Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Inez Miyamoto, *Connections QJ* 20, no. 2 (2021): 47-55
https://doi.org/10.11610/Connections.20.2.05

Research Article

Disinformation: Policy Responses to Building Citizen Resiliency

Inez Miyamoto

Daniel K. Inouye Asia Pacific Center for Security Studies

Abstract: Maligned actors use fake social media accounts and automated tools, also called computational propaganda, to launch disinformation operations. While technology companies and researchers continue to advance computational propaganda detection, they also know that eradicating social bots and disinformation is impossible. Since computational propaganda continues to increase, governments need to focus their efforts on developing policies that decrease citizen demand for disinformation. The purpose of this article is to explore disinformation at the intersection between technology and citizen resiliency. First, the current landscape will be explored to understand the impact of disinformation on society and its citizens. Second, the effect of technology on the supply of disinformation will be examined. Third, methods to decrease the demand for disinformation will be considered to increase citizen resiliency.

Keywords: disinformation, digital literacy, citizen resilience.

Introduction

With the growth of social media, there is a flood of unregulated content available on the Internet. Gone are socially-responsible publishers, editors, and subject matter experts to evaluate information that was available with traditional media.[1] Instead, citizens are left to decide what is fake or real, while maligned actors leverage this opportunity, along with the openness of democracies, to influence societies with disinformation. Disinformation is defined as the purposeful use of

[1] Institute for the Study of Diplomacy, *The New Weapon of Choice: Technology and Information Operations Today* (Washington: Institute for the Study of Diplomacy, October 2020), https://georgetown.app.box.com/s/ivwz4irk3un8blngm3wo0t3uwfc6hpz8.

false information created and spread intentionally as a way to confuse or mislead, which may contain a blend of truth and untruth or purposefully exclude context.[2] Governments need to focus their efforts on developing policies to decrease citizen demand for disinformation because controlling the supply of disinformation is a formidable task when machines are increasingly creating the content.

Governments, civil society groups, and technology companies recognize disinformation as a global problem, but they struggle with their responses. Malign actors sow discord and distrust using newer and better tools, leaving citizens, who are the target of disinformation operations, worried about the impact of disinformation on the Internet. Knuutila and colleagues found that 53% of regular internet users (154,195 respondents in 142 countries) were concerned about encountering disinformation online, with the highest concern (65%) coming from North America.[3] They were more concerned about disinformation than online fraud or harassment.

This article examines disinformation at the intersection between technology and citizen resiliency. First, the current landscape will be explored to understand the impact of disinformation on society and its citizens. Second, after examining the impact of technology on the supply-side of disinformation, the demand-side of disinformation is examined for citizen resiliency. Finally, this article concludes with policy recommendations for starting a citizen resiliency program.

Computational Propaganda

Malign actors use fake social media accounts and automated tools, also called computational propaganda, to launch disinformation operations. Woolley and Howard (2016) define computation propaganda as "algorithms, automation, and human curation to purposefully distribute misleading information over social media networks."[4] As an illustration, the computational propaganda tools include bots, sock puppets, robo-trolls, and deepfake videos.

First, bots—short for robots—are software programs with legitimate uses, such as automating tasks on websites. In disinformation operations, social media bots impersonate a human on social media by communicating and interacting

---

[2] Samantha Bradshaw and Lisa-Maria Neudert, "The Road Ahead: Mapping Civil Society Responses to Disinformation," Working Paper (Washington: National Endowment for Democracy, January 2021), https://www.ned.org/mapping-civil-society-responses-to-disinformation-international-forum.

[3] Aleksi Knuutila, Lisa-Maria Neudert, and Philip N. Howard, "Global Fears of Disinformation: Perceived Internet and Social Media Harms in 142 Countries," COMPROP Data Memo 2020.8, December 15, 2020, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2020/12/Global-Fears-of-Disinformation-v.13.pdf.

