AY 2023-2024

Advancing Cyber Defense and Information Integrity: A Comprehensive Approach to Securing U.S. National Security

ES-6700 Networking and Media Industry Study

Dr. James Van De Velde

Seminar 9 Group Paper

Word Count (Excluding Preface): 8.421

13 May 2024

The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University Fort McNair, Washington, D.C. 20319-5062

The views expressed in this paper are those of the author and do not reflect the official policy or position of the National Defense University, the DoD, or the U.S. Government.

Table of Contents

Seminar 9 Students and Faculty

Students

Lt Col Jessica Adkins, U.S. Air Force

COL Dilya Akhmetova, Kazakhstan Army

CDR William Corley, U.S. Navy

LTC Todd Harkrader, U.S. Army

Mr. Thomas Hilleary, Department of State

Ms. Shannon Holmes, Department of Air Force

Cdre Abu Sazzad Hossain, Bangladesh Navy

Lt Col Daniel Kim, U.S. Air Force

Mr. Daniel Krimowski, McKinsey & Company

CDR Kimberly Mazur, U.S. Navy

Mr. Wolfgang Petermann, Department of Army

LTC Frank J. Quintana, U.S. Army National Guard

Lt Col Daniel Richardson, U.S. Air Force

Ms. Molly Sanchez Crowe, Department of State

LTC Mallory Wampler, U.S. Army

Mr. Mark Zimmer, Department of State

Faculty

Dr. James Van de Velde, Ph.D., Industry Study Lead, Director of Research and Writing

Ms. Ana M. Gamonal de Navarro, Industry Study Deputy, DOE/NNSA Faculty Chair

Field Studies Hosts and In-Class Guest Speakers

Academia

1. Professor Jennifer Golbeck, University of Maryland, *Networking*
2. Professor Dan Silverman, Carnegie Melon University, *Misinformation in War*
3. Dr. Mike Wolmetz, Johns Hopkins Applied Research Lab, *Human and Machine Intelligence*
4. Tai Ming Cheung, Director of the University of California Institute on Global Conflict and Cooperation and Professor in the School of Global Policy and Strategy, *China's Defense Economy, and Industrial Base*
5. Dr. Richard Love, National War College, *The Gerasimov Doctrine in Cyberspace, The Russian Way of War and Cyber*

Industry

6. Omri Lavie, NSO Group Technologies, *Offensive Cyberspace Capabilities*
7. Mia Stender, Palantir Technologies, *Artificial Intelligence in Assisting National Security Operations*

Government/NDU President's Lecture Series (PLS)

8. Lt. Gen. Timothy Haugh, Deputy Commander, CYBERCOM, *Overview of CYBERCOM and National Security Implications*
9. Dr. Streilein and Lt. Col Wong, Task Force Lima, *AI and Language Learning Models*
10. Dr. Kimberly Sablan, Office of the Assistant Secretary of Defense for Critical Technologies, *DoD Progress on AI*
11. Amanda Bennett, CEO, U.S Agency for Global Media (USAGM); Alen Mlatisuma, Voices of America (VOA) Acting Director, Eurasia Division; Ayesha Tanzeem, VOA South, and Central Asia Division Director; Matthew Baise, VOA Director of Digital Strategy and Audience Development, *Challenges in Countering Mis/Disinformation Globally*
12. Karl Stoltz, Senior Advisor; COL Jason Wright, Senior Military Advisor; Brad Evans, Counterterrorism Division Director, Global Engagement Center (GEC), US Department of State Cyber Operation Center, *Understanding the Threat and Building Global Consensus*
13. Chris Miller, Chip Wars, *The Semiconductor Arms Race*
14. Dr. Rebecca Spyke Keiser, Chief of Research Security Strategy and Policy at the National Science Foundation (NSF), *Strengthening Cyber Resilience in U.S. Research and Development, Cyber Workforce Professionalization, and other related topics*

Washington DC Couplet

15. Ms. Erin Joe, OCISO Google Cloud, Cybersecurity
16. John Arquilla, Professor, Naval Postgraduate School (NPS), *The Security of Information Flows: Securing the Undersea Cable Network*
17. Dr. Lindsay Hundley, Influence Operations Policy Lead, Ms. Ingrid Dickenson, Security Policy Manager, Global Threat Disruptions, Meta, *Countering Covert Influence Operations*

18. Mr. Dylan Presman, Director for Budget and Assessment- Office of the National Cyber Director Executive Office of the President, *Strategic ecosystem 20 years ago looked very different and evolved organically; cybersecurity is largely bipartisan.*
19. Mr. Paul Mazzucco, J5 US Cyber Command, Liaison to the US Cyberspace Interagency, *Status quo is not winning; escalation tit-for-tat; must leverage allies and partners DoD-wide; 'best mix vs best athlete'*
20. Matt Altomare, Deputy Chief of Operations, Threat Hunting, Cybersecurity Division, U.S. Department of Homeland Security, Cybersecurity, and Infrastructure Security Agency (CISA)
21. Scott Jasper, NPS, *Malign Cyberspace Activities by the Russian Government in Ukraine*
22. Dr. Diane Janosek, former Senior Executive Service, National Security Agency, *The Regulatory World of Cyberspace – What is Government's Role and Erosion of Trust*
23. Michael Wolmetz and Shaill Vasavada, Johns Hopkins Applied Physics Lab, *LIVELab Overview; Intelligent Systems Center; The Human and Machine Intelligence Program*

New York City Couplet

24. Mr. Amit Kachhia-Patel, Special Agent in Charge, FBI Cyber Division, NYC Cyber, *Malign Activities, and the Role of the FBI*
25. UN Cyber Stability Conference: Panel on *How Artificial Intelligence is Changing the Threat Landscape,* Charles Ovink, Political Affairs Officer, UNODA; Lauren Stockton, Consulting Senior Analyst, Accenture; Kaleem Usmani, Head of Computer Emergency Response Team (CERT), Republic of Mauritius; Shimona Mohan, Associate Researcher Gender, Security & Technology, UNIDIR Impact Technology is Having in Shaping the ICT Threat Landscape
26. Mohamed Telab, CISA, National Urban Security Technology Laboratory and the Role of CISA
27. Gabelli Center, Fordham University, Gabelli School of Business, Amy Jones, EY.ai AI and Large Language Models; Dr. Steve Kim, Con Edison, Cyber Kinetics
28. NASDAQ, Lee Anne Milhiser, VP, Head of Global Enterprise Risk Management; Discussion of how NASDAQ protects the financial sectors from cyber intrusions.

California (Silicon Valley)

29. Google, Courtney Chatman, *Google Core Services and User and Content Safety*; Toni Gidwani, *Global Threat Landscape*; Stephan Somogyi, *Protection of Data Online*
30. Lawerance Livermore Laboratories (Classified), Reg Beer, *Lab Overview*; Michael Schneider, *Decision Superiority*; Brian Wihl, *Autonomous Sensors and Systems*; John Breneman, *Cyber* Defense and Software Assurance; David Lettis, JCATS
31. Apple, Jon McCormick, Perspectives on Malign Information Operations
32. Stanford University, Jacquelyn Schneider, Hoover Institution, Cyber War Game
33. IBM, Spike Narayan, IBM Research Overview; John Arthur, North Pole; Sandeep Gopisetty, Watson; Kevin Roche, Quantum
34. NVIDIA, Kevin Berce, Govt Affairs Team, and Engineering staff, Application of AI in the Commercial Market Beyond Gaming
35. Applied Intuition, John Mark Wilson, Defense Govt Affairs Team, Scalable, Reliable Diffusion Modeling, and Catastrophic Forgetting; Joseph Cymerman, Govt Affairs Team, AI applications in DoD Acquisitions and Supply Chains

36. HP, Dr. Tommy Gardner, Chief Technology Officer, *Overview of AI and Future Applications to Government and Commercial Sector*, Chandrakant Patel, HP Senior Fellow, and Chief Engineer; *Future of Cyber and Getting Back to Basics*

Latvia, Estonia, and Finland
(All officials highlighted that cyber and disinformation attacks are predominately from Russia. All are supportive of Ukraine because if Russia is victorious, they could be the next targets.)

Latvia

37. Ambassador Christopher T. Robinson, *Latvia overview, Cyber and Disinformation Threats*
38. Dr. Ieva Berzina, Latvia Ministry of Defense, *National Defense Academy Overview*
39. MoD Roundtable – Mr. Rolands Henins, Ms. Dace Kundrate, Mr. Edgars Kiukucans, *Hybrid Warfare Geography Matters; NATO is Latvia's Calvary; Ukraine Protected by Whole-of-Society*
40. Mario Nicolini and Jon Sunderland, NATO StratCom Center of Excellence (accredited by NATO, not funded by NATO (Baltic-led CoE), *PRC and Russia have no limits when it comes to cyber employment; Kremlin influence in cyber domain becoming an existential threat to neighboring countries; Disinformation in Democracy*

Estonia

41. U.S. Ambassador George Kent and staff, *Update on the Current State of Estonia: Cyber, Disinformation, and Hybrid Warfare*
42. Angelica Tikk and USN CDR Jack Shis, *Russian threats on Estonia and Tallinn Manual*
43. Col Uku Arnold, MoD, Deputy Chief of Estonian Defense Forces Strategic Communication, *Countering Russian Activities*
44. Harry Puusepp, Estonian Secret Service, *Information Operations and Countering Hostile Activities*
45. Martin Reisner, Defence Willingness Department, *Digital and Cyber Literacy*, *Whole of Society, National Defence Approach*
46. Cyber Panel Marko Kaseleht, CEO, SensusQ, *Building Military Intelligence Software*; Mihkel Tikk, CyberCom, *National Cyber Defense*; and Gert Auvaart, Deputy Director, National Information System Authority, *Tracking of Threats and How to Counter*

Finland

47. Ambassador Douglas Hickey and Maj Mike "MO" Morris, Finnish Media and Digital Literacy, Role as a new NATO Member, and Finnish Defense Policies; Comprehensive Security, Conscription, Hybrid Threats
48. Pekka Toveri, Member of Parliament, Russian Hybrid Warfare and Finland's Comprehensive National Defense
49. Lt Col Tuomas Liukko, MoD J5, *Defense Cooperation with Partners and National Defense Planning, the Difference between NATO Partnership and Membership, Weaponized Migration, Huge Ecosystems, and a Holistic Outlook on Security*
50. National Defence University, Col Huhtnen, *Overview of NDU*; Maj Maria Keinonen, *Cyber and Information Warfare and Deterrence*; Lt Col Marko Palokangas, *Fog of War and*

Comprehensive Strategy to Counter; Dr. Miina Kaurkoski, *"Defence Will" of the Population and Strategic Communications*

51. Tero Koskinen, Head of Preparedness, Senior Adviser in Media Resilience, Medipooli, *Countering Malign Influence: Public/Private Collaboration and Leveraging Social Media Influencers to Counter Hybrid Threats and Disinformation*
52. Mart Noorma, NATO Hybrid Center of Excellence, *Hybrid Warfare in the 21st Century, Cyber is Military Power*
53. Tapio Pyysalo, Hybrid Center of Excellence – Hybrid Wars, *Coordinated and Synchronized Actions Targeting Systemic Vulnerabilities; Exploit Attribution; Cyber is Equal to Conventional Military Power*
54. Ms. Johanna Räty, Specialist, International Affairs, National Emergency Supply Agency, *How Finland Bridges between Public/Private Sectors to Plan and Secure the Supply Chain*
55. Antti Nyqvist, Preparedness Manager, Digipool, *Digital Security and Supporting and Promoting Preparedness through Media and Strategic Communications*
56. Mr. Jussi Toivanen, Head of Communications, TRAFICOM, *Cyber Security Across All Aspects of the Finnish Government*

Executive Summary

Current cyber and information operations defenses will likely remain inadequate to counter the growing trend of malign cyberspace activities despite significant legislative, strategy, and policy efforts. The United States faces considerable challenges in safeguarding its critical infrastructure and maintaining the integrity of its democratic processes against sophisticated cyber threats and pervasive disinformation campaigns. These threats, foreign and domestic, aim to disrupt government functions, degrade the stability of American democracy, and sow discord. The People's Republic of China (PRC), Russia, North Korea, and Iran intensify these challenges through cyber-attacks, economic espionage, criminal activities, and influence operations that seek to displace the United States as a global leader.

