NCAFP

National Committee on American Foreign Policy

Fortifying the Future

Building Resilience in the Age of Disinformation

SUMMARY REPORT

This work is sponsored by NATO's Public Diplomacy Division

NCAFP

National Committee on American Foreign Policy

Acknowledgements

The National Committee on American Foreign Policy (NCAFP) is tremendously grateful to each of the panelists who participated in the discussions that informed this report. Furthermore, the NCAFP extends its thanks to Nicholas Thompson for the depth and insights he brought forth as the series' moderator.

This initiative saw significant contributions from several members of the NCAFP staff, including Mr. Stephen Whittaker, Ms. Erin O'Donnell, Mr. Sampson Oppedisano, and interns Ms. Sarah Moon and Ms. Lenna Giorgiadis.

This work was made possible by a generous grant from the Public Diplomacy Division of NATO.

The report presented here represents the notes and reflections of the authors alone and is not a consensus document, nor an expression of policy from NATO or any other organization.

Fortifying the Future

Building Resilience in the Age of Disinformation

SUMMARY REPORT

On **November 29** and **December 6**, 2021, the National Committee on American Foreign Policy hosted a two-part, public discussion series **Fortifying the Future: Building Resilience in the Age of Disinformation**. The series, which brought together experts with diverse public sector, business, media, military, and academic backgrounds, sought to bring greater awareness to, and lay out potential policy solutions for, the rampant problem of disinformation[1].

While social media channels and new technologies have rightly been lauded for their ability to foster community and bridge global divides, they can also create challenges when weaponized by nefarious actors. Disinformation campaigns are underway and routinely spread skepticism and animosity within civil society, the press, and, critically, between the public and their elected officials. Disinformation can easily and cheaply be used to persuade the public at an accelerated and dangerous rate, just as the very algorithms utilized by digital platforms inadvertently encourage the sharing of false information.

The first event, focused on U.S. policy, emphasized how the public and private sectors could work in tandem to reduce threats and discussed some potential paths to mitigating the threat of disinformation. The second, taking a more Europe-centric approach, looked at disinformation in a broader context and worked to place it within the competing priorities and policy frameworks of national and multilateral governance.

The report that follows here is a summation of the discussions held over the two public sessions. It outlines the key issues at hand and navigates the potential means to build resilience against an amorphous threat. Key policy recommendations drawn from the discussions are noted at the conclusion.

1 Disinformation: the deliberate intent to spread misinformation or false information

The Scope of the Threat

Central to the discussions held on November 29 and December 6 was assessing the scope of the threat presented by disinformation. The disinformation "toolkit" is varied, and creating false or misleading information can take different shapes. Thus, the scope of the issue at hand is vast, running the gamut from mere nuisance all the way to near-existentially damaging. Disinformation can influence behavior, political and tactical decisions, and can arguably shape otherwise democratic processes if left unchecked. It is not a new problem—some would argue it is the evolution of techniques and tactics used extensively during the Cold War—but it is made easier, cheaper, and accessible to even non-state actors through the proliferation of certain technologies.

> *"COVID-19 has dominated the disinformation landscape for the past two years…it accelerated the ability of disinformation actors to cooperate, it accelerated their ability to exploit fears of society, and it accelerated their creativity."*
>
> **– Dominika Hajdu**

The spread of disinformation has been a problem facing the internet since its inception, as the connectivity of the web, particularly with the advent of social media, allows for the amplification of voices across it. The COVID-19 pandemic created an opportunity for malicious actors to double-down on their nefarious behavior and has even seen the emergence of cooperation in a space where it did not previously exist. Sources and materials from across the web, provided not only by users within countries such as China and Russia, but also the United States and Europe, are proliferating and creating an information space that, in the context of a global pandemic, can literally provide narratives—health advice even—that can result in death if taken as truth.

