



# Ensuring A Digitally Secure Europe: Combatting mis- and disinformation in the Comprehensive New European Architecture

*by Elliot Gerson*



Elliot Gerson is Executive Vice President, The Aspen Institute.

**M**is- and disinformation have subverted societies around the world. While the globalization and democratization of information sharing through digital devices have brought our world closer together, we must contend with the ways this era of instant communication has been weaponized to drive us apart. Through the lens of the Russian war in Ukraine, we can see the way in which disinformation can penetrate societies and be used as a tool of war by both state and non-state actors. Disinformation has been key in disrupting digital ecosystems to shape public narratives and perceptions about the war. As we begin to consider the reconstruction of Ukraine and a Comprehensive New European Architecture, we must be prepared to account for the effects of mis- and disinformation on international security and democracy.

## **A Modern Tool of War: Disinformation**

Mis- and disinformation's role in undermining democracy<sup>1</sup> and provoking conflict around the world<sup>2</sup> it is one of the most significant challenges of the 21st century.<sup>3</sup> Disinformation has the power to disrupt the fabric of society, provoke mistrust, incite violence<sup>4</sup>, influence policy, and meddle with elections.<sup>5</sup> In the Russian war in Ukraine, we see

---

<sup>1</sup> <https://www.reuters.com/article/us-brazil-election-whatsapp-explainer/facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-idUSKCN1MU0UP>

<sup>2</sup> [https://www.wilsoncenter.org/sites/default/files/media/documents/publication/vulnerable\\_landscapes\\_case\\_studies.pdf](https://www.wilsoncenter.org/sites/default/files/media/documents/publication/vulnerable_landscapes_case_studies.pdf)

<sup>3</sup> [https://www.foreignaffairs.com/articles/world/2021-11-30/how-disinformation-corrodes-democracy?check\\_logged\\_in=1&utm\\_medium=promo\\_email&utm\\_source=lo\\_flows&utm\\_campaign=registered\\_user\\_welcome&utm\\_term=email\\_1&utm\\_content=20220831](https://www.foreignaffairs.com/articles/world/2021-11-30/how-disinformation-corrodes-democracy?check_logged_in=1&utm_medium=promo_email&utm_source=lo_flows&utm_campaign=registered_user_welcome&utm_term=email_1&utm_content=20220831)

<sup>4</sup> [https://www.wilsoncenter.org/sites/default/files/media/documents/publication/vulnerable\\_landscapes\\_case\\_studies.pdf](https://www.wilsoncenter.org/sites/default/files/media/documents/publication/vulnerable_landscapes_case_studies.pdf)

<sup>5</sup> <https://www.reuters.com/article/us-brazil-election-whatsapp-explainer/facebooks-whatsapp-flooded-with-fake-news-in-brazil-election-idUSKCN1MU0UP>

---

the global extent of disinformation campaigns. Coordinated campaigns by Putin-allied actors aim to sow division among allies of Ukraine through “whataboutisms”, doctored images and videos, and false historical narratives. Ironically, Russian disinformation campaigns use social media blocked within Russia to spread disinformation to other countries.

## The Path to a Digitally Secure Europe

Disinformation campaigns from Russia - and increasingly from China, Iran and other state actors - are a persistent threat that Europe will need to combat as it creates a **Comprehensive New European Architecture**. Throughout the Russian war in Ukraine, harmful narratives have affected public opinion in Europe and beyond in an attempt to undermine democratic norms and friendly Western relations. As Ukraine begins to rebuild and Europe considers how to strengthen its security, information disorder must be addressed.

Members in the European Union (EU) and the North Atlantic Treaty Organization (NATO) have each taken meaningful actions to combat disinformation. In June, the European Commission’s signatories of the 2018 Code of Practice on Disinformation strengthened the Code’s commitments to regulating digital platforms.<sup>1</sup> The improved Code of Practice also includes a new framework for monitoring the implementation of the Code and establishing a Transparency Centre, where the public can view policies implemented by signatories of the Code and other relevant metrics on disinformation in digital media.

NATO has also held a close focus on disinformation. In May 2022, NATO held its first meeting dedicated to discussing the cyber threat landscape following the war in Ukraine.<sup>2</sup> Also in 2022, NATO scientists wrote a book on “lessons learned” and key strategies to combat disinformation.

