign cyber effects in NATO operations, also known as SCEPVA.8 As cyber effects are often costly in time and resources to develop, difficult to predict and verify, and involve a risk of confliction, it is argued that the types of offensive cyber operations that are highly destructive and specialized, with a view to enabling other (kinetic) military effects, are the most difficult to integrate. In contrast, less complex disruptions used to persistently annoy and confuse adversaries hold more promise. In order to work in NATO, these effects require more flexibility in the way CYOC sends requests to and interacts with the member states.

Second, in the light of the renewed scholarly attention being given to NATO’s capacity to deter Russia, the article unpacks and assesses the suggestion that a centre for integrating offensive cyber effects contributes to NATO’s deterrence posture.9 It assesses the addition of cyber effects to NATO’s operational toolbox in the light of the (hybrid) threat environment which is currently being articulated in NATO, and argues that such integration adds little to the existing deterrence posture. NATO’s superior conventional capabilities—with or without cyber effects—already threaten punishment to adversaries who may consider invading allied countries. Yet CYOC and the alliance as a whole do not deter the more frequent (hybrid) cyber activity against member states that does not reach the threshold of armed conflict.

### Alliance Coop Key to Liberation International Order

#### Alliance cohesion key to global liberal order - the alliance must cooperate or cease to operate

Carafano, Heritage Foundation Allison Center for Foreign Policy Studies director & Davis Institute for International Studies vice president, -78-22

[James, 7-8-22, The Heritage Foundation, "How U.S. Allies Can Engage Effectively With The Biden Administration", https://www.heritage.org/global-politics/commentary/how-us-allies-can-engage-effectively-the-biden-administration accessed on 7-13-22, hooch//cs]

How Can U.S. Allies Better Work with America?

From these developments, we can draw some lessons on how America’s allies and partners can engage effectively with the Biden administration. Interestingly, it is the kind of approach that will resonate with American conservatives—even those who are skeptical of overseas engagement. In short, to get Biden’s attention, our allies must show initiative, suggest concrete action, and demonstrate their own willingness to put skin in the game and fight.

In the examples above, both NATO and South Korea showed initiative in reaching out to the U.S. They didn’t just ask for help. They brought ideas and initiatives to the table and made the case for how joint action would serve American interests as well as theirs.

When Trump reprised the term “America First,” he never meant “America Alone.” Our friends and allies have figured that out. They now understand the need to argue why joint action not only advances grand notions such as “a rules-based order,” “advancing shared values,” or “international norms,” but also will be good for every everyday Americans.

More importantly, they recognize that partnership entails taking responsibility and sharing in the burden, risks, and rewards. In defense of Ukraine, for example, Estonia has committed the equivalent of one-third of its annual defense budget to provide resources for Kyiv. That gives them street cred in looking to partner with the U.S. Finland and Sweden want to join NATO. The U.S. will support that because they are not looking to be free riders, but are bringing serious capabilities to the security table. Their membership serves U.S. interests.

## Prebunking Solvency

### Prebunking Solves Disinformation Narrative

#### Through prebunking, the NATO and its member states have been able to control the narrative in Ukraine

Tom, intelligence corps officer, 22

[Capt Tom, 3-18-2022, Wavell Room, "How the West is starting to win the disinformation war » Wavell Room,", https://wavellroom.com/2022/03/18/disinformation-russia-nato/, Accessed 7-15-2022, LASA-LR]

In the run up to Russia’s invasion of Ukraine, the U.S. declassified an unprecedent amount of intelligence regarding how Putin was going to justify his actions. While Putin was saying that the buildup of troops was just an exercise, the U.S. revealed that blood supplies were being moved up to basing areas; a key indicator that Russia expected to take casualties. Before Putin could even begin his ‘false flag’ operations, the U.S. revealed that these were a pretext for invasion. The U.K. got in on the act as well, releasing intelligence that Russia planned to install a pro-Moscow government in Kiev. Unfortunately, this intelligence was largely ignored – and even ridiculed by the Ukrainian government – with many Europeans believing that invasion was not Putin’s planned course of action. As we now know, the intelligence was remarkably accurate.

Despite this, the releasing of intelligence that preempted Russia’s actions had a significant effect in undermining the narrative that Putin planned on building; that of a belligerent NATO, an aggressive Ukrainian government, and a people who needed saving. Ever since Putin has been struggling to control the narrative around the invasion. Claims made that Ukraine was close to building a ‘dirty bomb’, and that it was planning an offensive operation against the Donbass seem like a regime scrabbling to retrospectively legitimise its actions, and failing.

NATO and the West has struggled to control disinformation, particularly when it’s emanated from Russia. Putin was able to dictate the narrative around his use of ‘little green men’ in Crimea in 2014 and exploit US political divisions to cover his interference in the 2016 U.S. Presidential elections. However, the use of classified intelligence to ‘prebunk’ Russian disinformation in Ukraine demonstrates a tool that the West and NATO can exploit to get ahead in the disinformation fight. But for this to be effective it will not only require the sharing of intelligence with the public to become more widespread, but a change in how intelligence agencies operate.

#### Prebunking is based on intelligence with high visibility

Myre, NPR National Security Correspondent, 22

(Greg Myre, NPR national security correspondent with a focus on the intelligence community, NPR, 2-8-2022, "As Russia threatens Ukraine, the U.S. 'pre-bunks' Russian propaganda ," https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda, accessed 7-15-2022) SS:/

The Biden administration says it doesn't know whether Russian leader Vladimir Putin will invade Ukraine with the more than 100,000 troops he's amassed near their shared border.

But Biden's national security team says a Russian disinformation campaign is already well underway. Pentagon spokesman John Kirby recently outlined what he described as a Russian plan to create a phony video that could be used as a pretext for a Russian invasion.

"As part of this fake attack, we believe that Russia would produce a very graphic propaganda video, which would include corpses, and actors that would be depicting mourners."

In a similar vein, Britain recently announced that Russia might try to stage a coup in Ukraine and install a leader friendly to the Kremlin — who could then "invite" Russian troops into the country.

This kind of intelligence usually remains secret, but the U.S. and its allies have clearly made a decision to go public.