Strategic Environment and Threat Landscape. The appeal of cyberspace for malign actors lies in its inherent characteristics—low cost, asymmetry, deniability, and scalability. Cyber tools have become favored weapons in modern conflict due to their ability to easily manipulate digital environments—from social media platforms to critical national infrastructure, presenting opportunities for adversaries to exploit software vulnerabilities, hardware flaws, and human factors such as social engineering.

Vulnerabilities and Defensive Challenges. Cyber has no borders, and nearly everything connected to the internet is vulnerable. Adversaries only need a single-entry point to compromise nascent to national security-critical systems, exploiting all attack vectors from software vulnerabilities to humans. The pervasive influence of algorithms and the rise of artificial intelligence further complicates the cyber battlefield, enhancing the capabilities of cyber tools, increasing risk, and significantly challenging defensive efforts.

Government and Societal Response. A whole-of-government and society approach is imperative to address these challenges. This includes enhancing cybersecurity defenses, promoting digital and media literacy, regulating social media platforms, and leveraging civil society initiatives to foster public resilience. The approach must involve improved collaboration and cooperation with industry, academia, and private citizens to implement a strategy drawing on successful international models of comprehensive societal engagement, cyber and media literacy, and modernization. U.S. strategy must expand offensive cyber capability to compel adversaries to stop attacking U.S. sovereignty when deterrence fails and defense is insufficient.

Recommendations. America must implement a comprehensive “whole of society” approach with four primary lines of effort. 1) Expanding education and messaging to combat cyber and disinformation threats across the public and private sectors. 2) Strengthening partnerships with allies, private industry, and academia for sharing cyber threat intelligence and coordinating defense strategies. 3) Enhancing cybersecurity regulations for critical infrastructure and digital platforms to mitigate misinformation and cyber espionage risks. 4) Targeting actions to modernize critical infrastructure and cyber defenses coupled with cyber compellence to deter malign activities.

Conclusion. Strengthening U.S. cyber and information operation defenses against growing threats requires a whole-of-society approach – engaging allies, the private sector, and the public – to protect national security, safeguard U.S democracy, and secure America’s role in the global order.

Introduction

Current cyber and information operations defenses will likely remain inadequate to address the growing increasingly sophisticated trend of malign cyberspace operations. Despite various legislative, policy, and strategic initiatives in a rapidly evolving digital landscape, the United States faces significant gaps and challenges in safeguarding critical infrastructure and maintaining the integrity of its democratic processes against sophisticated cyber threats and pervasive disinformation campaigns. These threats, orchestrated by foreign and domestic malign actors, aim to sow discord, disrupt government functions, and degrade the stability and security of American democracy. Internationally, the People's Republic of China (PRC), Russia, North Korea, and Iran intensify these challenges, with the PRC actively seeking to displace the U.S.-led global order through cyber-attacks, economic espionage, and influence operations. [1] [2] Domestically, deepening social polarization, exacerbated by disinformation spread through social media, poses additional vulnerabilities, particularly as the 2024 presidential election approaches.[3]

Given these threats, a comprehensive, whole-of-society approach is needed to bolster cybersecurity defenses, enhance digital and media literacy, sensibly regulate social media platforms to prevent manipulation, and leverage civil society initiatives to strengthen resilience. The United States must foster improved collaboration with industry, academia, and private citizens to devise a strategy that integrates all sectors of government and society. Drawing from successful models in Finland, Lithuania, and the European Union, this strategy should focus on extensive digital literacy, sensible social media regulations to protect civil liberties while combating disinformation, a proactive cyber posture, and modernizing critical infrastructure using secure by design principles.

A comprehensive, whole of society approach is needed to bolster cybersecurity defenses, enhance digital and media literacy, sensibly regulate social media platforms to prevent manipulation, and leverage civil society initiatives to strengthen cyber resilience.

The framework will focus on four key areas: awareness and education, engagement and collaboration, regulation and governance, and targeted action and implementation. This comprehensive approach aims to mitigate threats and build long-term resilience against evolving cyber and information security challenges.

[1] Ward, Jonathan D.T., "China's Vision of Victory," *The Ambassador's Brief*, 29 August 2019.

[2] Office of the Director of National Intelligence. "NIC-Declassified-ICA-Foreign Threats to the 2022 US Elections." December 2023. PDF file. https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf.

[3] Reuters, "Microsoft finds Russian influence operations targeting U.S. election have begun," April 17, 2024, https://www.reuters.com/world/us/microsoft-finds-russian-influence-operations-targeting-us-election-have-slowly-2024-04-17/

Strategic Environment and Threat Landscape

Operating within the cyber domain presents advantages such as low cost, asymmetry, deniability, standoff capability, and scalability, making cyber weapons highly attractive for state and non-state actors. This appeal drives its widespread adoption as a favored instrument in modern warfare. The rise of software developers being among the most influential figures globally is a testament to the power of algorithms, which companies exploit to shape behavior and drive profit. This alters the foundational underpinnings of society and creates opportunities for malicious actors to manipulate and inflict damage. The ease with which individuals can influence and disrupt from any location underscores the profound impact of cyber on global stability.

In this rapidly evolving domain, virtually every element can be manipulated, transforming cyberspace into a theater for a range of operations, from insider threats to coordinated attacks like denial of service. The capabilities for disruption are extensive, equating the strategic impact of cyber operations with conventional military power. The low cost of doing business entices cybercriminals to profit from nefarious activities. The most significant reason cyber is changing the character of war is because it touches nearly every aspect of everyday life – making the ease of attack vectors almost limitless.

> *The most significant reason cyber is changing the character of war is because it touches nearly every aspect of everyday life – making the ease of attack vectors almost limitless.*

Defensive efforts in cyberspace are fraught with challenges, as adversaries require only a single point of entry to compromise a system. This could involve exploiting software vulnerabilities, hardware flaws, or human factors like social engineering. The traditional perception of users as passive victims oversimplifies the dynamics of cybersecurity, ignoring the critical role individuals play in systems' vulnerability and resilience.

Governments and societies have only begun understanding cyberspace as a contested domain. Author Brian Mazanec notes, "…it is evidence of how early we are in the cyber era…as advanced cyber warfare is only now becoming possible and a robust target set emerging as societies become more immersed and dependent on cyberspace."[4] Opposite targets, users can also be insider threats,

[4] Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons* (Univ of Nebraska Pr, 2015), 163, https://aufric.idm.oclc.org/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=kdh&AN=BK0016961936&site=ehost-live&scope=site&custid=airuniv.

such as U.S. Air Force personnel's recent intelligence leaks on Discord servers.[5] Additionally, users can wittingly or unwittingly amplify disinformation and misinformation through social media platforms.[6] Given the increasing role of technology in our society, the challenge of defending against individual user threats will continue to grow.

Another consideration in the threat landscape and strategic environment is Artificial Intelligence (AI). AI transforms the cyber domain, enhancing cyber tools' processing capabilities and operational effectiveness. The intersection of AI with cyber operations is reshaping the battlefield, introducing autonomous systems that complicate attribution and response strategies. As noted in the Presidential Executive Order published in October 2023, AI presents a dual-edged potential of significant promise and peril.[7] Its role in disseminating misinformation and automating attacks elevates the stakes.

Lastly, cyber capabilities are reshaping the international geopolitical landscape, with significant powers such as Russia and China using these tools to challenge the established global order. These nations employ cyber strategies not only for intellectual property theft but also to manipulate international politics and undermine democratic norms, contrasting starkly with Western countries advocating for a regulated, secure cyberspace governed by international law. This divergence emphasizes the critical need for cyber defenses and greater international collaboration to tackle the complex threats from sophisticated cyber activities. Unlike autocracies, the United States and its allies promote a free, open, peaceful, and secure cyberspace, supporting international law and voluntary norms of responsible behavior.[8] This disparity in approaches highlights the strategic challenges in cyberspace - where cyber, as an instrument of power, could allow dominant actors to consolidate their influence further.[9]

[5] Courtney Mabeus-Brown, “Another Airman Probed by FBI for Allegedly Leaking Intel on Discord,” Air Force Times, March 26, 2024, https://www.airforcetimes.com/news/your-air-force/2024/03/26/another-airman-probed-by-fbi-for-allegedly-leaking-intel-on-discord/.

[6] Steven Lee Myers, “How Social Media Amplifies Misinformation More Than Information,” *The New York Times*, October 14, 2022, sec. Technology, https://www.nytimes.com/2022/10/13/technology/misinformation-integrity-institute-report.html.

[7] The White House. “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,” October 30, 2023. https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[8] NATO OTAN. “Cyber Deterrence.” September 14, 2023. https://www.nato.int/cps/en/natohq/topics_78170.htm

[9] Yuval Noah Harari, “Why Technology Favors Tyranny,” The Atlantic, October 2018 https://www.theatlantic.com/magazine/archive/2018/10/yuval-noah-harari-technology-tyranny/568330/

Vulnerabilities of Social Media

In a recent speech at the Summit for Democracy, U.S. Secretary of State Antony Blinken warned, "Our competitors and adversaries are using disinformation to exploit fissures within our democracies by further sowing suspicion, cynicism, and instability."[10] Social media platforms facilitate this exploitation. These platforms were once heralded as revolutionary tools for global connection, enabling governments, organizations, and individuals to communicate on a massive scale. Today, social media platforms are fertile ground for malign actors to disseminate information operations and propagate extremist content.

> *"Our competitors and adversaries are using disinformation to exploit fissures within our democracies by further sowing suspicion, cynicism, and instability."*
>
> *--- Secretary of State Antony Blinken.*

In the U.S alone, approximately 246 million people—72.5% of the population—are active Facebook, Twitter, and TikTok users.[11] These platforms are arenas where malign actors are attempting to undermine U.S. global influence and challenge the liberal international order abroad while sowing discontent with democracy in the United States. The powerful algorithms of these platforms foster addictive behaviors; they create an attention economy that thrives on continuous user engagement while tailoring content that aligns with already-held beliefs to encourage further engagement, which malign actors exploit to exacerbate societal divisions and spread misinformation.[12]

This cycle leads to the proliferation of echo chambers and homophily, where users are more likely to connect with others who share similar traits, such as race, gender, ethnicity, and ideology.[13] The expected privacy and anonymity within social media environments can be exploited to create artificial homophily, further deepening existing divisions and making political discourse more contentious. The manipulation of social media by malign actors not only shapes opinions and spreads misinformation and disinformation, but also creates a highly polarized partisan

[10] "Building a More Resilient Information Environment," United States Department of State, March 21, 2024, https://www.state.gov/building-a-more-resilient-information-environment/.