Though this "destructive" disinformation is commonplace and not new to the internet, the information marketplace is now seeing efforts to create "constructive" disinformation through which state actors and others are attempting to create narratives serving a proactive purpose. In some instances, this may be used to advance the efficacy of a less-than-effective vaccine or to serve as a form of propaganda meant to boost the standing of a state actor in a foreign nation.

The scope of the disinformation threat is large, and there is no one-size-fits-all approach, or silver bullet for solving the problem.

Disincentivizing and Demonetizing the Disinformation Economy

A recurring sentiment from the experts engaged in the November 29 and December 6 discussions centered on the importance of both disincentivizing and demonetizing the disinformation economy. Importantly, several framed the entire disinformation space in succinct economic terms, seeing it as a marketplace governed by supply and demand. In fact, it is common for social media platforms, in particular, to optimize their algorithms and technologies for the highest possible level of engagement. This serves to amplify the loudest voices, which inadvertently creates negative externalities. High levels of engagement raise profit for both the platforms and the content creators. However, if one can attack this primary driver of disinformation—financial gain—and take that incentive away, a large volume of malicious content can be taken off the board, so to speak.

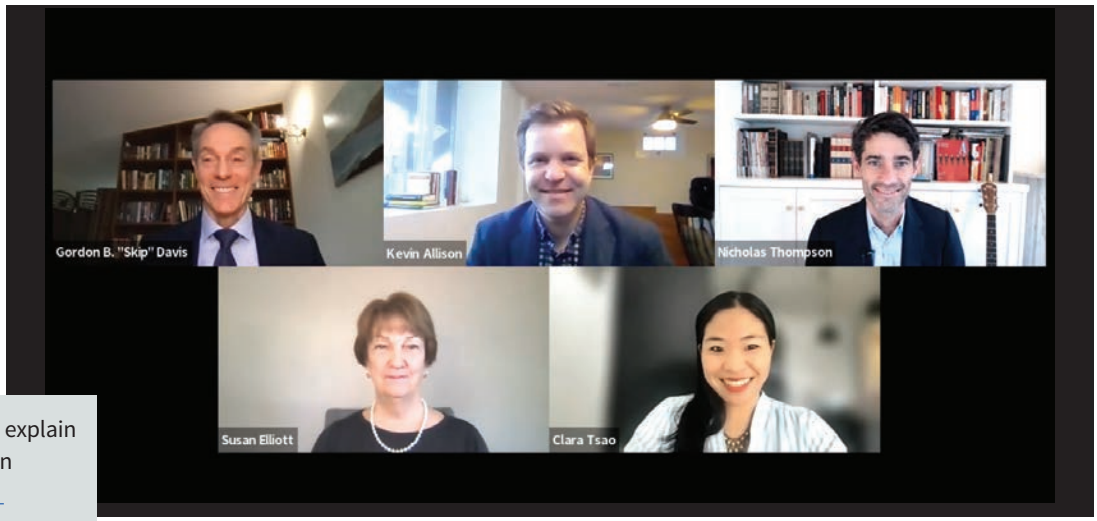
> *"Disinformation is dangerous not only for geopolitical reasons but also for practical individual security and human health."*
>
> **– Jakub Janda**

This is not a simple task, but it can be approached in several ways. First, engaging with advertisers to limit or pull spending from platforms known to spread disinformation can generate pressure to change industry or site-specific practices. Further, creating a counter-disinformation economy to raise the cost of doing business for nefarious actors can levy considerable financial burden. Bounty programs and law enforcement seizure of ransom payments are just two clear steps toward creating this alternative economy that demonetizes the extant one.

Ultimately, banning platforms or de-platforming specific actors may not provide enough of an impact in the long term. Those committed to operating in the information space are likely to find workarounds for such tactics. When they are hit in their wallets, however, behavior may start to change.

The Whole-of-Society Approach

The push to disincentivize and demonetize is vitally important, but bolstering resilience against disinformation also requires a broader suite of changes in both method and practice. Essential to tackling the issue will be a whole-of-society approach.