"This could potentially be called pre-bunking," said Nina Jankowicz, who's with the Wilson Center in Washington and the author of How To Lose the Information War: Russia, Fake News, and the Future of Conflict.

"Rather than debunking, the (U.S. and British) governments are getting ahead of a potential Russian narrative and attempting to pre-bunk it with this intelligence that they've been declassifying," she said.

U.S. claims face some skepticism

The U.S. and British governments have presented this information without offering proof. They say they can't reveal their sources and methods for obtaining it.

This has led to some skepticism. Critics note the U.S. failed to predict the rapid collapse of the Afghan government last year. And the U.S. invaded Iraq in 2003 on the false premise that Iraqi leader Saddam Hussein had weapons of mass destruction.

"I know that a lot of people will intuitively, instinctively say, 'Well, U.S. intelligence has gotten major things wrong in the past,'" said Professor Thomas Rid, who studies disinformation at Johns Hopkins University.

He thinks the U.S. and Britain have provided enough information to make their case in this instance.

"It appears that the U.S. intelligence community, with the United Kingdom and others, have very good visibility into Russian planning, because otherwise they wouldn't be able to reveal those details," said Rid, the author of Active Measures: The Secret History of Disinformation and Political Warfare.

### AT – Prebunking Ineffective

#### Prebunking is effective but underutilized, after the election is too late

Norman, Carnegie Mellon University Humanism Initiative Director, & Mcintyre, Boston University Center for Philosophy and History of Science Research Fellow, 22

(Andy Norman, Carnegie Mellon University Humanism Initiative Director, & Lee Mcintyre, Boston University Center for Philosophy and History of Science Research Fellow, Deseret News, 3-2-2022, "Opinion: What is ‘prebunking’ and what does it have to do with Russia?," https://www.deseret.com/opinion/2022/3/2/22955870/opinion-how-the-white-house-prebunked-putins-lies-disinformation-joe-biden-donald-trump-russia, accessed 7-15-2022) SS:/

White House officials have been using a powerful psychological technique to combat Russian disinformation.

They’re calling it out in advance.

As early as December, they began warning that Moscow might invent provocations to justify an invasion of Ukraine. A month later, they predicted a “false flag” operation and gave specifics: Russia had sent saboteurs into Ukraine and was planning to release a staged video of fake Ukrainian atrocities. When the video finally appeared, it fell flat. In fact, it was quickly recognized as propaganda and ridiculed as “dumb.” That’s how you combat disinformation.

White House press secretary Jen Psaki went on to clarify the administration’s approach: “We’ve made a decision — a strategic decision — to call out disinformation when we see it. We are much more cognizant of the Russian disinformation machine than we were in 2014. Russia has a boundless capacity to misrepresent truth.”

Because President Joe Biden’s team was proactive, Vladimir Putin’s lies gained almost no traction, and the civilized world stands in near universal opposition to Russia’s aggression in Ukraine. The importance of this accomplishment should not be underestimated. In a recent webinar hosted by American Purpose magazine, retired U.S. Army officer and strategy analyst Ben Hodges described Biden’s handling of the situation as brilliant. He went on to predict that “people are going to be studying this for a long time.”

Maybe so, but experts on disinformation have studied similar techniques for almost 60 years. Early researchers called it “mind-inoculation.” Today, many call the strategy “prebunking.” It’s a way to prevent false narratives from sinking roots into people’s minds — and guard against the more challenging salvage operation of “debunking” them later.

The Kremlin’s use of disinformation is not limited to military campaigns. Before Biden took office, Russian intelligence operatives propagated the wacky theory that Western COVID-19 vaccines would contain microchips. They pushed it out to one of their English language propaganda arms, and a month later, a CBS poll indicated that 44% of Republican voters believed it to be true.

We can draw important lessons from this. First, human beings can be astonishingly gullible; our susceptibility to nonsense is nearly bottomless. Second, we have to be proactive about combatting disinformation. Think about it: If Donald Trump had taken on Russian COVID-19 disinformation the way Biden took on Russian disinformation about Ukraine, hundreds of thousands of Americans might still be alive today.

Third, our brave new digital world gives bad actors unprecedented power to exploit vulnerable minds. Russian propagandists, domestic conspiracy theorists, demagogic politicians, cult leaders, peddlers of quack cures — our world is now teeming with people skilled at disrupting higher brain function. Scientists call it “amygdala hijacking” — the use of fear to sow division, stoke resentments, win followings and manufacture cynicism.

If the situation feels out of control, take heart. Scientists like Stephan Lewandowsky, Sander van der Linden and John Cook have been studying solutions. Their research suggests that prebunking is massively underutilized. We could be using it to combat climate denial, vaccine resistance, QAnonsense, political polarization and more.

Our own work, as researchers at the Cognitive Immunology Research Collaborative, suggests that prebunking is just the tip of a very large iceberg. In fact, there are many ways to boost “mental immune function” and thereby reduce susceptibility to bad information. It’s time we took a more systematic approach to fortifying minds against malicious influence. Cognitive immunology — the science of mental immunity — points the way.

Disinformation is insidious. Like biological weaponry, it releases infectious agents that spread corruption among the susceptible. With internet connectivity as a vector of transmission, the threat to our way of life is profound.

To many, Trump’s claims about the 2020 election looks like nothing more than the complaints of a sore loser. But by spreading allegations about rigged voting machines, corrupt election officials, bamboo ballots and more, Trump and his allies might be laying the groundwork for things they might do if they don’t like the results in 2024.

Will the Biden White House employ its new strategy of prebunking to combat Trump disinformation too? If they wait until election season, it may be too late.

In the meantime, there’s still plenty of disinformation out there about Ukraine to keep the debunkers busy, such as fake photos on social media (with some images even taken from video games) and lies about the Ukrainian president having already fled Kyiv or raised the white flag.

In the future, once people become more aware of the prevalence of disinformation and the power of prebunking, it will be possible to head off some of this nonsense before it starts, by making people more skeptical of what they see and hear and building up their mental immunity in advance.