[4] Samuel C. Woolley and Philip N. Howard, "Automation, Algorithms, and Politics: Political Communication, Computational Propaganda, and Autonomous Agents – Introduction," *International Journal of Communication* 10 (2016), https://ijoc.org/index.php/ijoc/article/view/6298.

with people and systems. For example, they can be social bots, which are fake, automated accounts, or cyborgs, which are accounts operated by a human with bot technology assistance. Malign actors also use a massive number of social media bots to create the illusion of large-scale consensus for online propaganda.[5]

Second, sock accounts or sock puppets are fictitious online accounts created by an individual or group with an intent to deceive. For example, an individual or group will create multiple accounts on a social media platform to influence social media by generating followers by "liking" or voting on posts. They can also slant or distort an online discussion or support a particular online account. As a case in point, Russian intelligence operated a Twitter sock account under the name of Jenna Abrams, which had 70,000 followers, to influence conservative voters during the 2016 US elections.[6]

Third, trolls are real individuals who intentionally provoke others online by posting inflammatory or offensive messages. When their accounts are automated through the use of software, they are called robo-trolls and are capable of generating content.[7] Researchers are concerned about the use of robo-trolls by extremists or terrorists. Therefore, they are testing text-generating artificial intelligence (AI) software, which could be used in the future by robo-trolls.[8] The text-generating AI software would be a powerful tool for extremists or terrorists because they could speedily create propaganda, which at present is manually created by humans and thus a time-intensive process.

Fourth, AI-enabled tools allow the creation of deepfake videos – digitally altered videos used for deceptive purposes. According to Sensity AI (formerly DeepTrace), the amount of deepfake videos is increasing, with 96% of online deepfake videos consisting of non-consensual, celebrity pornography.[9] Experts believe these videos will continue to grow in numbers and sophistication as more

---

5 Samuel C. Woolley and Philip N. Howard, "Computational Propaganda Worldwide: Executive Summary," Working Paper No. 2017.11 (Oxford: University of Oxford, 2017), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/06/Casestudies-ExecutiveSummary.pdf.

6 Ben Collins and Joseph Cox, "Jenna Abrams, Russia's Clown Troll Princess, Duped the Mainstream Media and the World," *The Daily Beast*, November 3, 2017, https://www.thedailybeast.com/jenna-abrams-russias-clown-troll-princess-duped-the-mainstream-media-and-the-world.

7 Tom Simonite, "To See the Future of Disinformation, You Build Robo-Trolls: AI-Powered Software Is Getting Better and Could Soon Be Weaponized for Online Disinformation," *Wired*, November 19, 2019, https://www.wired.com/story/to-see-the-future-of-disinformation-you-build-robo-trolls.

8 Simonite, "To See the Future of Disinformation, You Build Robo-Trolls."

9 Henry Ajder, Giorgio Patrini, Francesco Cavalli, and Laurence Cullen, *The State of Deepfakes: Landscape, Threats and Impact* (Amsterdam: Deeptrace, 2019), https://sensity.ai/reports/.

deepfake services and tools become available to the public.[10] Even now, high-quality deepfake videos are difficult to detect.[11]

In response to increasing computational propaganda, technology companies began deploying AI-enabled countermeasures. As companies became better at detecting and blocking bots, bot developers began using more sophisticated techniques, such as AI-generated images, text, and videos.[12] In view of the fact that synthetically-generated content mimics a human's style, distinguishing AI content from human-generated content is challenging.[13] And recent social bots are more similar to human-operated accounts because AI is being used to create a hybrid of automated and human-driven behaviors."[14] Compounding this problem is the fact that malign actors are able to weave true information with false information, making it even more difficult for technology companies to label disinformation as truthful or untruthful.[15] Consequently, in the future, it will be impossible for citizens to determine the veracity of information or legitimacy of accounts.

Meanwhile, computation propaganda is increasing globally. Bradshaw et al. noted that state and political actors in 81 countries are using social media to spread computational propaganda.[16] This increase is problematic because computational propaganda is a "powerful tool that can undermine democracy."[17,18] While technology companies and researchers continue to advance computational propaganda detection, they also know that eradicating social bots and disinformation is impossible. Instead, a whole-of-society approach is necessary to build citizen resilience against a growing threat that is undermining societal trust.

---

10 Ajder, Patrini, Cavalli, and Cullen, *The State of Deepfakes.*

11 Matt Groh, "DetectDeepFakes: How to Counteract Misinformation Created by AI," accessed January 28, 2021, www.media.mit.edu/projects/detect-fakes/overview.

12 Stefano Cresci, "A Decade of Social Bot Detection," *Communications of the ACM* 63, no. 10 (October 2020): 72-83, https://doi.org/10.1145/3409116.

13 Renée DiResta, "The Supply of Disinformation Will Soon Be Infinite: Disinformation Campaigns Used to Require a Lot of Human Effort, but Artificial Intelligence Will Take Them to a Whole New Level," *The Atlantic*, September 20, 2020, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400.