[11] Brian Dean, "Social Network Usage & Growth Statistics: How Many People Use Social Media in 2024?" Backlinko, February 21, 2024, https://backlinko.com/social-media-users.

[12] Supernova, "How the Invention of Infinite Scrolling Turned Millions to Addiction," Medium, November 25, 2020, https://bootcamp.uxdesign.cc/how-the-invention-of-infinite-scrolling-turned-millions-to-addiction-3096602ef9af.

[13] Miller McPherson, Lynn Smith-Lovin, and James M. Cook, "Birds of a Feather: Homophily in Social Networks," Annual Review of Sociology 27, no. Volume 27, 2001 (August 1, 2001): 415–44, https://doi.org/10.1146/annurev.soc.27.1.415.

environment where political compromise is complicated and undervalued.[14] Ultimately, this contributes to the erosion of liberal institutions, challenging the integrity of democratic societies.

As the reliance on social media for news and commentary has grown, trust in information accuracy has declined, correlating with diminishing trust in government and media institutions. The likely cause of declining institutional trust is a corresponding dip in confidence in information received from social media.[15] As faith in informational accuracy declines, research shows that Americans' willingness to pay for news is also declining.[16] This situation creates a vicious cycle: as Americans become less willing to pay for news, news outlets become more dependent on digital advertising, incentivizing sensationalized and politically biased reporting to capture users' attention on social media platforms. This model, centered on monetizing user attention, leaves social media platforms particularly vulnerable to exploitation by both state and non-state actors. Actors use echo chambers and homophily generated by social media algorithms to launch information operations and propagate extremist content, aiming to sow discord and weaken American social cohesion and faith in democracy.

A notable example of such exploitation is the extensive information warfare campaign orchestrated by Russia's Internet Research Agency (I.R.A.), which aimed to generate social and political division within the U.S, eroding trust in democratic processes.[17] This campaign impacted the 2016 American Presidential election; the I.R.A. leveraged social media to disseminate disinformation to influence voters, reaching 126 million U.S. Facebook users and 288 million Twitter users.[18] Russia's disinformation operations continued during its 2022 invasion of Ukraine, alleging U.S. involvement in biological weapons labs, a narrative amplified by China to cast further doubt on American values and intentions. The ability of actors to use social media to exploit societal fissures underscores the significant threats posed by disinformation campaigns.[19]

Social media platforms serve as hubs for extremist activities, with 90 percent of internet-based

[14] "How Social Media Platforms Enable Politicians to Undermine Democracy - Vox," accessed April 24, 2024, https://www.vox.com/policy-and-politics/2019/1/22/18177076/social-media-facebook-far-right-authoritarian-populism.

[15] Elisa Shearer and Amy Mitchell, "News Use Across Social Media Platforms in 2020," Pew Research Center, January 12, 2021, https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/.

[16] Gallup and Knight Foundation, "American Views 2022: Part 2 Trust, Media and Democracy" (Washington, D.C.: Knight Foundation, February 15, 2023), 45–49, https://knightfoundation.org/wp-content/uploads/2023/02/American-Views-2022-Pt-2-Trust-Media-and-Democracy.pdf.

[17] U.S. Senate, "Report of the Select Committee on Intelligence, United States Senate, on Russian Active Measures, Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia's Use of Social Media with Additional Views," (Washington, DC: U.S. Government Publishing Office, 2019), 8.

[18] Christina Nemr and William Gangware, "Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age," Park Advisors, March 2019, 15.

[19] David Rising, "China Amplifies Unsupported Russian Claim of Ukraine Biolabs," A.P. News. Associated Press, March 11, 2022.

terrorist actions occurring on these platforms.[20] According to the Government Accountability Office, social media and gaming platforms offer violent extremist groups expansive and readily accessible networks that are frequently under-monitored. This environment allows groups to inject extremist ideologies into the mainstream, recruit new members, conduct training, and incite violence.[21] The National Counterterrorism Innovation, Technology, and Education Center highlighted violent extremist groups are expanding influence internationally, often using social media to interact across borders with like-minded extremists. These groups collaborate extensively, sharing experiences and tactics while accessing common resources to strengthen global operations. Although concrete evidence of Russian support is lacking, observed interactions between U.S. extremists and the Russian Imperial Movement suggest a probable connection to Russian state backing.[22]

As Americans become less digitally literate and technologies like Generative Artificial Intelligence (GenAI) make information operations more sophisticated, public vulnerability grows. A recent example was during the 2024 primaries when a deepfake robocall falsely portrayed President Biden, discouraging New Hampshire residents from voting.[23]

The spread of violent extremist ideology through social media, along with proliferating information operation campaigns, poses a threat to democratic institutions and American sovereignty. Combined with eroding public trust in media and government, these technologically advanced campaigns highlight the need to take action to protect U.S. influence, foster unity, and uphold the liberal global order while enhancing social cohesion and trust in democracy at home.

Factor Conditions

Factor Conditions - Cyber

Cyberspace is increasingly the domain of choice for actors and nation-states, especially since most actions are perceived to be below the threshold of armed conflict. Operating within the cyber domain and employing cyber weapons has advantages, including low cost, asymmetry, deniability, standoff capability, and ability to scale. Premeditated, politically or socially motivated attacks

[20] Suzanne Waldman and Simona Verga, "Countering Violent Extremism on Social Media," Defence Research and Development Canada – Centre for Security Science, DRDC-RDDC-2016-R229, November 2016, https://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf.

[21] Triana McNeil, "Countering Violent Extremism: FBI and DHS Need Strategies and Goals for Sharing Threat Information with Social Media and Gaming Companies," U.S. Government Accountability Office, GAO-24-106262, January 31, 2024, publicly released February 28, 2024, accessed April 22, 2024, https://www.gao.gov/assets/d24106262HIGH.pdf.

[22] Martha Crenshaw and Kaitlyn Robinson, "Transnational Ties Between Selected U.S. and Foreign Violent Extremist Actors: Evidence from the Mapping Militants Project" (National Counterterrorism Innovation, Technology, and Education Center, June 30, 2023), https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1043&context=ncitereportsresearch.

[23] Wolf, Zachary. “Analysis: The Deepfake Era of US Politics Is upon Us.” CNN, January 24, 2024. https://www.cnn.com/2024/01/24/politics/deepfake-politician-biden-what-matters/index.html.

against a computer-dependent society can affect nations at any level.[24] Intelligence gathering, espionage, preparation of the environment, and attacks are common in cyberspace because of four interrelated factor conditions:

- Malicious actors have advantages in cyberspace.
- There is an insufficient number of trained cyber professionals.
- U.S. policies are insufficient to deter nation-states.
- U.S. political will to punish attributed attackers is limited.

Malicious Actors Have Advantages in Cyberspace

In his January 2024 testimony before the Congressional House Select Committee on Great Power Competition between the U.S. and the PRC, FBI Director Christopher Wray highlighted the ongoing sophisticated and covert cyber threats from the PRC. Wray detailed their systematic targeting of critical infrastructure in the U.S. and the significant yet underreported threat they pose.[25] While this specific threat is attributed to the PRC, it is consistent with the behavior of other nation-state malign actors with varying levels of capability.

Video Clip 1: FBI Director Wray testifies to Congressional Select Committee on CCP, January 31, 2024

Cyber terrain grows daily - giving malicious actors more potential attack vectors while complicating defenders' jobs. Consider U.S. critical infrastructure: a prime target for nation-state actors and one that is expanding to support increasing demands from the U.S. population. Today, approximately 80-85% of U.S. critical infrastructure is privately owned and widely distributed, complicating the enforcement of unified cybersecurity standards and leading to inconsistent protective measures across sectors.[26] Many legacy operational technology (OT) systems, some over 30 years old, were initially designed for reliability, not cybersecurity, and have unresolved vulnerabilities.[27] As OT and information technology (IT) systems become more integrated, merging traditionally separate operational

[24] Daniel Brecht. "Cyber Warfare and Cyber Weapons, a Real and Growing Threat," January 15, 2015. https://www.infosecinstitute.com/resources/general-security/cyber-warfare-cyber-weapons-real-growing-threat/

[25] Wray, Christopher. "Director Wray's Opening Statement to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party." FBI News. April 4, 2024. https://www.fbi.gov/news/speeches/director-wrays-opening-statement-to-the-house-select-committee-on-the-chinese-communist-party.

[26] King, Angus, and Tom Fanning. "To Combat Cyberattacks, the US Government and Businesses Must Work More Closely." CNN Business, July 19, 2021. https://www.cnn.com/2021/07/19/perspectives/cyberattacks-security-us-government-businesses/index.html.

[27] Allissa, Ayman, Begonha, Duarte, et al., "How to Enhance the Cybersecurity of Operational Technology Environments," *McKinsey & Company,* March 29, 2024, accessed on April 21, 2023, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/how-to-enhance-the-cybersecurity-of-operational-technology-environments.

domains increases susceptibility to cyberattacks.[28] Critical infrastructure is a target-rich environment. The detection of malicious activity in cyberspace is complex. The PRC increasingly uses living off the land (LotL) tactics, exploiting system administrative tools like internal utilities, scripting languages, and trusted applications to hide in plain sight until ready to strike.[29] These covert tactics enable prepositioning, espionage, and sabotage, potentially leading to severe disruptions or catastrophic damage.

Insufficient Supply of Trained Cyber Professionals

As the attack surface grows, more users become targets, and detection becomes more complex; more trained cyber professionals are needed. The leading association for cybersecurity professionals, the International Information System Security Certification Consortium (ISC2), publishes an annual workforce study. Its 2023 report noted the United States had a deficit of 521,827 cybersecurity professionals, a 19.7% increase from the previous year.[30] According to the report, most respondents indicate organizations are under-resourced and require additional capabilities to respond to cyber threats effectively.[31]

U.S. Policies are Insufficient to Deter Nation States

The decades-long prioritization of growth over security left the nation with a vulnerable technological infrastructure. U.S. companies historically prioritized technological development and innovation due to the competitive advantages and potential for significant financial returns these investments can offer. This focus often overshadows cybersecurity considerations, which, although crucial, are sometimes perceived as cost centers rather than revenue generators. Investments in cybersecurity are necessary for risk mitigation but do not generate direct revenue, making them less attractive from an investment perspective.[32] Some companies underestimate the potential impact of cyber threats, especially if they have yet to experience significant breaches. This underestimation led to a lower prioritization of cybersecurity measures.[33] However, the global environment has changed, requiring companies to approach cybersecurity proactively.

[28] Boles, Christina, "How to Address OT And ICS Cyberattack Vulnerabilities." *Forbes*. February 8, 2024, accessed on April 21, 2024, https://www.forbes.com/sites/forbestechcouncil/2024/02/08/how-to-address-ot-and-ics-cyberattack-vulnerabilities/?sh=7081c77c3622[1].

[29] Day, Arik, "Playbook of The Week - Fending Off Living Off the Land Attacks." *Palo Alto Networks Blog*. January 29, 2024, accessed April 22, 2024, https://www.paloaltonetworks.com/blog/security-operations/playbook-of-the-week-fending-off-living-off-the-land-attacks/.

[30] ISC2. 2023. ISC2 Cybersecurity Workforce Study, pg. 12. Accessed April 23, 2024. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.

[31] ISC2. 2023. ISC2 Cybersecurity Workforce Study, pg. 12. Accessed April 23, 2024. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e.