#### U.S. is able to see potential threats and disinformation attacks that are being utilized now – Russia propaganda in Ukraine proves

Myre, NPR national security correspondent, 22

[Greg Myre, 2-8-2022, NPR.org, "As Russia threatens Ukraine, the U.S. 'pre-bunks' Russian propaganda ,", https://www.npr.org/2022/02/08/1079213726/as-russia-threatens-ukraine-the-u-s-pre-bunks-russian-propaganda, Accessed 7-15-2022, LASA-LR]

But Biden's national security team says a Russian disinformation campaign is already well underway. Pentagon spokesman John Kirby recently outlined what he described as a Russian plan to create a phony video that could be used as a pretext for a Russian invasion.

"As part of this fake attack, we believe that Russia would produce a very graphic propaganda video, which would include corpses, and actors that would be depicting mourners."

In a similar vein, Britain recently announced that Russia might try to stage a coup in Ukraine and install a leader friendly to the Kremlin — who could then "invite" Russian troops into the country.

U.S. says Russia is planning a staged attack in Ukraine to justify an invasion

This kind of intelligence usually remains secret, but the U.S. and its allies have clearly made a decision to go public.

"This could potentially be called pre-bunking," said Nina Jankowicz, who's with the Wilson Center in Washington and the author of How To Lose the Information War: Russia, Fake News, and the Future of Conflict.

"Rather than debunking, the (U.S. and British) governments are getting ahead of a potential Russian narrative and attempting to pre-bunk it with this intelligence that they've been declassifying," she said.

## Solvency – AT – Say No/Internal Disinformation

#### Status quo efforts to counter Russian disinformation campaigns prove that they are popular within international institutions like NATO but absent the aff they fail

Kowalski, Chatham House Russia & Eurasia Programme research assistant, 6-22

[Adam, 6-22, Chatham House "Disinformation fight goes beyond Ukraine and its allies," <https://www.chathamhouse.org/2022/06/disinformation-fight-goes-beyond-ukraine-and-its-allies>, accessed 7-14-22]

Reactive response to new information realities

As the Kremlin tightened its grip over the media space in Russia and increased spending on information dissemination, the international response was fast and unified with many tech companies and social media platforms increasing efforts to highlight and remove malicious information actors.

Fact-checking and debunking organizations ramped up their operations and the UK and Australia explicitly asked social networks to block Russia state-linked services and content providers. The European Union (EU) and the UK banned both Sputnik and RT, and Canada announced increased funding for the G7’s Rapid Response Mechanism, which was created to respond to threats from foreign actors ‘seeking to undermine democratic societies and institutions’.

International responses to Russia’s malign information tactics are based on decades of experience and are now supported by growing funding and a heightened awareness of the nature of the problem. During the war in Ukraine, they have demonstrated how quickly they can react to new information realities – changing narratives, target audiences, or methods of spreading information.

But if these approaches to the growing disinformation threat cannot be extended to the Kremlin’s other targets, including those [closer to home](https://balkaninsight.com/2022/05/09/russia-targets-bosnia-with-disinformation-about-ukrainian-war/), pressure from beyond national borders will grow to [make concessions which are advantageous](https://www.chathamhouse.org/2022/03/cost-ceding-advantage-russia-far-reaching) to Russia’s longer term aims.

## Topicality

### Security Cooperation Is Not Excusively Military-to-Military

#### Security cooperation is not exclusively military-to-military

Skorupski, Congressional Research Service Research Assistant & Serafino, Congressional Research Service Specialist in International Security Affairs, 16

[Bolko J. & Nina M., 8-23-16, Congressional Research Service, “DOD Security Cooperation: An Overview of Authorities and Issues,” <https://sgp.fas.org/crs/natsec/R44602.pdf>, p. 2, accessed 7-12-22]

DOD defines “security cooperation” as a broad set of activities undertaken by DOD to encourage and enable international partners to work with the United States to achieve strategic objectives. Included in the definition are DOD interactions with both foreign defense and foreign nonmilitary security establishments. Security cooperation includes all DOD-administered security assistance programs that (1) build defense and security relationships that promote specific U.S. security interests, including all international armaments cooperation activities and security assistance activities; (2) develop allied and friendly military capabilities for self-defense and multinational operations; and (3) provide U.S. forces with peacetime and contingency access to host nations.4 According to DOD, security assistance is a subset of DOD's security cooperation portfolio.

### Disinfo Meets Cyber

#### Disinformation is a cybersecurity issue

United States Cyberspace Solarium Commission, 21

[December 2021, Cyberspace Solarium Commission, “COUNTERING DISINFORMATION IN THE UNITED STATES, CSC White Paper #6,” <https://www.solarium.gov/public-communications/disinformation-white-paper>, p. 4, accessed 7-12-22]

INTRODUCTION – WHY DISINFORMATION IS A CYBERSPACE ISSUE

The United States Cyberspace Solarium Commission (CSC) was created by Congress in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy? While disinformation is considered by some an issue largely separate from cybersecurity or network security,1 the Commission addressed disinformation in the very narrow context of elections in its final report in March 2020. As the COVID-19 pandemic swept across the globe, the Commission revisited the issue, this time in the context of disinformation about the pandemic itself, noting, “Our adversaries’ disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts with which Americans are best acquainted.”2

Over the course of the intervening months, the Commission received demand signals from constituents within Congress and the executive branch to treat the topic of disinformation and potential policy recommendations more extensively. The Commission has previously been reluctant to delve deeply into the topic of disinformation for two reasons.

First, disinformation as a policy issue, unlike many aspects of cybersecurity policy, has been marked by a strong partisan divide. Researchers have identified an association between strong partisanship and vulnerability to misinformation;3 more than two-thirds of U.S. citizens believe that Republicans and Democrats disagree about basic facts;4 and while U.S. citizens in both major parties agree that disinformation is a problem, they disagree about who is responsible for it and what ways to tackle the threat are appropriate.5 Although this partisan divide persists today, it is the sense of the members of the Commission that there is room to reach some agreement on core issues.