14 Cresci, "A Decade of Social Bot Detection."

15 Kate Starbird, "Disinformation's Spread: Bots, Trolls, and All of Us," *Nature* 571, no. 449 (2019), https://doi.org/10.1038/d41586-019-02235-x.

16 Samantha Bradshaw, Hannah Bailey, and Philip N. Howard, *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation* (Oxford: University of Oxford, 2021), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report20-FINALv.3.pdf.

17 Woolley and Howard, "Computational Propaganda Worldwide."

18 Stanford History Education Group (SHEG), "Evaluating Information: The Cornerstone of Civic Online Reasoning," Working Paper (Stanford: SHEG, 2016), https://stacks.stanford.edu/file/druid:fv751yt5934/SHEG%20Evaluating%20Information%20Online.pdf.

Governments are responding to disinformation from both sides of the supply-demand equation. The supply-side of disinformation involves limiting the flow of disinformation into the information ecosystem. The demand-side involves addressing citizen consumption of disinformation.[19] Next, this article explores both sides of the supply-demand equation of disinformation.

Supply-Side of Disinformation

Without a doubt, tackling the supply-side of disinformation necessitates the government, technology companies, and civil society to work together to develop a whole-of-society response. From a policymaker's perspective, countering supply-side disinformation is challenging because there may not be a lead agency responsible for countering disinformation operations. For this reason, a country may not have a coordinated policy response. Consequently, when there is a disinformation attack on domestic affairs (e.g., election security, disasters, pandemic response and vaccinations), the functional agency may not be equipped to respond to an attack. And, when there are overlapping equities or responsibilities, determining which government agency should lead a response may become a problem (e.g., homeland security, defense department, justice department, election authority, or another agency). Malign actors understand the seams between government agencies and leverage them to launch their attacks.

Supply-side approaches to curbing the spread of disinformation include legislation, government fact-checkers, and information troops; however, it is still too early to know which ones are most effective.[20] For example, in 2017, Germany passed the Network Enforcement Act, compelling social media companies to remove hate speech and other illegal content. The downside of this type of law is that it can lead to censorship and curtail free speech.[21]

Another supply-side approach is the European Union's implementation of a voluntary, self-regulatory standard for technology companies, such as Google, Facebook, Mozilla, and Twitter. In 2018, they signed the European Commission's Code of Practice on Disinformation and committed to increasing the transparency of political ads, closing fake accounts, and addressing the malicious use of bots. However, the preliminary report of the Code of Practice was mixed. There continues to be a lack of trust between social media companies, governments,

---

[19] Alina Polyakova and Daniel Fried, "Democratic Defense Against Disinformation 2.0," *Atlantic Council*, June 2019, https://www.atlanticcouncil.org/wp-content/uploads/2019/06/Democratic_Defense_Against_Disinformation_2.0.pdf.

[20] Olga Robinson, Alistair Coleman, and Shayan Sardarizadeh, "A Report of Anti-Disinformation Initiatives" (Oxford: University of Oxford, August 2019), https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/08/A-Report-of-Anti-Disinformation-Initiatives.

[21] "Germany: Flawed Social Media Law," *Human Rights Watch*, February 14, 2018, https://www.hrw.org/news/2018/02/14/germany-flawed-social-media-law.

and civil society, primarily because technology companies give only limited access to their data.[22] In 2020, the European Commission implemented a comprehensive response to counter disinformation through the European Democracy Action Plan.[23] One of the initiatives is to overhaul the Code of Practice into a co-regulatory framework.

In contrast, Estonia, which has been the target of Russian disinformation since 2007, involves civil society in its approach. The government created a voluntary security force called the Estonia Defense League within the Ministry of Defense. The Estonia Defense League supports cyber defense but also monitors the Internet for disinformation and uses an anti-propaganda blog to counter distorted narratives. Estonia also involves an internet activist group called the Baltic Elves to respond to Russian trolls, report bots, provide counter-narratives.[24] In addition, since Estonia has a sizeable ethnic-Russian population, it operates a Russian-language television station to counter disinformation.