Session I Panelists explain the disinformation economy. See the entire session.

The above points regarding disincentivizing platforms and content creators go hand-in-hand with the necessity of crafting solutions in cooperation with the very platforms on which disinformation is shared. The most significant social media and "Big Tech" companies are deeply entrenched within the global economy and are here to stay, thus, they must be part of the solution. Governments and other society actors should view the private sector as potential partners rather than adversaries.

The media plays an essential role in building resilience against disinformation as well. Journalists were long held to be the gatekeepers to public knowledge and information, yet trust in the media is plummeting and punditry is proliferating across not only the United States and Europe, but globally. The disinformation economy plays a key role here again, as the same optimization for engagement that drives the dissemination of false information across tech platforms promotes a media environment in which it is rewarding to do the same. Often, the relevance of a news organization is measured by its click rate and metrics for public engagement—and nothing drives engagement quite as well as a polarizing story of dubious origin.

Education and civil society are also vital in combating disinformation, with a particular need in regions such as Central and Eastern Europe to foster critical thinking and a more complete understanding of history to build a bulwark against false narratives. Both educational institutions and civil society actors can press for greater media literacy and a strengthening of engagement with the concept of legitimacy—noting that it is possible that not all sides of a story or issue need be explored.

Problematically, these sociological and broad-based approaches are difficult to implement and require enormous political cachet to move with meaningful impact. This creates a need to engage with government at all levels to advance projects and policy initiatives forward. Crossing sectoral lines, business interests, media attention, and bureaucratic capabilities is required to have effective long-term, sustainable impact in combating disinformation. The sharing of information, intelligence, and experience throughout this whole-of-society approach will also be necessary, and building the trust to do so starts at the top.

The Knowledge Gap

A fundamental difficulty with managing the problem of disinformation at the highest levels of government and international organizations is simply the lack of trained and experienced experts connected to key decision-makers. Furthermore, the lines of communication within government are often unclear regarding where you turn when faced with a disinformation-related issue that must be addressed. The confusion not only exists within single governments, but also crosses borders, as a knowledge gap also exists between states.

Identifying, tracking, and countering disinformation requires a diverse skillset. Those with the skills needed to operate effectively in this space are often employed by the private sector or have training in some of the needed fields but not others. This problem can be addressed in a multitude of ways, including secondments and staff exchanges, up through professional training and certification programs that standardize best practices and knowledge. Ultimately, a coordinated approach between the United States and partners in Europe and elsewhere can create standards and norms in an industry that is ever-changing and in need of attention.

Bridging the knowledge gap both within and between governments is also essential and overdue. The European Union and many of its member states are seeing a greater need to compete in the information sphere and on the ground in tackling problems such as disinformation, but they can only do so through coordinated efforts. Information and intelligence sharing, and cross-training through established channels, such as those created through the NATO Alliance, are steps in the right direction. Further, Taiwan, as an example, is a global leader in government-led responses to disinformation and hostile information activities. They have created an innovative “Digital Minister” position in their government and have established clear policies focused on the identification, response to, and removal of disinformation within two hours of it surfacing. European leaders have been slow to engage Taiwan for a variety of reasons, and the United States has not adopted any of their innovative practices, but there are excellent opportunities to engage in greater cooperation and mutual education.

The establishment of new and bespoke government agencies or departments can also provide a more centralized hub of knowledge, or a place to direct relevant inquiries. Sweden stands out as an example of a country working toward creating a government department dedicated to the challenges created by disinformation and other concerns in the information space. Ultimately, streamlining expertise and communications across government by any means would be a welcome change.