Similarly civil society groups and academic researchers are collaborating to understand and advance recommended solutions to mitigate harmful information and increase public resilience to negative influence. The Aspen Institute has been

---

<sup>6</sup> <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

<sup>7</sup> <https://thehill.com/policy/cybersecurity/3493265-nato-cyber-coordinators-hold-first-ever-meeting-amid-russias-invasion/>

---

active in this space. This past year, the Institute's [Aspen Digital program](#) formed **The Commission on Information Disorder**, to “identify and prioritize the most critical sources and causes of information disorder and deliver a set of short-term actions and longer-term goals.”<sup>1</sup> While largely focused on the US context, its findings and suggestions could be applicable to Europe and contribute to ongoing conversations about practical methods to combat disinformation. Taking from the Commission's report, I emphasize three areas that should be of priority on the path to a digitally secure Europe. They are as follows: **increasing transparency, building trust, and reducing harms.**

## The Commission's Recommendations

The Commission's first set of recommendations focused on battling mis- and disinformation is to **increase transparency** efforts on social media platforms by enacting federal protections for researchers and journalists conducting research for the greater public good. Recently, some social media platforms adjusted their terms of service to block access to researchers. Social media transparency is pivotal to developing public policy solutions that can actively combat mis- and disinformation efforts. The commission says, “While the protection of user privacy is important, platforms should not be permitted to use privacy as a pretext for restricting and stopping research and journalism in cases where the risk to privacy is minimal in relation to the public interest in the research, as Stanford professor Nate Persily has proposed.” Another effort to increase transparency involves federal action that would require social media platforms to publish key data such as content, source account, and reach data for organically delivered posts. This recommendation is particularly important in battling disinformation campaigns where their primary place of attack is through social media platforms. This required public disclosure allows key experts to analyze and decipher potentially harmful posts as well as provide informative counteractions to the disinformation identified.

The second set of recommendations is around **building trust** in an increasingly polarized society. The Commission's report highlights the need for truth and transformation. Often mis- and disinformation target marginalized groups or

---

<sup>1</sup> <https://www.aspeninstitute.org/programs/commission-on-information-disorder/>

---

communities, making it ever-more important to identify imbalances of power, access, and equity and for news outlets and social media platforms to diversify their workforces. Part of building this trust includes greater workforce diversity, to include a range of perspectives in positions of power, particularly in the media. It also includes developing platforms that center healthy discourse and privilege truth over amplifying extreme views; investment in local journalism, to strengthen their capacity to deliver balanced information to those who need it most; education campaigns centered on our election processes, to restore trust and resiliency in our democratic institutions; and a cultural shift toward holding those who violate the public trust accountable through professional standards bodies. Another method could be withholding advertisement support from platforms that fail to protect their users from harmful information or encouraging existing media companies to implement practices that give their users fact-based information.

To impact the root causes of this issue, we must also elevate initiatives that focus on reconciliation, community building, and remedy longstanding inequities faced by marginalized groups. By acknowledging that our structural inequities have created an environment of distrust in marginalized communities and working to alleviate and elevate marginalized voices, our communities will be built on a foundation of mutual respect and understanding where mis- and disinformation cannot take hold.

Finally, to **reduce harms**, the Commission identified several approaches from the national to civic scale. They suggested that the US administration create a comprehensive federal approach that would result in a national strategic plan to combat mis- and disinformation. A national strategy led by a nonpartisan team could fund powerful countermeasures like the education, research, and local media investments identified above. A clear position from the federal government would encourage social media platforms to take more accountability for the messages spread on their platforms by holding “superspreaders” of mis- and disinformation accountable, create a higher standard of care to prevent targeted harassment and harmful promoted content, and by providing media literacy education to their users.

All sectors of society, and all of us around the globe, have a shared responsibility to work together to combat this persistent challenge of mis- and disinformation. It is especially important for European nations to prioritize focus on these dangerous

---

disinformation campaigns during the Russian war in Ukraine. These campaigns are targeting fear in the general public and highlighting government failures to cause chaos and raise sympathy for Russia. **A New Comprehensive European Architecture is one that recognizes that disinformation campaigns go far beyond false narratives on social media, but that it is a dangerous tool of war that can affect social order, nation relationships, democracy, and international security.**

I commend the work of the Aspen Institute's Aspen Digital Commission on Information Disorder as well as the Institute's current work being done in Europe for their extensive efforts in identifying actionable solutions to combat this persistent challenge. While this Commission's report had a US focus, their findings are sparking conversations and encouraging questions within European spaces as officials work to create the New Comprehensive European Architecture. The Aspen Institute and its international network are dedicated to combating mis- and disinformation to promote a more just and democratic society. The full report from the Commission may be found [here](#).