Taiwan is another country with a whole-of-society approach to curbing the supply-side of disinformation. Since 2018 when Taiwan appointed its first Digital Minister, the country instituted several civic-tech initiatives to build citizen and civil society trust. The Digital Minister not only developed a transparent government but also combined the efforts of government teams, technology companies, and private citizens to counter disinformation. Taiwan deployed several successful initiatives, including an Internet Fact-Checking Network, chatbots for social media fact-checking, and memes to challenge disinformation narratives.[25]

The greatest strength of Estonia and Taiwan's approach is the involvement of citizens in combatting disinformation. The battle against disinformation can only be won by starting with the citizens who are consuming and spreading disinformation. When the disinformation can be ignored by citizens, its spread will decrease. In the next section, this article explores methods to address the demand-side of disinformation.

---

[22] James Pammet, "EU Code of Practice on Disinformation: Briefing Note for the New European Commission" (Carnegie Endownment for International Peace, March 3, 2020), https://carnegieendowment.org/2020/03/03/eu-code-of-practice-on-disinformation-briefing-note-for-new-european-commission-pub-81187.

[23] European Commission, "European Democracy Action Plan," accessed February 2, 2021, https://ec.europa.eu/info/strategy/priorities-2019-2024/new-push-european-democracy/european-democracy-action-plan_en.

[24] Joseph Robbins, "Countering Russian Disinformation" (Center for Strategic & International Studies, September 23, 2020), https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation.

[25] Rorry Daniels, "Taiwan's Unlikely Path to Public Trust Provides Lessons for the US," *Brookings*, September 15, 2020, https://www.brookings.edu/blog/order-from-chaos/2020/09/15/taiwans-unlikely-path-to-public-trust-provides-lessons-for-the-us.

Demand-Side of Disinformation

One way to achieve demand-side reduction is through digital literacy education and disinformation awareness.[26] There is evidence that digital literacy can be an effective strategy to help counter disinformation.[27] Since there is no universal definition of digital literacy, in this article, digital literacy includes media, news, and information literacy and is defined as "the ability to use information and communication technologies to find, evaluate, create and communicate information, requiring both cognitive and technical skills."[28]

A common misconception is that older citizens are more susceptible to disinformation than younger citizens because of their lack of comfort with digital technology. There is evidence that senior citizens are more likely to share disinformation using social media.[29] However, younger citizens, who may be more comfortable with technology, are also susceptible to disinformation because they lack digital literacy skills. The Stanford History Education Group found that middle school, high school, and college students had difficulty evaluating the credibility of social media information. They incorrectly perceived information as trustworthy based on incorrect facts: a search engine result appearing at the top, a website using the .org domain or a Twitter account with many followers.[30] These gaps, therefore, demonstrate a societal need for digital literacy.

Policymakers and educators are rethinking the framework of digital literacy to ensure that critical thinking and civics are included in the curriculum. In the past, governments were more focused on developing digital skills needed for "digital transformation" initiatives that did not necessarily include critical thinking and civics. However, newer programs include citizen resiliency. For example, in 2019, Canada created a Digital Citizen Initiative using a multi-stakeholder approach. The initiative supports citizen-focused activities, such as the development of learning materials, investment in research programs, and promotion of

[26] Polyakova and Fried, "Democratic Defense Against Disinformation 2.0."

[27] Andrew M. Guess et al., "A Digital Media Literacy Intervention Increases Discernment Between Mainstream and False News in the United States and India," *Proceedings of the National Academy of Sciences* 117, no. 27 (2020): 15536-15545, www.pnas.org/content/pnas/117/27/15536.full.pdf.

[28] American Library Association (ALA), "Literacy for All: Adult Literacy through Libraries," (Chicago: ALA, 2019), http://www.ala.org/aboutala/sites/ala.org.aboutala/files/content/Literacy%20for%20All_Toolkit_Online.pdf.

[29] Andrew Guess, Jonathan Nagler, and Joshua Tucker, "Less Than You Think: Prevalence and Predictors of Fake News Dissemination on Facebook," *Science Advances* 5, no. 1 (January 2019), https://doi.org/10.1126/sciadv.aau4586.