Regulation and Government Controls

The setting of regulations and government controls is also an important component of building resilience against disinformation. The amorphous nature of the threat creates problems in establishing a regulatory framework for it—notably because many of its most troubling iterations are legal. The European Commission and other bodies in Europe are taking steps toward platform regulation, in particular, through efforts to guide recommendation systems, hardening the rules around political advertising, and other systemic changes. Further, the EU serves as a global leader in privacy legislation. This protection of user data can be used to prevent foreign actors from establishing dominance in the information space and engaging in the practice of micro-targeting by limiting the flow of personal data available to them.

Efforts dedicated to regulating the information space need not only take the shape of government intervention. It is also possible, and should be encouraged, that industry groups and trade associations establish baselines and standards among themselves. The creation of Bar Association-like regulatory bodies for professionals working in this space not only can provide needed training, but they can also set the tone for the entire industry. Rules of the road related to disinformation are sorely needed, whether they come from a government or industry body.

Regulations and controls can also be put in place to establish a greater degree of transparency regarding lobbying and foreign engagement. The United States' Foreign Agents Registration Act provides a sound model that could be emulated by European nations and others in seeking to build resilience against disinformation threats not only coming from abroad, but within their own borders.

Threats Within

Though often framed as an entirely external threat, a tremendous amount of disinformation impacting Europe and the United States is homegrown. The circumstances that lay the groundwork for eager acceptance of false narratives, or that drive polarization within communities, are often definitively domestic. Foreign actors may be good at exploiting domestic flaws and concerns, but those flaws and concerns were born and raised at home. Building resilience against disinformation requires engaging with the deepest challenges internal to societies as well.

Driven by a proliferation of conspirators spreading information found online, disinformation flows freely from the accounts of many, including political leaders. Often shared widely by

Session II Panelists discuss ways to counter false narratives. See the entire session.

far-right parties or actors in Europe and the United States, the wide use of local languages and context in many examples points to sourcing from like-minded domestic channels.

A vital step in pushing back against disinformation threats from within also includes rooting out corruption and challenging kleptocracy. Many of the most zealous purveyors of disinformation do so from a corrupted position, either in furtherance of a malign agenda or to yield financial gain. Treating corruption as a root cause of disinformation through the implementation of regulatory or penal sanctions is not only necessary but overdue. Of particular note is the practice of anticipated corruption. Well-established actors in government or other positions of power are often rewarded for spreading disinformation through lucrative speaking fees or plum corporate positions controlled by the purveyors of the false information. These practices can and should be regulated—as they are at the EU level—by national governments. Until corrupt actors and practices can be rooted out, it will persistently be difficult to counter the narratives created by disinformation.

Countering the Narrative

In conjunction with actions meant to disincentivize its spread, and within the whole-of-society-approach is also the need to counter disinformation. It is unrealistic to expect the disseminators of false information to stop completely, particularly when they are state-level actors with whom there is little leverage to change the behaviors in question. Taking on this challenge requires a framework for response—a playbook—through which coordinated efforts in the establishment of guardrails and norms set clear redlines and boundaries. There is not necessarily a need to engage in a tit-for-tat kinetic or even virtual response if there is an established escalation ladder that can offer the appropriate signals and/or deterrent measures to instigate a mutual backing-down.

It is possible to negotiate terms and conditions in this space, and some suggest looking to the legacy of the Cold War for answers. Responses to largely digital confrontations need not necessarily follow the legacy of that era's nuclear agreements to the letter, but they provide important precedent for negotiating and coming to an understanding of normative behavior involving dangerous technologies. Nations and international organizations, notably NATO through its Article V provisions, clearly elicit their potential responses to kinetic action. They are less adept at signaling or taking appropriate action in the cyber or information space. It is within this response gap that partnerships and deepened cooperation between states and organizations can be forged to take advantage of what potential partners simply do better. NATO has a considerable role to play here, as avenues for cooperation already exist within the Alliance, and deterrence frameworks can be formed and adopted across its 30 member states.