[32] "Prioritizing Cyber Security for Business Owners," The Hartford, accessed May 6, 2024, https://www.thehartford.com/insights/cyber/business-cyber-security-prioritization-tips.

[33] Keman Huang et al., "The Devastating Business Impacts of a Cyber Breach," *Harvard Business Review*, May 4, 2023, https://hbr.org/2023/05/the-devastating-business-impacts-of-a-cyber-breach.

Effective and timely U.S. government attribution of nation-state cyber activities, typically more subtle and sophisticated, also inhibits deterrence. Congressional Research Service reports conclude achieving high confidence through primary sources "remains difficult despite having a process to determine attribution."[34] Companies like Microsoft and Alphabet can lead to faster attribution without sacrificing accuracy.

Underdeveloped legal frameworks limit U.S. cyber deterrence policy effectiveness, often because attribution presents legal and political complexities. Terrance Check, Senior Counsel at CISA, explains that LotL tactics, where malicious actors are positioned to inflict harm but have not yet caused economic, physical, or informational damage, challenge traditional interpretations of international law regarding state sovereignty and cyberattacks.[35] Scott Jasper, a cyber policy expert, underscores the need for aggressive countermeasures extending beyond national borders when a malicious actor is prepositioned on U.S. sovereign cyberspace terrain.[36] He advocates for a justified and proportional approach under international law to punish malicious actors to bolster future deterrence.[37]

U.S. Political Will to Punish Attributed Attackers is Limited

Cyber warfare is prevalent in competition and conflict; however, exaggerated escalation concerns limit the U.S. political will to punish attributed actors through cyberattacks. The U.S. government is reticent to engage in retaliatory cyberattacks, especially against active cyber adversaries like Russia and China. In contrast, the U.S. government has taken substantial steps to compete with both countries in other areas. While the USG has been willing to take action against countries and individuals who violate laws, rules, and norms in other domains, such as violations of non-proliferation agreements,[38] breaches of international law, such as Russia's invasion of and war against Ukraine,[39] or individuals involved in terrorism or narcotrafficking,[40] in cyberspace, the U.S. government has been reluctant to punish malicious actors. Attribution is often convoluted, and there is often fear of retaliation. Using cyber tools that can then be used against the U.S. could be prolific, given the magnitude of people connected to the internet. Additionally, cyber tools often

[34] Jaikaran, Chris. "Cybersecurity: Selected Cyber Attacks." Congressional Research Reports, R46974 (congress.gov), accessed May 13, 2024.

[35] Check, Terence. 2023. "The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure." National Security Law Brief 13 (1): pg. 8. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,url,uid&db=tsh&AN=172265866&site=ehost-live&scope=site.

[36] Jasper, Scott. Strategic Cyber Deterrence: The Active Cyber Defense Option. Lanham: Rowman & Littlefield Publishers, 2017, CH. 7, pp. 165-167.

[37] Jasper, Scott. Strategic Cyber Deterrence: The Active Cyber Defense Option. Lanham: Rowman & Littlefield Publishers, 2017, CH. 7, pp. 165-167.

[38] "Nonproliferation Sanctions," *United States Department of State* (blog), accessed May 8, 2024, https://www.state.gov/key-topics-bureau-of-international-security-and-nonproliferation/nonproliferation-sanctions/.

[39] "Imposing New Measures on Russia for Its Full-Scale War and Use of Chemical Weapons Against Ukraine," *United States Department of State* (blog), accessed May 8, 2024, https://www.state.gov/imposing-new-measures-on-russia-for-its-full-scale-war-and-use-of-chemical-weapons-against-ukraine-2/.

[40] "Office of Foreign Assets Control," accessed May 8, 2024, https://ofac.treasury.gov/faqs/topic/1501.

do not differentiate between combatants and non-combatants. However, data shows that cyber escalation risks and fears are exaggerated, and the United States is overly self-restrained. Furthermore, offensive cyber operations are poor tools of escalation due to four factors: "1) retaliatory offensive cyber operations may not exist at the time they are needed; 2) their effects are uncertain and often limited; 3) they generate necessary tradeoffs that may make decisionmakers hesitant to use them; and 4) cross-domain escalation is unlikely given the inherent limitations of offensive cyber operations."[41]

In recent years, the number of cyberattacks has dramatically increased and with broader effects, but responses have been minimal. Malicious cyber actors (MCAs) attacked the Colonial Pipeline in May 2021 and caused significant disruptions along the U.S. East Coast, leading to panic buying. The attack was attributed to a Russian cybercriminal hacking group; however, the U.S. response focused on defense and regulatory actions.[42] While those actions are necessary, they do not impose costs or compel MCAs to stop. The lack of punishment invites more attacks. Meanwhile, Russia's cyberattacks in Ukraine have not led to cyber escalation outside the conflict zone. The United States is unnecessarily restraining itself in cyberspace.

Factor Conditions - Social Media

The backbone of social media consists of the algorithms that powerful companies like Google, Facebook, Twitter, Instagram, and YouTube develop to captivate audiences (targets). These algorithms learn from users' behavior to tailor more content that appeals to the user. This translates directly into revenue through advertising, subscriptions, in-app purchases, and data mining. In other words, "time—spent online—is money." Firms like Alphabet and Meta rank among the top ten largest companies in the world by market capitalization.[43] Their market positions contrast traditional media's plummeting circulation and revenues since the early 2000s, including digital subscriptions and the declining share of U.S. adults who follow traditional media.[44]

A recent MIT study of verified false and true news spread on Twitter concluded that false news unequivocally reaches more people than true news. The top one percent of false news diffused between 1000 to 100,000 people, whereas truthful news rarely diffused to more than 1,000 people. Moreover, researchers concluded false news spread six times faster than truth.[45] This amplifies

[41] Erica D. Borghard and Shawn W. Lonergan, "Cyber Operations as Imperfect Tools of Escalation," *Strategic Studies Quarterly* 13, no. 3 (2019): 122.

[42] "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA," May 7, 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

[43] "Companies Ranked by Market Cap - CompaniesMarketCap.com," accessed April 23, 2024, https://companiesmarketcap.com/.

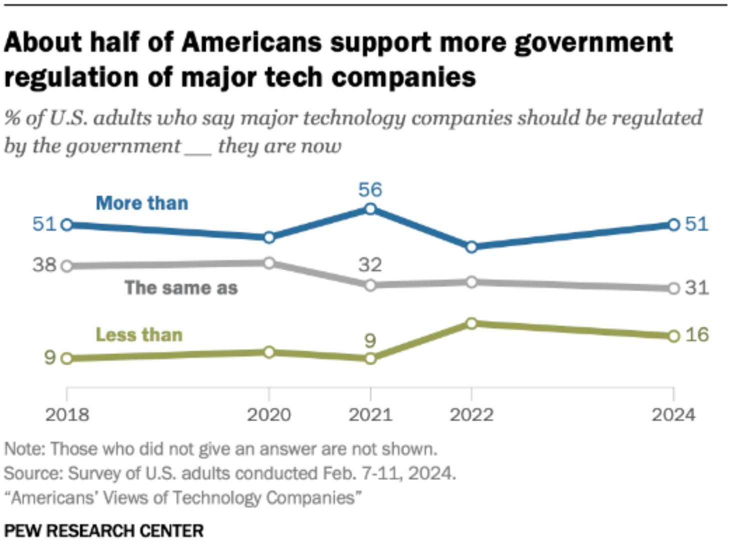
[44] Beshay, "Audiences Are Declining for Traditional News Media in the U.S. – With Some Exceptions," *Pew Research Center*, April 14, 2024, https://www.pewresearch.org/short-reads/2023/11/28/audiences-are-declining-for-traditional-news-media-in-the-us-with-some-exceptions/.

[45] Soroush Vosoughi, Deb Roy, and Sinan Aral, "The Spread of True and False News Online," *Science* 359, no. 6380 (March 9, 2018): 1146–51, https://doi.org/10.1126/science.aap9559.

two opposing trends. First, users primarily see content that reinforces existing beliefs to maintain engagement.[46] This induces homophily, where groups share increasingly strong beliefs and view individuals with differing beliefs with increasing negativity. Secondly, negative emotions, including fear, anger, and comparison, generate greater user engagement than positive emotions. Empirical research confirms this, and a survey of Americans found that anger was one of the two emotions most frequently experienced while on social media.[47]

Limited Accountability and Responsibility

While social media platforms have become prominent channels for disseminating news, they often eschew the associated responsibility of verifying the accuracy of the information they distribute. Instead, social media platforms have been viewed through the lens of Section 230 of the Communications Decency Act, passed in 1996, which says an "interactive computer service" cannot be treated as the publisher or speaker of third-party content.[48] As such, social media platforms are not liable for content posted by third parties and are not held to the same standards as broadcasting companies. There is vigorous ongoing debate in the U.S about balancing social media regulation with the protection of free speech, a fundamental democratic value.



About half of Americans support more government regulation of major tech companies

% of U.S. adults who say major technology companies should be regulated by the government __ they are now

Note: Those who did not give an answer are not shown.
Source: Survey of U.S. adults conducted Feb. 7-11, 2024.
"Americans' Views of Technology Companies"

PEW RESEARCH CENTER

Figure 2 Pew Research Study on American's Views of Regulating Technology Companies

Limited Social Media Literacy

With the rocket-like rise in disinformation and deep fakes, the need for an informed and educated

[46] Glenn S. Gerstell, "The National-Security Case for Fixing Social Media," *The New Yorker*, November 13, 2020, https://www.newyorker.com/tech/annals-of-technology/the-national-security-case-for-fixing-social-media.

[47] Susann Kohout, Sanne Kruikemeier, and Bert N. Bakker, "May I Have Your Attention, Please? An Eye Tracking Study on Emotional Social Media Comments," *Computers in Human Behavior* 139 (February 2023): 107495, https://doi.org/10.1016/j.chb.2022.107495; Aaron Smith, "Public Attitudes Toward Computer Algorithms" (Pew Research Center, November 16, 2018), https://www.pewresearch.org/internet/2018/11/16/algorithms-in-action-the-content-people-see-on-social-media/.

[48] Valerie C. Brannon and Eric N. Holmes, "Section 230: An Overview," accessed April 24, 2024, https://crsreports.congress.gov/product/pdf/R/R46751.

populace has never been greater.[49] CISA's efforts in social media education largely limited to infographics and tools users can leverage to mitigate vulnerabilities. Additionally, the 2023 Cyber Workforce and Education Strategy addressed the need to be aware of the threats posed by social media and cyber but similarly did not prioritize education. [50]

Only three states require digital literacy in their K-12 education systems.[51] Public service announcements, such as those by the Ad-Council, do not address social media literacy, although it is recognized as a societal threat. All the platforms make social media literacy a "user pull" function since deliberately making people aware of the risks may lead them to spend less time on the platforms and, hence, less revenue.

The national security threats stemming from digital illiteracy are significant. Contemporary national security debates focus on the impacts of malign disinformation campaigns on Western democracies. Many campaigns originate in autocratic nations, driven by algorithms and bots to fill social media feeds with content designed to illicit anger or reaffirm false narratives leading to societal divisions. Although not readily apparent, the success of malign information campaigns has its roots in a digitally illiterate population.

Low Level of Trust in Traditional Media

In the 24/7 misinformation and disinformation era, the American population has never been more vulnerable to invisible adversary influence via algorithms that dominate everyday life. As social media use for news and commentary increases, trust in the accuracy of the information has declined, likely contributing to similar declines in government and media trust.