[30] Stanford History Education Group, "Evaluating Information: The Cornerstone of Civic Online Reasoning."

media literacy (civic, news, and digital).[31] In contrast, there are also non-government-led programs. For example, two institutes located at the University of South Florida (Florida Center for Cybersecurity and the Florida Center for Instructional Technology) partnered with New America (a non-profit, non-partisan think tank) to develop cyber citizenship skills for primary and secondary students. They aim to create a Cyber Citizenship Working Group to collaborate with various civil society stakeholders and establish a Cyber Citizenship Portal to provide an educational toolkit for the public.[32]

It is still too soon to determine the effectiveness of the digital literacy education and awareness programs. Moreover, preparing citizens for digital literacy is only the first step to other knowledge and skillsets, such as algorithmic literacy and data literacy (as a result of AI).[33] For the challenges ahead, policymakers need to use strategic foresight to prepare citizens for the next-generation disinformation attacks better. In summary, the below policy recommendations are a starting point for developing citizen resiliency.

Policy Recommendation #1: Improve the Digital Literacy of All Citizens

Governments must develop a digital literacy program to educate all citizens about digital literacy by establishing a standard or framework. There are many frameworks to use as a foundation for creating a digital literacy program. They include the United Nations Educational, Scientific and Cultural Organization (UNESCO) Digital Literacy Global Framework, the European Union Digital Competence Framework for Citizens, and Dr. Yuhyun Park's Digital Intelligence (DQ) Framework.

Once the framework is developed, the government should create a digital literacy curriculum that meets the need of citizens at different stages of life (primary, secondary and tertiary levels). By developing curricula for different levels, educators and trainers can quickly adapt the material to their educational program. Methods to make the content accessible for adults include producing massive open online courses and creating online videos supporting lifelong, self-paced learning. The digital literacy skills will not only build citizen resilience to disinformation but will also prepare citizens for the impending digital transformation, which is the adoption of digital technology to transform society.

---

[31] UNESCO, "Digital Citizen Initiative," *UNESCO Diversity of Cultural Expressions*, accessed February 1, 2021, https://en.unesco.org/creativity/policy-monitoring-platform/digital-citizen-initiative.

[32] "Cyber Florida, Florida Center for Instructional Technology and New America Launch New Partnership to Improve 'Cyber Citizenship' Skills for K-12 Students," *New America* (International Security), December 16, 2020, www.newamerica.org/international-security/press-releases/cyber-florida-fcit-new-america-partnership-to-improve-cyber-citizenship.

[33] Ramesh Srinivasan, "This Is How Digital Literacy Can Transform Education," *World Economic Forum*, March 3, 2020, https://www.weforum.org/agenda/2020/03/why-is-digital-literacy-important.

Policy Recommendation #2: Include Digital Security in Annual Cybersecurity Awareness Campaigns

Citizen awareness begins with public awareness campaigns. Many governments already use annual cybersecurity awareness month or week to promote online safety and advocate for security practices. Since a core component of cybersecurity deals with understanding the online threats that jeopardize citizen safety, disinformation is an appropriate topic for raising awareness. For example, issues for attention could include a lesson on social bots or on evaluating the sources of online information. An awareness campaign provides yet another opportunity to sensitize citizens about disinformation.

Policy Recommendation #3: Empower Civil Society by Building Trust and Sharing Information on State and Political Actors Using Computation Propaganda

Empowering citizens by building trust and sharing information builds citizen resilience. Citizens do not understand the volume and intensity of the computational propaganda attacks against their country unless they are strengthened with information. They need to know who, what, where, when, and how disinformation attacks occur and what they can do to counter the disinformation. Since political computation propaganda attacks can be state-sponsored attacks, the government may not fully share the details of an attack due to classification reasons. To achieve trust, governments must find a way to be transparent about the attacks while balancing the need for security. Also, when sharing information, plain language should be used, omitting technical and government jargon.

Governments can also foster public-private partnerships to share information and collaborate to solve the technical computational propaganda and citizen resiliency challenges. In view of the fact that technology companies possess the data that government, civil society groups, and researchers need to develop countermeasures, the partnership provides an opportunity to create innovative solutions through crowdsourcing and trust through information sharing and open dialogue. Now, more than ever, government, technology companies, and civil society must work together to build collective trust and citizen resiliency.

Disclaimer

The views expressed are solely those of the author and do not represent official views of the PfP Consortium of Defense Academies and Security Studies Institutes, participating organizations, or the Consortium's editors.

About the Author

Inez Miyamoto is a cybersecurity professor at the Daniel K. Inouye Asia Pacific Center for Security Studies. E-mail: miyamotoi@dkiapcss.net

Acknowledgment

Connections: The Quarterly Journal, Vol. 20, 2021, is supported by the United States government.