Second, as noted above, disinformation is seen by many as an issue largely separate from cybersecurity and cyber policy in the United States. While the Commission understands this view, continuing to bifurcate these issues has become untenable. From a strategic perspective, the United States and its policymakers do themselves a disservice by continuing to differentiate between the two when our adversaries do not.6

In order to craft a comprehensive strategy to defend the United States from cyberattacks of significant consequence, policy-makers must account for the entire arsenal employed by adversaries to cause harm in cyberspace, including information. It is also important to take a more operational or risk management perspective: disinformation campaigns waged against the United States by foreign actors are often carried out by many of the same threat actors as are active in cyberspace and are often the consequence of cyberattacks.

For these reasons, members of the Commission believe that elements of the topic of disinformation are within our mandate. This white paper is the result of deep research, interviews with experts, and deliberations by the Commission. It seeks to explain how the Commission’s proposed strategy of layered cyber deterrence applies to combating disinformation and contributes a set of policy recommendations to better position the United States to prevent, counter, and withstand the consequences of disinformation launched against it.

#### Countering disinformation is cybersecurity---terrain, tactics, targets, and temptations prove. The EU votes aff.

EU DisinfoLab, 21

[5-24-21, This paper provides feedback from the EU DisinfoLab on the EU’s updated cybersecurity strategy, the Joint Communication on the EU’s Cybersecurity Strategy for the Digital Decade (16 Dec 2020) and is developed based on our experience conducting investigations into sophisticated disinformation campaigns run by state and non-state backed actors, recent publications, and ongoing discussions with public authorities and civil society partners in the European Union (EU), the UK, and the US, on how to counter the evolving threat., EU Disinfo Lab, “Why Disinformation is a Cybersecurity Threat,” <https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat/>, accessed 7-12-22]

Context: Why Disinformation is a Cybersecurity Issue

Drawing on our research into coordinated disinformation campaigns and our own experience as an NGO in the field, we wish to highlight four areas of convergence between disinformation and cybersecurity of relevance to EU policymakers: the “terrain” on which disinformation is distributed (the social web and the internet stack, networking infrastructure, routing services), the “tactics” that increasingly combine disinformation as part of the cyberattack delivery package, the “targets” leading to victims of cyberattacks simultaneously being victim of disinformation, and what we could call the “temptation”, ie. the lucrative possibility of both disinformation campaigns and cyberattacks.

Terrain: While there is much focus on disinformation across major social media platforms, disinformation is an inherently distributed phenomenon. Disinformation campaigns continue to make use of networking infrastructure and routing services, leveraging different levels of the internet stack. As EU DisinfoLab’s  recent investigations have demonstrated, social media platforms often serve as gateways and amplifiers of disinformation websites. In this way, disinformation and cybersecurity implicate many of the same members of the private sector and the internet technical community.

Tactics: There is significant overlap between disinformation and cybersecurity regarding the tools and methods of attack. Disinformation is increasingly part of the cyberattack delivery package, used to deliver malware by manipulating people’s fears and heightened emotions (for instance the deployment of “fearware”, a subset of phishing lures that rose in prominence during the pandemic and rely on anxieties and informational deficits). The continuous proliferation of hack and leak operations as well as the coordination between hybrid tactics (illustrated in the Sandworm case) demonstrates this convergence. There is also significant convergence between disinformation campaigns and the  tactics used in cybercrime, for example, via illegal dark web transactions, illegally obtained documents, and various kinds of fraud.

Targets: Disinformation campaigns and cyberattacks can cause similar harms and are sometimes combined to reach the same targets. While a data breach can compromise information security, so can the manipulation of data. We saw an example of this related to Covid-19 vaccines early this year, when hackers stole confidential documents from the European Medicines Agency (EMA) a European Union regulatory body to  seow mistrust in the Pfizer-BioNTech vaccine. Meanwhile, so-called “anti-democracy attacks” and “cyber influencing attacks” like media manipulation and astroturfing in the context of elections illustrate the hybrid nature of interference in democratic processes.

Temptations: Hacking, cybercrime and influence operations are lucrative endeavors, often outsourced to skilled professionals. While individuals and businesses may have increased their readiness for ransomware attacks, disinformation strategies like defamation and extortion are now being used to cause reputational damage and seek profit. These activities all have strong financial incentives and as yet insufficient consequences, due in part to the challenges of attribution but also to the lack of dissuasive/restrictive measures.

### Cyber Includes Protecting Info Systems

#### US and NATO definitions included protection information

Costigan, George C. Marshall European Center for Security Studies professor & Hennessy, Royal Military College of Canada History professor, 16

[Sean S. & Michael A., July 2016, NATO, “Cybersecurity: A Generic Reference Curriculum,” <https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_10/1610-cybersecurity-curriculum.pdf>, p. 15, accessed 7-12-22]

For definitional clarity, we have relied on the U.S. National Institute of Standards and Technology (NIST) definition of cyberspace, the interdependent network of information technology infrastructures, which includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers….” Cybersecurity has been defined as “the activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification or exploitation.” That basic definition shapes what we have included throughout this document.

#### Experts say disinformation is cybersecurity

Camancion, University of Albany information science PhD, et al., 22

[Kevin Matthe, & Yueqi Li, Elisabeth DuBois, Ellie Seoe Jung, 4-12-22, Data, “The Missing Case of Disinformation from the Cybersecurity Risk Continuum: A Comparative Assessment of Disinformation with Other Cyber Threats”, <https://www.mdpi.com/2306-5729/7/4/49/pdf,> p. 1-2, accessed 7-17-22]

According to a report by the Institute for Public Relations, 63% of Americans view disinformation as a major problem in society, yet there are limited avenues to combat it outside of media literacy and news spaces [1]. similarly, a report by Neustar International Security Council (NISC) found that 48% of cybersecurity professionals think of disinformation as a threat, of which 49% say the threat is very significant. The study also found that 91% of cybersecurity professionals thought that stricter measures should be implemented on the Internet [2]. The gravity of the impact of disinformation on the confidentiality, integrity, and availability of information makes it necessary to view disinformation not simply as an error of information but as a form of cyberattack.