Today, Americans trust the government and the media less than in the mid-2000s, making it more difficult for the government to mobilize public support. Pew Research Center has shown that trust in government has noticeably declined since 2005, regardless of political party or ideology.[52] This mirrors a long-running Gallup poll on trust in mass media—defined as newspapers, TV, and radio—which has seen a 14-percentage point decline in trust between 2005 and 2021.[53]

[49] Jeff Seldin, "Foreign Election Disinformation Campaigns Well Underway, Researchers Say," Voice of America, October 13, 2022, https://www.voanews.com/a/foreign-election-disinformation-campaigns-well-underway-researchers-say-/6789393.html.

[50] The White House, "FACT SHEET: Biden-Harris Administration Announces National Cyber Workforce and Education Strategy, Unleashing America's Cyber Talent," The White House, July 31, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/31/fact-sheet-biden-harris-administration-announces-national-cyber-workforce-and-education-strategy-unleashing-americas-cyber-talent/.

[51] Pat Condo, "Just 3 States Require Teaching Media Literacy. Growth of AI Makes It Essential," October 10, 2023, https://www.the74million.org/article/just-3-states-require-teaching-media-literacy-growth-of-ai-makes-it-essential/.

[52] Peter Bell, "Public Trust in Government: 1958-2023," Pew Research Center, September 19, 2023, https://www.pewresearch.org/politics/2023/09/19/public-trust-in-government-1958-2023/.

[53] Megan Brenan, "Americans' Trust in Media Dips to Second Lowest on Record," Gallup, October 7, 2021, https://news.gallup.com/poll/355526/americans-trust-media-dips-second-lowest-record.aspx.

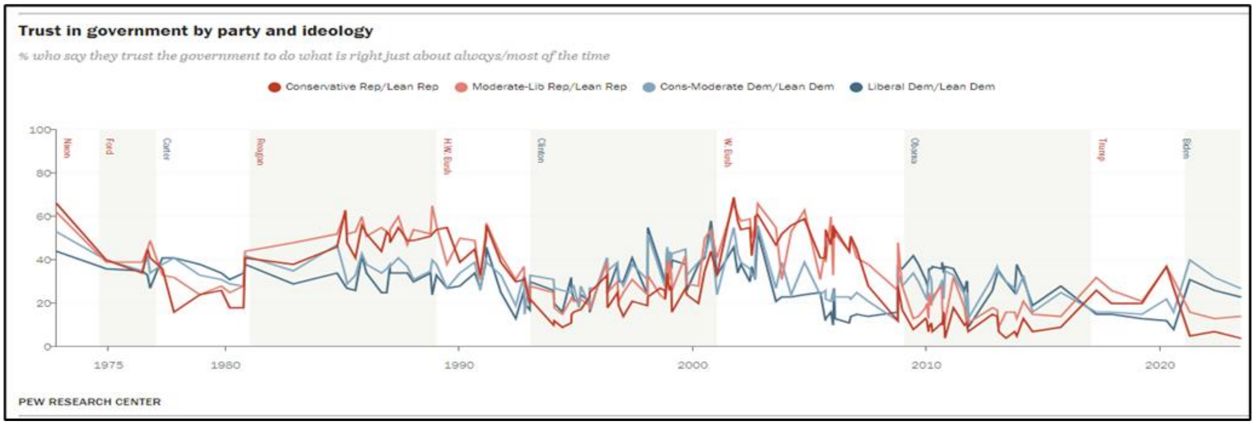


Figure 3: Pew Research Center's Trust in U.S. Government Survey, with Trust Measurements for Four Political Ideologies Spanning Both Major Political Parties Between 1973 and 2023

Pew Research Center surveys show that inaccuracy is the top concern of U.S. adults consuming news on social media, with the strength of that concern growing 9 percentage points from 2018 to 2023.[54] Another Pew Research survey showed that six in ten U.S. adults believed news on social media was inaccurate, with nearly identical results each year from 2018 to 2020.[55]

[54] Luxuan Wang and Naomi Forman-Katz, "Many Americans Find Value in Getting News on Social Media, but Concerns about Inaccuracy Have Risen," *Pew Research Center* (blog), February 7, 2024, https://www.pewresearch.org/short-reads/2024/02/07/many-americans-find-value-in-getting-news-on-social-media-but-concerns-about-inaccuracy-have-risen/.

[55] Elisa Shearer and Amy Mitchell, "News Use Across Social Media Platforms in 2020," Pew Research Center, January 12, 2021, https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/.

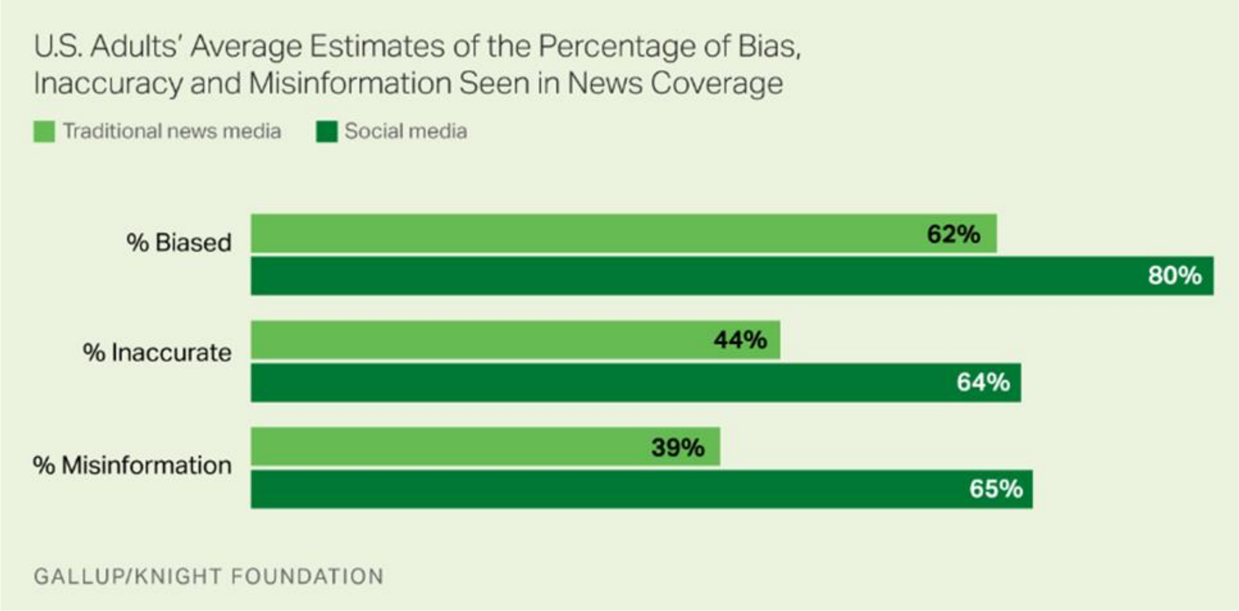


Figure 4: 2018 Gallup Poll Highlighting Strong U.S. Adult Perceptions of Bias, Inaccuracy, and Misinformation in Social Media and News Coverage[56]

As trust in informational accuracy declines, research from the Knight Foundation shows that Americans' willingness to pay for news also declines.[57] Without paid subscribers, news outlet profitability becomes increasingly tied to digital advertising, further incentivizing biased journalism to capture social media platform algorithms.

National Security Implications

> *Cybersecurity is essential to the basic functioning of our economy, the operations of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."*
>
> *-President Joseph R. Biden*
> *2023 National Cybersecurity Strategy*

[56] Jeffrey M. Jones, "Americans: Much Misinformation, Bias, Inaccuracy in News," Gallup, June 20, 2018, https://news.gallup.com/opinion/gallup/235796/americans-misinformation-bias-inaccuracy-news.aspx.
[57] Gallup and Knight Foundation, "American Views 2022."

U.S. Cyber Deterrence Policy Failures

While increased cyber interconnectedness creates opportunities, it also brings unprecedented cybersecurity challenges to the United States and its allies. The weaponization of information, coupled with the revolutionary technological advancements of the 21st century, enables rapid change in the strategic environment, likely redefining both competition and conflict at home and around the globe. Adversaries use proxies, state-sponsored cyber forces, and cybercriminals to influence political will. This new reality has profound national security implications for the United States.

In recognition of the increasing impact of information, in 2017, the Chairman of the Joint Chiefs of Staff issued an out-of-cycle change to Joint Publication 1, Doctrine of the Armed Forces of the United States, introducing "Information" as the Seventh Joint Function.[58] This issuance portends significant changes in how the joint force plans and executes transregional, multidomain, and multifunctional operations.[59]

President Biden noted in his administration's 2023 National Cybersecurity Strategy, "Cybersecurity is essential to the basic functioning of our economy, the operation of our critical infrastructure, the strength of our democracy and democratic institutions, the privacy of our data and communications, and our national defense."[60] The strategy, coupled with efforts included in an Executive Order on Improving the Nation's Cybersecurity[61], attempts to address the growing risks cyberspace brings to national security. However, even with the added emphasis by senior officials, there are countless examples of U.S. cyber deterrence failures. Those failures put U.S. critical infrastructure at risk.

At the heart of U.S. national security are the foundational tenets of a democracy. "Elections play a vital role in a free and fair society and are a cornerstone of American democracy."[62] When Russia meddled in the U.S. elections, the foundation of the nation was shaken. Russia's adversarial influence in cyberspace remains significant, planting seeds of mistrust and fueling polarized sentiments nationwide. Sowing mistrust across the spectrum of media while simultaneously attacking critical infrastructure, adversarial threats persistently compromise democracy. In January 2017, the Department of Homeland Security officially designated election infrastructure as a subset of the government facilities sector, making clear that election infrastructure qualifies as

[58] James Van de Velde, Information and Cyberspace Lesson 1 Presentation, slide 7.

[59] Grynkewich, Alexus G. "Introducing Information as a Joint Function." Joint Force Quarterly, April 1, 2018. https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-89/jfq-89_6-7_Grynkewich.pdf?ver=2018-04-11-125441-307.

[60] The White House, National Cybersecurity Strategy (Washington, D.C., March 1, 2023), 1.

[61] The White House, "Executive Order on Improving the Nation's Cybersecurity," The White House, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[62] Homeland Security. *Election Security*. Updated November 6, 2023. https://www.dhs.gov/topics/election-security

critical infrastructure.[63] Fast forward seven years, and U.S. Secretary of State Anthony Blinken said the United States now sees evidence of Chinese attempts to influence and interfere with the upcoming elections, despite an earlier commitment from Chairman Xi not to do so.[64]

Similarly, cyberspace allows governments, organizations, and individuals to connect at scale globally. Communities of interest and niche groups, including extremists and other malign actors, can develop and grow unconstrained by distance. Tech giants use addictive algorithms to influence behavior. Social media has allowed for personalized press, meaning that users are likelier to be shown information that adheres to and supports their worldview.[65] It is not a natural human tendency to consider both sides of an argument. Adversaries and MCAs can target user vulnerabilities through artificial homophily enabled by social media to weaken trust in democratic institutions and drive further schisms across the United States. Artificial homophily provides credibility by mirroring a target audience's ideas, culture, and ethnicity. This credibility increases the ability of malicious actors like the Russian Internet Research Agency (IRA) or the Chinese Communist Party to inflame tensions across the United States.

Impact of Malign Information Operations

Malign information operations are a growing threat to U.S. national security, leveraging the pervasive reach of digital technology to undermine democratic institutions, sow discord, and manipulate public opinion. These operations, conducted by foreign and domestic actors, exploit the interconnectedness of the digital age to spread disinformation rapidly and widely, challenging America's resilience and response capabilities.