Ultimately, however, countering the narratives created by disinformation should not be overlooked as a matter of sound strategic communication and well-rounded public diplomacy efforts. Before creating frameworks for response, it is vital to consider reciprocity and proactive foreign policy. Experimenting with and pushing out new types of programming on public news networks to counter those of adversaries, helping civil society to move media away from a pundit economy, and offering forums in which disinformation can be readily and publicly refuted are just a few steps that need to be taken to halt it before it can diffuse.

Conclusions

The challenge of building resilience against disinformation is one that is multifaceted. As discussed during the National Committee on American Foreign Policy's two-part event series Fortifying the Future, it is essential to disincentivize and demonetize the disinformation economy; to recognize that resilience requires a whole-of-society approach that addresses knowledge gaps, regulatory hurdles, and domestic threats; and that steps should be taken to counter the narratives created by disinformation proactively, and through the establishment of reactive response frameworks.

It is crucial to continue an open dialogue among allies, partners, and even adversaries on this topic. The spread of disinformation and false narratives may not be a new phenomenon, but through international engagement and a deepened understanding of new technologies, new approaches to creating more resilient societies may be found.

Policy Recommendations

The recommendations below are meant to serve as general guidance for policymakers and thought leaders in the United States, Europe, NATO, and other like-minded international organizations.

- **Deepen the Counter-Disinformation Economy**
  - Strengthen bounty programs in cooperation with tech platforms
  - Enhance the ability of law enforcement to seize ransom payments
  - Sanction individuals to whom disinformation can be attributed
- **Close the Knowledge Gap**
  - Incentivize private sector secondment and/or professional exchange programs between governments, international organizations, and technology companies
  - Establish professional and industry associations to standardize and enhance training and professional opportunities in the data, tech, and information sectors
  - Strengthen cross-border collaboration and intelligence and information sharing
- **Disrupt Domestic Threats**
  - Bolster anti-corruption legislation, including "revolving door" policies that disallow or disincentivize the rapid movement of public officials into lobbying or business interests tied to their portfolios
  - Establish and/or strengthen Foreign Agents Registration Act-type legislation to enhance transparency
- **Counter the Narrative**
  - In conjunction with allies and partners, establish agreed-upon response frameworks for managing reactions to nefarious action
  - Develop counter-programming through public channels to disrupt false narratives pressed by foreign news sources or online platforms
  - Establish forums, such as EUvsDisinfo, where disinformation can be publicly refuted

Event Panelists

Kevin Allison
Director, Geo-Technology
Eurasia Group

MG (ret.) Gordan B. "Skip" Davis
Senior Fellow, Transatlantic Defense and Security
Center for European Policy Analysis

Benjamin Haddad
Senior Director, Europe Center
Atlantic Council

Dominika Hajdu
Policy Director, Centre for Democracy and Resilience
GLOBSEC Policy Institute

Jakub Janda
Director
European Values Center for Security Policy

James Pamment
Associate Professor
Lund University

Clara Tsao
Co-Founder and Board Member
Trust & Safety Professional Association

Moderator

Nicholas Thompson
CEO, The Atlantic

About the NCAFP

The National Committee on American Foreign Policy (NCAFP) identifies, articulates, and helps advance American foreign policy interests from a nonpartisan perspective within the framework of political realism. Founded in 1974 by Professor Hans J. Morgenthau and others, the NCAFP is a nonprofit policy organization dedicated to the resolution of conflicts that threaten U.S. interests.

The NCAFP fulfills its mission through Track I ½ and Track II diplomacy. These closed door and off-the-record conferences provide opportunities for senior U.S. and foreign officials, subject experts, and scholars to engage in discussions designed to defuse conflict, build confidence, and resolve problems. Believing that an informed public is vital to a democratic society, the NCAFP offers educational programs and issues a variety of publications that address security challenges facing the United States.

Connect with Us Online!

www.ncafp.org

twitter.com/NATLCOMMITTEE

facebook.com/NATLCOMMITTEE