Cybersecurity relates to the protection and defense of personal information, computer systems, and critical infrastructure. Cyber threats tend to compromise the confidentiality, integrity, and availability of technology systems. Disinformation, the sharing of deliberately misleading or biased information, has been formally classified as an information disorder by the Council of Europe (2017) [3]. The goal of disinformation is to change an individual’s thoughts and behaviors, consequently influencing public opinion by altering one’s view of reality or accentuating one’s prior held beliefs to disrupt truth-seeking. Deceptive information can leave people confused about basic facts and current events, creating a dangerous situation affecting public safety, organizational reputations, or governmental functions. In many ways, disinformation is thus similar to a cyberattack, where instead of compromising a computer system, it compromises our cognitive abilities. Such disruptions have been coined cognitive hacking—where such practices can result in a greater threat than a cyberattack on critical infrastructure [4]. The damage caused by disinformation can be challenging to repair, as people form opinions based on cognitive and confirmation biases. The deceptive nature of disinformation is further accentuated by economic pressures and advertisement-centric models that incentivize disinformation to overload information channels, often drowning the truth. Just as technology and social media expansion increase cybersecurity risks, they exacerbate the impact of disinformation.

## CP Answers

### US Key to Solve

#### US is key – US experience, expertise, and capabilities are unmatched

Libicki, US Naval Academy Center for Cybersecurity Studies Distinguished Visiting Professor, 17

[Martin C., Spring 2017, “The Convergence of Information Warfare,” StrategicStudies Quarterly, Vol. 11, Issue 1, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11\_Issue-1/Libicki.pdf, p. 61-62, accessed 7-15-22]

The Future of US Information Warfare

Given the trends and convergence of information warfare, how might the United States exploit these trends? On the face of it, no country is better positioned to carry out information war. US skills at cyberwar have no equal. US institutions lead the world in the commercialized arts of persuasion, and the collection and analysis of personal information for commercial and political purposes have proceeded farther in the United States than anywhere else. No country is more advanced in digitizing and networking things. US expertise in systems integration is unchallenged. But figuring out how to effectively harass another country's citizens one at a time does not seem like an urgent or important, much less permissible, US national security problem to solve.

Nevertheless, because other countries are interested in figuring out how to combine these elements of information warfare into a unified whole, the United States ought to understand how to do so itself. First, there may be useful techniques learned even if the larger idea is unacceptable. Second, even though the prospect of operating a harassment campaign based on IW is unpalatable, one cannot rule out occasions in which the only way to stop others from doing so (short of armed conflict) may be a credible offensive capability. Third, just as the Defense Advanced Research Projects Agency was established shortly after Sputnik launched for the purposes of preventing surprise- -and then went ahead to develop technology that surprised others- dabbling in the arts of IW could help prevent external developments from surprising the United States.

If the United States were to embed cyber operations within a broader context of IW, then the mission and organization of US Cyber Command would have to change. Today it boggles the mind to ask an organization (deservedly) wrapped in great secrecy to take the lead for influence operations, which are ineluctably public. But in time, the choice to overlook the psychological effects of cyber operations or the potential synergy between psychological operations and cyber operations would make just as little sense.25 Serious thought may be needed on how to build an information warfare authority, whether housed under one organization or achieved through intense coordination among the various communities: cyber warriors, cyber intelligence collectors, electronic warriors, psychological operators, and, in some cases, special operators.

Perceptions of cyberwar might also need rethinking. One could debate the plausibility of a determined cyber attack campaign unaccompanied by violence. However, it is harder to imagine a cyber attack campaign unaccompanied by other elements of information warfare, in large part because almost all situations where cyber attacks are useful are also those which offer no good reason not to use other elements of IW. For instance, if another country is trying to exhaust US will by conducting cyber attacks on information systems that underlie US commerce, they would not necessarily try to blow up trucks. Rather, cyber attacks that compromise trucks, to reduce confidence in their safe operation, are more plausible, if achievable. It is also quite likely that in a systematic campaign, attackers would try to jam GPS or override satellite uplinks, using cyber espionage to create the impression that they are watching Americans and are prepared to dox particular individuals, or letting a thousand trolls bloom to create a news environment that would pit Americans against each other. The latter activities have attributes of nonlethality, unpredictability, ambiguity, and persistence that allow them to fit the strategic niche occupied by cyber attacks. Preparations to retain resilience and accelerate recovery after a cyber attack campaign would also do well to address the complications that could arise if other elements of IW were used in conjunction with cyber attacks.

### EU CP – UK Solvency Deficit

#### The UK has counter disinformation strategies that are key to stopping disinformation

**Sawers, VentureBeat Technology Staff Writer, , 20** (Paul, 3-30-2020, VentureBeat, "U.K. fights coronavirus disinformation with rapid response team", https://venturebeat.com/2020/03/30/u-k-fights-covid-19-disinformation-with-rapid-response-team/, accessed on 7-15-2022, SR)

**The U.K. government has announced new measures to crack down on the spread of false COVID-19 information online, including implementing dedicated specialist units to tackle misinformation.**

The new rapid response unit will operate from inside the U.K.’s Cabinet Office and will look at ways to counter “harmful narratives” on the internet — addressing the scourge of “experts” issuing false and harmful misinformation, as well as fraudsters operating phishing scams.

“We need people to follow expert medical advice and stay at home, protect the NHS [National Health Service], and save lives,” U.K. Culture Secretary Oliver Dowden said in a statement. “It is vital that this message hits home and that misinformation and disinformation which undermines it is knocked down quickly.”

Disinformation and “fake news” are major blights on 21st-century society, enabled by ubiquitous connectivity that delivers deceptive information directly to people’s pockets 24/7. We’ve already seen how social media can be abused to further political agendas, and over the past few months a similar trend has emerged with the COVID-19 outbreak.

Earlier this year, the World Health Organization (WHO) referred to the issue as a massive “infodemic.” The WHO characterized this as an “over-abundance of information — some accurate and some not — that makes it hard for people to find trustworthy sources and reliable guidance when they need it” in a report published in February. In response, social media companies have attempted to separate fact from fiction, with Twitter deleting COVID-19 misinformation that could cause physical harm and Facebook launching a new Messenger hub to highlight ways users can identify false or misleading information about the virus.

Dowden said the U.K. government is working directly with technology companies to step up these efforts.

“We’re working with social media companies, and I’ll be pressing them this week for further action to stem the spread of falsehoods and rumors [that] could cost lives,” he said.