Malign information operations—aimed at undermining democracy and threatening national security—are becoming more prevalent and influential.

The digital revolution has connected the world like never before, providing a platform for rapid disinformation operations and malign influence aimed at causing instability and threatening national security. American adversaries launch information operations in the digital environment to undermine democratic institutions, sow discord, amplify divisions, and erode trust in the media. Just as the character of war changes with the evolution of technology, so too does the design and distribution of disinformation operations.

Malign information operations occur in the gray zone below the threshold of conflict. The ambiguity and uncertainty that characterize successful information operations campaigns give the

[63] Cybersecurity & Infrastructure Security Agency. *Election Security.* Accessed April 23, 2024. https://www.cisa.gov/topics/election-security.

[64] Simone McCarthy, "Blinken tells CNN the US has seen evidence of China attempting to Influence upcoming US elections," April 26, 2024, accessed April 26, 2024, https://www.cnn.com/2024/04/26/politics/blinken-china-interview-intl-hnk/index.html.

[65] Kyle Chin, "The Impact of Social Media on Cybersecurity," May 8, 2023, https://www.upguard.com/blog/the-impact-of-social-media-on-cybersecurity#:~:text=Exposure%20to%20a%20user's%20social,potential%20identity%20fraud%20or%20theft.

adversary the advantage and place the United States. in a reactionary posture. These operations are especially effective in strategic competition because they are inexpensive, simple, and subtle; attribution is challenging, and devising a response depends on a nation's political will and risk tolerance. Malign information operations are an asymmetric alternative to conventional weapons and serve to confuse, disorient, distract, overwhelm, and cause decision paralysis.

Malign information operations sow discord and amplify divisions, creating instability and polarization.

Malign information operations exploit societal vulnerabilities by targeting fragmented or polarized communities to deepen divisions and incite conflict. By manipulating pre-existing beliefs and emotions, these operations amplify the natural tendency toward homophily, where individuals prefer information confirming their worldviews. This strategy effectively silences diverse perspectives and critical discourse, reinforcing echo chambers that compromise societal resilience and complicate efforts to unify matters of public concern.

Malign influence operations amplify or create conspiracy theories that cause confusion at one end of the spectrum and cause harm at the other.

These operations use disinformation and misinformation to seed doubt and mistrust among the public. At one end of the spectrum, these operations confuse by muddling the truth, making it difficult for individuals to discern fact from fiction. This confusion can lead to public indecision or apathy towards critical societal issues, paralyzing civic engagement. On the other hand, these operations can cause significant harm. By promoting false narratives and conspiracy theories, they can incite real-world violence, fuel hatred, and deepen social divides.

Revanchist autocracies are weaponizing social media to weaken democracy and undermine the rules-based global order.

Russia's information and propaganda operations are not new, but the speed and frequency with which disinformation spreads is unprecedented and will continue to increase as AI advances exponentially. China's disinformation efforts similarly continue to mature and evolve as objectives expand from population repression to aggressive pro-China narratives, touting an ideological alternative to the declining West. Beijing’s narratives will also increasingly be AI-driven.

PRC and Russia are increasing coordination on malign information operations.

The PRC and Russia have been using coordinated efforts on social media to spread disinformation and influence public opinion, particularly regarding the war in Ukraine. Case in point, in September 2022, Meta disrupted misinformation campaigns from the PRC and Russia that targeted Ukrainians and exploited Ukraine's tensions with Russia. Additionally, in August 2023, Meta took down the largest covert Chinese influence operation it had seen, which used a sprawling network of fake accounts across over fifty websites to spread pro-China messages and attack critics of Beijing's policies. The operation failed to gain a large following but demonstrated China's investment in state propaganda.[66]

Domestic actors—America's homegrown digital authoritarians—also wield disinformation to disorient and manipulate the public.

While foreign malign information operations often capture headlines, domestic fringe media outlets, and unscrupulous political figures and their supporters have also adopted a deliberate strategy to cultivate confusion and information fatigue, erode trust in traditional media, redirect attention from their policy failures, and maintain control over political narratives in support of their agendas. These efforts threaten U.S. national security, which must be tackled at home.

Supporting Industries and Supply Chain Issues

Vulnerabilities in the cyber domain have repercussions across all sectors, and addressing cyber and information threats requires effort from the whole society, including private industry, academia, civil society, and government. It must also include the involvement of individual users whose poor cyber hygiene or unwitting amplification of malign influence operations represent threats to national security.

Supporting Industries

- Large tech corporations, e.g., Microsoft, Google, Amazon
- Cybersecurity firms
- Critical infrastructure companies
- Small, medium, and large enterprises across supply chains (Cybersecurity lapses at any point in the supply chain can create broad vulnerabilities)
- Academic institutions- higher education and K-12
- Social media companies
- Public and private media outlets
- Non-governmental organizations

Government Institutions

Government leadership and coordination are essential to protecting U.S. national security in the cyber domain. Protecting the cyber domain involves a cross-section of government entities:

- The National Cyber Director
- CISA
- NSA
- NIST
- DOJ
- FBI

[66] Shannon Bond, "Meta Says Chinese, Russian Influence Operations Are among the Biggest It's Taken Down," *NPR*, August 29, 2023, sec. Untangling Disinformation, https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d.

- DHS
- Department of Defense
- Department of State
- Department of Education
- State and Local Authorities

Allies and Partners

Coordination must include allies and partners to create “a world where responsible state behavior in cyberspace is expected and reinforced and where irresponsible behavior is isolating and costly.”[67] The United States must coordinate through bilateral diplomacy and multilateral engagement, including with NATO, the United Nations, and other multinational bodies and institutions.

Supply Chain Issues

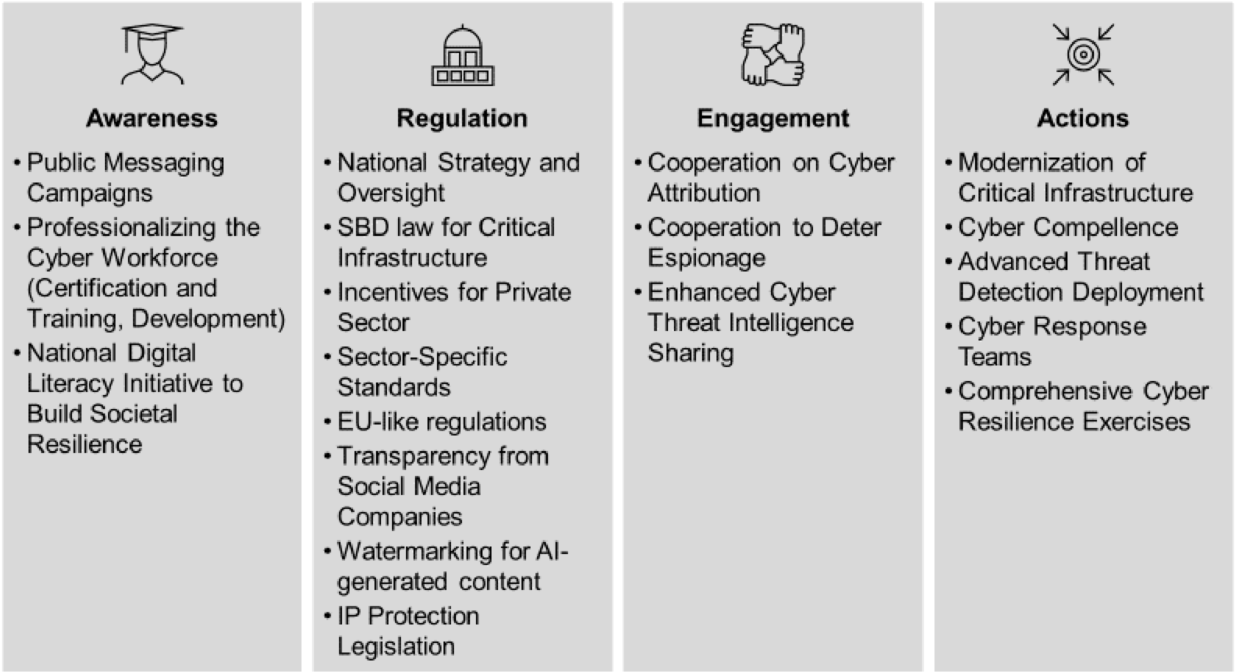
Supply chain vulnerabilities in the cyber domain stem from third-party vendors, poor information security across the supply chain, vulnerabilities in software or hardware, lack of workforce capacity to meet the needs of industry and government, and the subsequent need to rely on foreign workers to meet the demand.[68]

Lines of Effort and Corresponding Recommendations

The following recommendations are designed to address the abovementioned challenges and are assigned by line of effort: awareness and education, engagement and collaboration, regulation and governance, and targeted action. Implementing these recommendations will likely strengthen U.S. national security by improving cyber and information operations defenses and resiliency.

[67] The White House, “FACT SHEET: Biden-Harris Administration Announces National Cybersecurity Strategy,” The White House, March 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/.

[68] “Building More Resilient ICT Supply Chains Fact Sheet | CISA,” April 3, 2023, https://www.cisa.gov/resources-tools/resources/building-more-resilient-ict-supply-chains-fact-sheet.



Awareness

- Public Messaging Campaigns
- Professionalizing the Cyber Workforce (Certification and Training, Development)
- National Digital Literacy Initiative to Build Societal Resilience

Regulation

- National Strategy and Oversight
- SBD law for Critical Infrastructure
- Incentives for Private Sector
- Sector-Specific Standards
- EU-like regulations
- Transparency from Social Media Companies
- Watermarking for AI-generated content
- IP Protection Legislation

Engagement

- Cooperation on Cyber Attribution
- Cooperation to Deter Espionage
- Enhanced Cyber Threat Intelligence Sharing

Actions

- Modernization of Critical Infrastructure
- Cyber Compellence
- Advanced Threat Detection Deployment
- Cyber Response Teams
- Comprehensive Cyber Resilience Exercises

Figure 5: Lines of Effort Chart

Line of Effort 1: Awareness and Education

Public Messaging Campaigns

To counter divisive information operations and loss of trust, all relevant agencies, led by the White House, should proactively and consistently engage the domestic public via the press, social media, and public outreach, with consistent messaging underscoring the strength and importance of American democracy and democratic institutions, including the value of a free press. Concurrent messaging to foreign audiences should emphasize democratic values and the commitment of the United States as a reliable partner in support of those values. Both campaigns should focus on how democracy has delivered for its citizens. "International examples suggest people are motivated by positive messages and concrete actions."[69]

Professionalizing the Cyber Workforce (Certification and Training, Development)

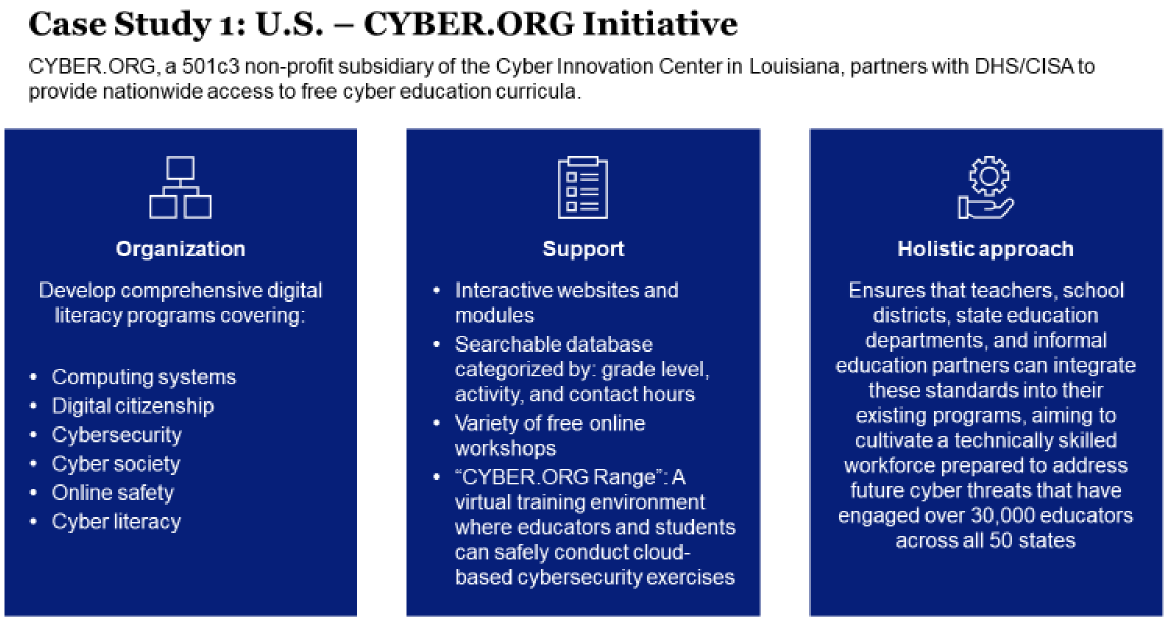
Implement continuing education requirements for cybersecurity/IT/OT professionals in critical infrastructure sectors. The U.S must prioritize a human capital strategy to improve performance and grow a stronger cybersecurity workforce. In the DOD, there must be career paths in the military for cyber professionals to progress through the ranks, develop technical expertise, and

[69] Rachel Kleinfeld, "Five Strategies to Support U.S. Democracy," Carnegie Endowment for International Peace, accessed May 8, 2024, https://carnegieendowment.org/2022/09/15/five-strategies-to-support-Unite-democracy-pub-87918.

hone the skills required to thrive in a highly competitive field. Cultivating a competitive cyber workforce can extend beyond the DoD. Industry, especially within the sixteen critical sectors, must also incentivize and develop cyber experts. Furthermore, training cyber educators within the educational system is critical to building resilient users.

Establish a National Digital Literacy Initiative to Build Societal Resilience

Develop and implement a comprehensive K-12 digital literacy campaign to equip the next generation with critical cyber hygiene and civic education skills. This initiative will enhance societal resilience against malign information threats and support a generational approach to safeguarding national security. The following are case study models that can be emulated nationally.



Case Study 1: U.S. – CYBER.ORG Initiative

CYBER.ORG, a 501c3 non-profit subsidiary of the Cyber Innovation Center in Louisiana, partners with DHS/CISA to provide nationwide access to free cyber education curricula.

Organization

Develop comprehensive digital literacy programs covering:

- Computing systems
- Digital citizenship
- Cybersecurity
- Cyber society
- Online safety
- Cyber literacy

Support

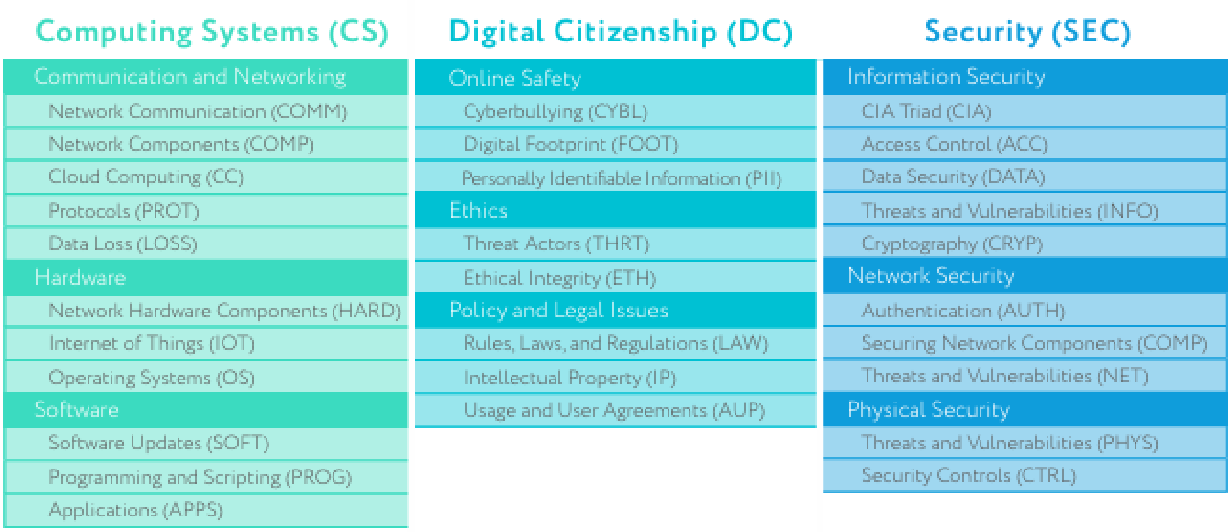
- Interactive websites and modules
- Searchable database categorized by: grade level, activity, and contact hours
- Variety of free online workshops
- "CYBER.ORG Range": A virtual training environment where educators and students can safely conduct cloud-based cybersecurity exercises

Holistic approach

Ensures that teachers, school districts, state education departments, and informal education partners can integrate these standards into their existing programs, aiming to cultivate a technically skilled workforce prepared to address future cyber threats that have engaged over 30,000 educators across all 50 states

Case Study 1: U.S. - CYBER.ORG Initiative

CYBER.ORG, a 501c3 non-profit subsidiary of the Cyber Innovation Center in Louisiana, partners with DHS/CISA to provide nationwide access to free cyber education curricula. The organization develops comprehensive digital literacy programs covering several topics, including computing systems, digital citizenship, cybersecurity, cyber society, online safety, and cyber literacy. CYBER.ORG supports these curricula with interactive websites and modules and a searchable database categorized by grade level, activity, and contact hours. The organization also offers a variety of free online workshops and has developed the "CYBER.ORG Range," a virtual training environment where educators and students can safely conduct cloud-based cybersecurity exercises. This comprehensive approach ensures teachers, school districts, state education departments, and informal education partners can integrate these standards into existing programs, aiming to cultivate a technically skilled workforce prepared to address future cyber threats. This expansive outreach has engaged over 30,000 educators across all fifty states. [70] [71] [72] [73] [74] [75]



Computing Systems (CS)	Digital Citizenship (DC)	Security (SEC)
Communication and Networking	Online Safety	Information Security
Network Communication (COMM)	Cyberbullying (CYBL)	CIA Triad (CIA)
Network Components (COMP)	Digital Footprint (FOOT)	Access Control (ACC)
Cloud Computing (CC)	Personally Identifiable Information (PII)	Data Security (DATA)
Protocols (PROT)	Ethics	Threats and Vulnerabilities (INFO)
Data Loss (LOSS)	Threat Actors (THRT)	Cryptography (CRYP)
Hardware	Ethical Integrity (ETH)	Network Security
Network Hardware Components (HARD)	Policy and Legal Issues	Authentication (AUTH)
Internet of Things (IOT)	Rules, Laws, and Regulations (LAW)	Securing Network Components (COMP)
Operating Systems (OS)	Intellectual Property (IP)	Threats and Vulnerabilities (NET)
Software	Usage and User Agreements (AUP)	Physical Security
Software Updates (SOFT)		Threats and Vulnerabilities (PHYS)
Programming and Scripting (PROG)		Security Controls (CTRL)
Applications (APPS)		

Figure 6: K-12 Cybersecurity Learning Standards

[70] Cyber Innovation Center, “Cyber.Org - Education,” accessed April 24, 2024, https://www.cyberinnovationcenter.org/education.”

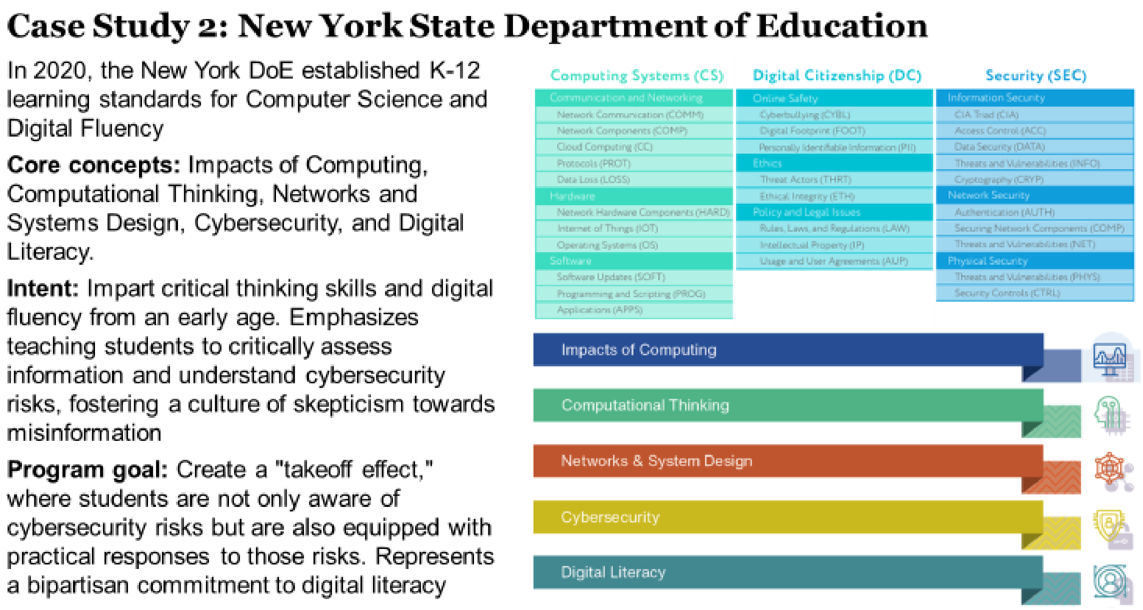
[71] Cyber Innovation Center, “Cyber Innovation Center Awarded $129M in Federal Funding to Boost Louisiana’s Cybersecurity Leadership, Air Force Innovation,” October 31, 2023, https://www.cyberinnovationcenter.org/news/cyber-innovation-center-awarded-129m-in-federal-funding-to-boost-louisiana-cybersecurity-national-security.

[72] CYBER.ORG, “K12 Cybersecurity Learning Standards” (Cyber Innovation Center, 4 Aug 21), https://cyber.org/sites/default/files/2021-10/K-12%20Cybersecurity%20Learning%20Standards_1.0.pdf.

[73] CYBER.ORG, “Find Curricula,” accessed April 24, 2024, https://cyber.org/find-curricula.

[74] CYBER.ORG, “Events,” accessed April 24, 2024, https://cyber.org/workshops-events/events.

[75] CYBER.ORG, “CYBER.ORG Range,” accessed April 24, 2024, https://cyber.org/range.



Case Study 2: New York State Department of Education

In 2020, the New York DoE established K-12 learning standards for Computer Science and Digital Fluency

Core concepts: Impacts of Computing, Computational Thinking, Networks and Systems Design, Cybersecurity, and Digital Literacy.