False claims of potential vaccines and far-fetched notions that avoiding cold or spicy foods can help prevent the spread of COVID-19 have been shared widely across social media over the past few months. “Miracle cures” such as rinsing your mouth with a saline solution or drinking bleach have also reared their heads.

**The U.K. government said it is already identifying up to 70 incidents each week involving “false narratives” with multiple misleading claims, and its Rapid Response Unit will work to address any false claims that gain traction by issuing rebuttals on social media, asking platforms to remove the offending content, and promoting legitimate public health campaigns through “reliable sources.”**

### Canada Gets the DA Links

#### CP links to the DA – US follow-on triggers the link - Even if the US does not adopt the policy, it triggers a debate in Congress – NATO normal means

\*Also answers social media solvency deficits – system wide involves policy recommendations (which also go to associate member nations as a bonus!)

#### NATO Parliamentary Assembly, No Date

(NATO Parliamentary Assembly, NATO Parliamentary Assembly Content, No Date, “Policy Recommendations”, https://www.nato-pa.int/content/policy-recommendations, accessed 7-15-2022) SS:/

Policy recommendations represent formal statements of the Assembly's views. These are usually drafted in the Assembly's Committees before being discussed, amended and adopted by the full Assembly in plenary sitting at the annual session.

Occasionally, a policy recommendation is presented directly to the plenary sitting. This usually takes place if the subject is seen as being directly relevant to more than one Committee.

The policy recommendations are not binding, but are widely circulated to governments and parliaments of members and associate member nations.

NATO's Secretary General provides a written reaction to each of the policy recommendations.

## K Answers

### Scenario Planning Good

#### Scenario analysis is pedagogically valuable. It enhances creativity and self-reflexivity, deconstructs cognitive biases and flawed ontological assumptions, and enables the imagination and creation of alternative futures

Barma, Assistant Professor of National Security Affairs at the Naval Postgraduate School National Security Affairs professor, et al. 16

(Naazneen, Brent Durbin, PhD in Political Science from UC-Berkeley, Professor of Government at Smith College, Eric Lorber, JD from UPenn and PhD in Political Science from Duke, Gibson, Dunn & Crutcher, Rachel Whitlark, PhD in Political Science from GWU, Post-Doctoral Research Fellow with the Project on Managing the Atom and International Security Program within the Belfer Center for Science and International Affairs at Harvard, May 2016, International Studies Perspectives 17 (2), “‘Imagine a World in Which’: Using Scenarios in Political Science,”, pp. 1-6, <http://www.naazneenbarma.com/uploads/2/9/6/9/29695681/using_scenarios_in_political_science_isp_2015.pdf> accessed 7-16-22)

Over the past decade, the “cult of irrelevance” in political science scholarship has been lamented by a growing chorus (Putnam 2003; Nye 2009; Walt 2009). Prominent scholars of international affairs have diagnosed the roots of the gap between academia and policymaking, made the case for why political science research is valuable for policymaking, and offered a number of ideas for enhancing the policy relevance of scholarship in international relations and comparative politics (Walt 2005,2011; Mead 2010; Van Evera 2010; Jentleson and Ratner 2011; Gallucci 2012; Avey and Desch 2014). Building on these insights, several initiatives have been formed in the attempt to “bridge the gap.”2 Many of the specific efforts put in place by these projects focus on providing scholars with the skills, platforms, and networks to better communicate the findings and implications of their research to the policymaking community, a necessary and worthwhile objective for a field in which theoretical debates, methodological training, and publishing norms tend more and more toward the abstract and esoteric.¶

Yet enhancing communication between scholars and policymakers is only one component of bridging the gap between international affairs theory and practice. Another crucial component of this bridge is the generation of substantive research programs that are actually policy relevant—a challenge to which less concerted attention has been paid. The dual challenges of bridging the gap are especially acute for graduate students, a particular irony since many enter the discipline with the explicit hope of informing policy. In a field that has an admirable devotion to pedagogical self-reflection, strikingly little attention is paid to techniques for generating policy-relevant ideas for dissertation and other research topics. Although numerous articles and conference workshops are devoted to the importance of experiential and problem-based learning, especially through techniques of simulation that emulate policymaking processes (Loggins 2009; Butcher 2012; Glasgow 2012; Rothman 2012; DiCicco 2014), little has been written about the use of such techniques for generating and developing innovative research ideas.¶

This article outlines an experiential and problem-based approach to developing a political science research program using scenario analysis. It focuses especially on illuminating the research generation and pedagogical benefits of this technique by describing the use of scenarios in the annual New Era Foreign Policy Conference (NEFPC), which brings together doctoral students of international and comparative affairs who share a demonstrated interest in policy-relevant scholarship.3 In the introductory section, the article outlines the practice of scenario analysis and considers the utility of the technique in political science. We argue that scenario analysis should be viewed as a tool to stimulate problem-based learning for doctoral students and discuss the broader scholarly benefits of using scenarios to help generate research ideas. The second section details the manner in which NEFPC deploys scenario analysis. The third section reflects upon some of the concrete scholarly benefits that have been realized from the scenario format. The fourth section offers insights on the pedagogical potential associated with using scenarios in the classroom across levels of study. A brief conclusion reflects on the importance of developing specific techniques to aid those who wish to generate political science scholarship of relevance to the policy world.¶

What Are Scenarios and Why Use Them in Political Science?¶

Scenario analysis is perceived most commonly as a technique for examining the robustness of strategy. It can immerse decision makers in future states that go beyond conventional extrapolations of current trends, preparing them to take advantage of unexpected opportunities and to protect themselves from adverse exogenous shocks. The global petroleum company Shell, a pioneer of the technique, characterizes scenario analysis as the art of considering “what if” questions about possible future worlds. Scenario analysis is thus typically seen as serving the purposes of corporate planning or as a policy tool to be used in combination with simulations of decision making. Yet scenario analysis is not inherently limited to these uses. This section provides a brief overview of the practice of scenario analysis and the motivations underpinning its uses. It then makes a case for the utility of the technique for political science scholarship and describes how the scenarios deployed at NEFPC were created.¶

The Art of Scenario Analysis¶

We characterize scenario analysis as the art of juxtaposing current trends in unexpected combinations in order to articulate surprising and yet plausible futures, often referred to as “alternative worlds.” Scenarios are thus explicitly not forecasts or projections based on linear extrapolations of contemporary patterns, and they are not hypothesis-based expert predictions. Nor should they be equated with simulations, which are best characterized as functional representations of real institutions or decision-making processes (Asal 2005). Instead, they are depictions of possible future states of the world, offered together with a narrative of the driving causal forces and potential exogenous shocks that could lead to those futures. Good scenarios thus rely on explicit causal propositions that, independent of one another, are plausible—yet, when combined, suggest surprising and sometimes controversial future worlds. For example, few predicted the dramatic fall in oil prices toward the end of 2014. Yet independent driving forces, such as the shale gas revolution in the United States, China’s slowing economic growth, and declining conflict in major Middle Eastern oil producers such as Libya, were all recognized secular trends that—combined with OPEC’s decision not to take concerted action as prices began to decline—came together in an unexpected way.¶

While scenario analysis played a role in war gaming and strategic planning during the Cold War, the real antecedents of the contemporary practice are found in corporate futures studies of the late 1960s and early 1970s (Raskin et al. 2005). Scenario analysis was essentially initiated at Royal Dutch Shell in 1965, with the realization that the usual forecasting techniques and models were not capturing the rapidly changing environment in which the company operated (Wack 1985; Schwartz 1991). In particular, it had become evident that straight-line extrapolations of past global trends were inadequate for anticipating the evolving business environment. Shell-style scenario planning “helped break the habit, ingrained in most corporate planning, of assuming that the future will look much like the present” (Wilkinson and Kupers 2013, 4). Using scenario thinking, Shell anticipated the possibility of two Arab-induced oil shocks in the 1970s and hence was able to position itself for major disruptions in the global petroleum sector.¶ Building on its corporate roots, scenario analysis has become a standard policymaking tool. For example, the Project on Forward Engagement advocates linking systematic foresight, which it defines as the disciplined analysis of alternative futures, to planning and feedback loops to better equip the United States to meet contemporary governance challenges (Fuerth 2011). Another prominent application of scenario thinking is found in the National Intelligence Council’s series of Global Trends reports, issued every four years to aid policymakers in anticipating and planning for future challenges. These reports present a handful of “alternative worlds” approximately twenty years into the future, carefully constructed on the basis of emerging global trends, risks, and opportunities, and intended to stimulate thinking about geopolitical change and its effects.4 As with corporate scenario analysis, the technique can be used in foreign policymaking for long-range general planning purposes as well as for anticipating and coping with more narrow and immediate challenges. An example of the latter is the German Marshall Fund’s EuroFutures project, which uses four scenarios to map the potential consequences of the Euro-area financial crisis (German Marshall Fund 2013).¶

Several features make scenario analysis particularly useful for policymaking.5 Long-term global trends across a number of different realms—social, technological, environmental, economic, and political—combine in often-unexpected ways to produce unforeseen challenges. Yet the ability of decision makers to imagine, let alone prepare for, discontinuities in the policy realm is constrained by their existing mental models and maps. This limitation is exacerbated by well-known cognitive bias tendencies such as groupthink and confirmation bias (Jervis 1976; Janis 1982; Tetlock 2005). The power of scenarios lies in their ability to help individuals break out of conventional modes of thinking and analysis by introducing unusual combinations of trends and deliberate discontinuities in narratives about the future. Imagining alternative future worlds through a structured analytical process enables policymakers to envision and thereby adapt to something altogether different from the known present.¶

Designing Scenarios for Political Science Inquiry¶

The characteristics of scenario analysis that commend its use to policymakers also make it well suited to helping political scientists generate and develop policy-relevant research programs. Scenarios are essentially textured, plausible, and relevant stories that help us imagine how the future political-economic world could be different from the past in a manner that highlights policy challenges and opportunities. For example, terrorist organizations are a known threat that have captured the attention of the policy community, yet our responses to them tend to be linear and reactive. Scenarios that explore how seemingly unrelated vectors of change—the rise of a new peer competitor in the East that diverts strategic attention, volatile commodity prices that empower and disempower various state and nonstate actors in surprising ways, and the destabilizing effects of climate change or infectious disease pandemics—can be useful for illuminating the nature and limits of the terrorist threat in ways that may be missed by a narrower focus on recognized states and groups. By illuminating the potential strategic significance of specific and yet poorly understood opportunities and threats, scenario analysis helps to identify crucial gaps in our collective understanding of global politicaleconomic trends and dynamics. The notion of “exogeneity”—so prevalent in social science scholarship—applies to models of reality, not to reality itself. Very simply, scenario analysis can throw into sharp relief often-overlooked yet pressing questions in international affairs that demand focused investigation.¶

Scenarios thus offer, in principle, an innovative tool for developing a political science research agenda. In practice, achieving this objective requires careful tailoring of the approach. The specific scenario analysis technique we outline below was designed and refined to provide a structured experiential process for generating problem-based research questions with contemporary international policy relevance.6 The first step in the process of creating the scenario set described here was to identify important causal forces in contemporary global affairs. Consensus was not the goal; on the contrary, some of these causal statements represented competing theories about global change (e.g., a resurgence of the nation-state vs. border-evading globalizing forces). A major principle underpinning the transformation of these causal drivers into possible future worlds was to “simplify, then exaggerate” them, before fleshing out the emerging story with more details.7 Thus, the contours of the future world were drawn first in the scenario, with details about the possible pathways to that point filled in second. It is entirely possible, indeed probable, that some of the causal claims that turned into parts of scenarios were exaggerated so much as to be implausible, and that an unavoidable degree of bias or our own form of groupthink went into construction of the scenarios. One of the great strengths of scenario analysis, however, is that the scenario discussions themselves, as described below, lay bare these especially implausible claims and systematic biases.8¶ An explicit methodological approach underlies the written scenarios themselves as well as the analytical process around them—that of case-centered, structured, focused comparison, intended especially to shed light on new causal mechanisms (George and Bennett 2005). The use of scenarios is similar to counterfactual analysis in that it modifies certain variables in a given situation in order to analyze the resulting effects (Fearon 1991). Whereas counterfactuals are traditionally retrospective in nature and explore events that did not actually occur in the context of known history, our scenarios are deliberately forward-looking and are designed to explore potential futures that could unfold. As such, counterfactual analysis is especially well suited to identifying how individual events might expand or shift the “funnel of choices” available to political actors and thus lead to different historical outcomes (Nye 2005, 68–69), while forward-looking scenario analysis can better illuminate surprising intersections and sociopolitical dynamics without the perceptual constraints imposed by fine-grained historical knowledge. We see scenarios as a complementary resource for exploring these dynamics in international affairs, rather than as a replacement for counterfactual analysis, historical case studies, or other methodological tools.¶

In the scenario process developed for NEFPC, three distinct scenarios are employed, acting as cases for analytical comparison. Each scenario, as detailed below, includes a set of explicit “driving forces” which represent hypotheses about causal mechanisms worth investigating in evolving international affairs. The scenario analysis process itself employs templates (discussed further below) to serve as a graphical representation of a structured, focused investigation and thereby as the research tool for conducting case-centered comparative analysis (George and Bennett 2005). In essence, these templates articulate key observable implications within the alternative worlds of the scenarios and serve as a framework for capturing the data that emerge (King, Keohane, and Verba 1994). Finally, this structured, focused comparison serves as the basis for the cross-case session emerging from the scenario analysis that leads directly to the articulation of new research agendas.¶

The scenario process described here has thus been carefully designed to offer some guidance to policy-oriented graduate students who are otherwise left to the relatively unstructured norms by which political science dissertation ideas are typically developed. The initial articulation of a dissertation project is generally an idiosyncratic and personal undertaking (Useem 1997; Rothman 2008), whereby students might choose topics based on their coursework, their own previous policy exposure, or the topics studied by their advisors. Research agendas are thus typically developed by looking for “puzzles” in existing research programs (Kuhn 1996). Doctoral students also, understandably, often choose topics that are particularly amenable to garnering research funding. Conventional grant programs typically base their funding priorities on extrapolations from what has been important in the recent past—leading to, for example, the prevalence of Japan and Soviet studies in the mid-1980s or terrorism studies in the 2000s—in the absence of any alternative method for identifying questions of likely future significance.¶

The scenario approach to generating research ideas is grounded in the belief that these traditional approaches can be complemented by identifying questions likely to be of great empirical importance in the real world, even if these do not appear as puzzles in existing research programs or as clear extrapolations from past events. The scenarios analyzed at NEFPC envision alternative worlds that could develop in the medium (five to seven year) term and are designed to tease out issues scholars and policymakers may encounter in the relatively near future so that they can begin thinking critically about them now. This timeframe offers a period distant enough from the present as to avoid falling into current events analysis, but not so far into the future as to seem like science fiction. In imagining the worlds in which these scenarios might come to pass, participants learn strategies for avoiding failures of creativity and for overturning the assumptions that prevent scholars and analysts from anticipating and understanding the pivotal junctures that arise in international affairs.

## Disad Answers

### Politics – Countering Disinformation Politically Popular

#### Addressing disinformation in the cybersecurity context is politically popular

United States Cyberspace Solarium Commission, 21

[December 2021, Cyberspace Solarium Commission, “COUNTERING DISINFORMATION IN THE UNITED STATES, CSC White Paper #6,” <https://www.solarium.gov/public-communications/disinformation-white-paper>, p. 4, accessed 7-12-22]

INTRODUCTION – WHY DISINFORMATION IS A CYBERSPACE ISSUE

The United States Cyberspace Solarium Commission (CSC) was created by Congress in the National Defense Authorization Act (NDAA) for Fiscal Year 2019 to answer two fundamental questions: What strategic approach will defend the United States against cyberattacks of significant consequences? And what policies and legislation are required to implement that strategy? While disinformation is considered by some an issue largely separate from cybersecurity or network security,1 the Commission addressed disinformation in the very narrow context of elections in its final report in March 2020. As the COVID-19 pandemic swept across the globe, the Commission revisited the issue, this time in the context of disinformation about the pandemic itself, noting, “Our adversaries’ disinformation campaigns focused on the pandemic illustrate that disinformation activities can reach far beyond the political and electoral contexts with which Americans are best acquainted.”2

Over the course of the intervening months, the Commission received demand signals from constituents within Congress and the executive branch to treat the topic of disinformation and potential policy recommendations more extensively. The Commission has previously been reluctant to delve deeply into the topic of disinformation for two reasons.

First, disinformation as a policy issue, unlike many aspects of cybersecurity policy, has been marked by a strong partisan divide. Researchers have identified an association between strong partisanship and vulnerability to misinformation;3 more than two-thirds of U.S. citizens believe that Republicans and Democrats disagree about basic facts;4 and while U.S. citizens in both major parties agree that disinformation is a problem, they disagree about who is responsible for it and what ways to tackle the threat are appropriate.5 Although this partisan divide persists today, it is the sense of the members of the Commission that there is room to reach some agreement on core issues.

Second, as noted above, disinformation is seen by many as an issue largely separate from cybersecurity and cyber policy in the United States. While the Commission understands this view, continuing to bifurcate these issues has become untenable. From a strategic perspective, the United States and its policymakers do themselves a disservice by continuing to differentiate between the two when our adversaries do not.6

In order to craft a comprehensive strategy to defend the United States from cyberattacks of significant consequence, policy-makers must account for the entire arsenal employed by adversaries to cause harm in cyberspace, including information. It is also important to take a more operational or risk management perspective: disinformation campaigns waged against the United States by foreign actors are often carried out by many of the same threat actors as are active in cyberspace and are often the consequence of cyberattacks.

For these reasons, members of the Commission believe that elements of the topic of disinformation are within our mandate. This white paper is the result of deep research, interviews with experts, and deliberations by the Commission. It seeks to explain how the Commission’s proposed strategy of layered cyber deterrence applies to combating disinformation and contributes a set of policy recommendations to better position the United States to prevent, counter, and withstand the consequences of disinformation launched against it.