Intent: Impart critical thinking skills and digital fluency from an early age. Emphasizes teaching students to critically assess information and understand cybersecurity risks, fostering a culture of skepticism towards misinformation

Program goal: Create a "takeoff effect," where students are not only aware of cybersecurity risks but are also equipped with practical responses to those risks. Represents a bipartisan commitment to digital literacy

Computing Systems (CS)

- Communication and Networking
  - Network Communication (COMM)
  - Network Components (COMP)
  - Cloud Computing (CC)
  - Protocols (PROT)
  - Data Loss (LOSS)
- Hardware
  - Network Hardware Components (HARD)
  - Internet of Things (IOT)
  - Operating Systems (OS)
- Software
  - Software Updates (SOFT)
  - Programming and Scripting (PROG)
  - Applications (APPS)

Digital Citizenship (DC)

- Online Safety
  - Cyberbullying (CYBL)
  - Digital Footprint (FOOT)
  - Personally Identifiable Information (PII)
- Ethics
  - Threat Actors (THRT)
  - Ethical Integrity (ETH)
- Policy and Legal Issues
  - Rules, Laws, and Regulations (LAW)
  - Intellectual Property (IP)
  - Usage and User Agreements (AUP)

Security (SEC)

- Information Security
  - CIA Triad (CIA)
  - Access Control (ACC)
  - Data Security (DATA)
  - Threats and Vulnerabilities (INFO)
  - Cryptography (CRYP)
- Network Security
  - Authentication (AUTH)
  - Securing Network Components (COMP)
  - Threats and Vulnerabilities (NET)
- Physical Security
  - Threats and Vulnerabilities (PHYS)
  - Security Controls (CTRL)

Impacts of Computing

Computational Thinking

Networks & System Design

Cybersecurity

Digital Literacy

Case Study 2: New York State Department of Education

In 2020, the New York State Department of Education established K-12 learning standards for Computer Science and Digital Fluency, covering five core concepts: Impacts of Computing, Computational Thinking, Networks and Systems Design, Cybersecurity, and Digital Literacy. These comprehensive standards are structured to impart critical thinking skills and digital fluency from an early age, with the curriculum spanning various sub-topics tailored to different grade levels. The initiative strongly emphasizes teaching students to critically assess information and understand cybersecurity risks, fostering a culture of skepticism towards misinformation. Colin Ahern, the state's Principal Cyber Advisor, articulates the program's goal as creating a "takeoff effect," where students are not only aware of cybersecurity risks but are also equipped with practical responses to those risks. The program represents a bipartisan commitment to digital literacy, ensuring students are prepared to navigate and secure the digital space effectively. [76] [77]

[76] New York State Education Department, "Computer Science and Digital Fluency Learning Standards," accessed April 24, 2024, https://www.nysed.gov/curriculum-instruction/computer-science-and-digital-fluency-learning-standards.

[77] Ahern.

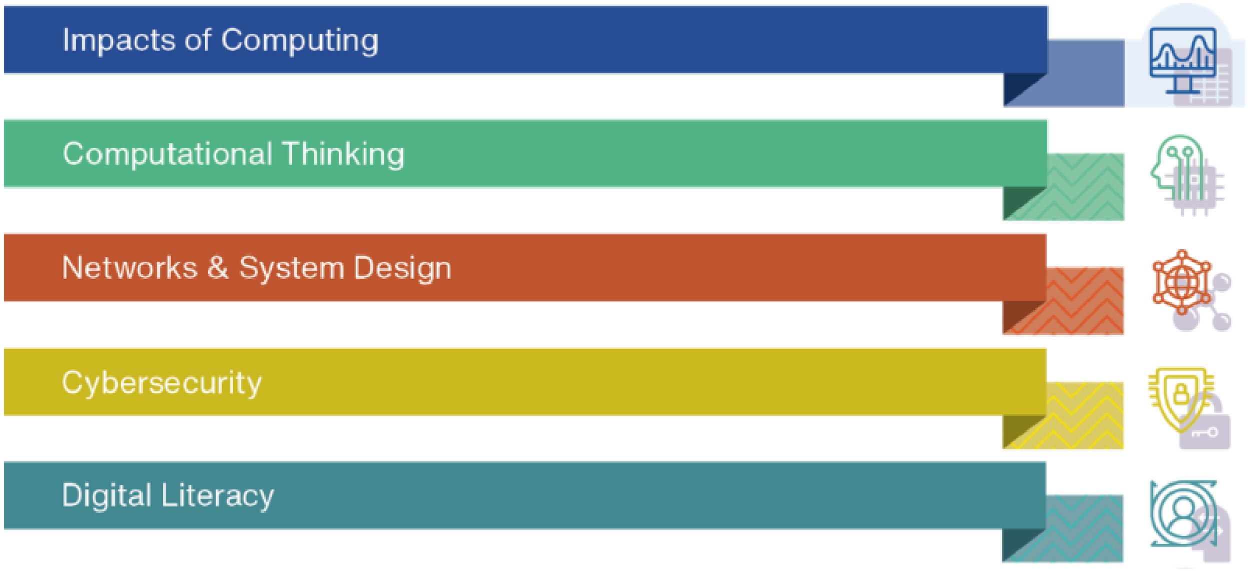
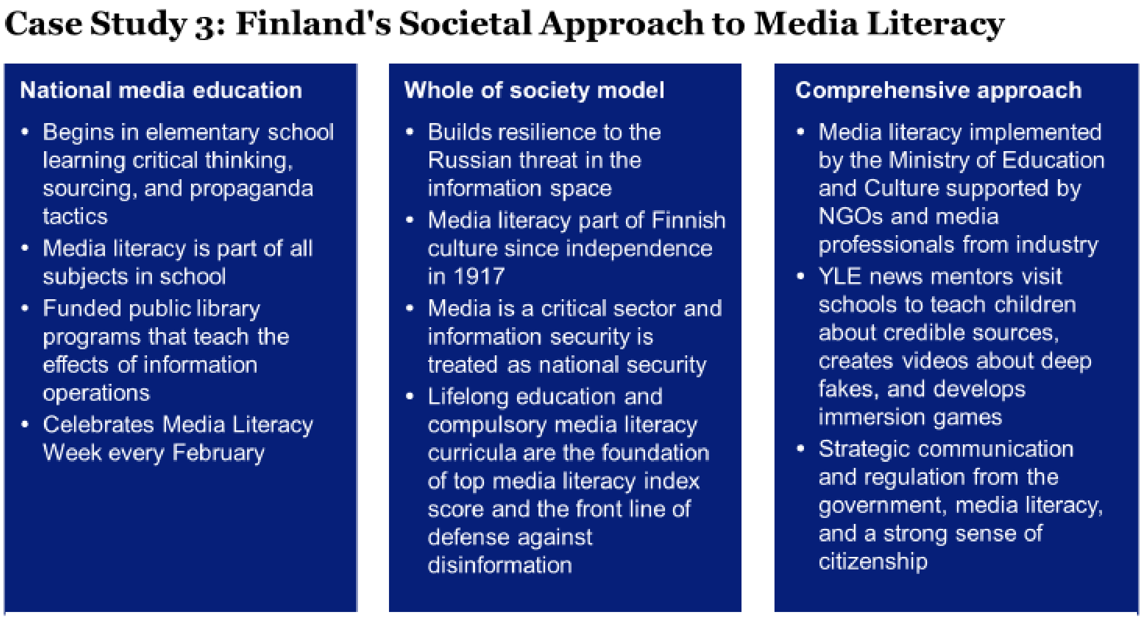


Figure 7: New York K-12 Learning Standards for Computer Science and Digital Fluency



Case Study 3: Finland's Societal Approach to Media Literacy

National media education

- Begins in elementary school learning critical thinking, sourcing, and propaganda tactics
- Media literacy is part of all subjects in school
- Funded public library programs that teach the effects of information operations
- Celebrates Media Literacy Week every February

Whole of society model

- Builds resilience to the Russian threat in the information space
- Media literacy part of Finnish culture since independence in 1917
- Media is a critical sector and information security is treated as national security
- Lifelong education and compulsory media literacy curricula are the foundation of top media literacy index score and the front line of defense against disinformation

Comprehensive approach

- Media literacy implemented by the Ministry of Education and Culture supported by NGOs and media professionals from industry
- YLE news mentors visit schools to teach children about credible sources, creates videos about deep fakes, and develops immersion games
- Strategic communication and regulation from the government, media literacy, and a strong sense of citizenship

Case Study 3: Finland's Societal Approach to Media Literacy

Finland employs a whole of society, cross-sector model to build resilience to the Russian threat in the information space. Media literacy (similar to digital literacy) has been a part of Finnish culture since its independence in 1917. Still, the country identified the need for further action following the uptick in Russian disinformation campaigns targeting immigration, the European

Union, and NATO membership in the early 2010s.[78] Media is a critical sector in Finland, and information security is treated as national security.[79] Lifelong education and compulsory media literacy curricula are the foundation of Finland's top media literacy index score and the front line of defense against disinformation.[80]

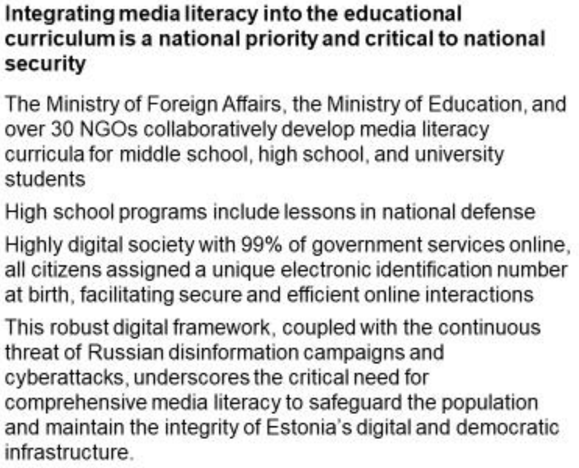
First published in 2013, Finland's national media education goals are comprehensive, high-quality, and systematic.[81] Beginning in elementary school, Finnish children learn critical thinking skills, source evaluation, and tactics of deception and propaganda.[82] Each subsequent year builds upon and deepens students' skills to identify disinformation, analyze the reliability of the information they consume, and question content. Media literacy is part of all subjects in school, from learning about statistics and algorithms in math to source evaluation and media criticism in literature to image manipulation in art.[83] To reach the adult population as part of the lifelong learning culture, the Finnish government has funded public library programs that teach the effects of information operations.[84] Further, Finland celebrates Media Literacy Week every February, where the country comes together to discuss new technology and TTP changes of malign actors.[85]

Finland adheres to a comprehensive security model to boost societal resilience. Media literacy ties into this model, and these education efforts are implemented by the National Audio-visual Institute under the Ministry of Education and Culture and supported by Non-Governmental Organizations (NGOs) and media professionals from the industry who provide fact-checking tools and educational materials that serve to fortify the population against Russia's disinformation campaigns.[86] YLE, a Finnish broadcasting company, has 14 news mentors who visit schools around Finland to teach children about credible sources. Additionally, the company creates videos about deep fakes and publishes them on its website. Finally, YLE develops immersion games where the player acts as a troll to create harmful material for massive disinformation distribution deliberately.[87]

Strategic communication and regulation from the government, media literacy curricula and educational materials from industry, and a strong sense of citizenship in Finland result in a resilient society where trust in the media and government is high.

[78] The Listening Post, “Inside Finland’s incredible education system,” Al Jazeera, podcast, January 22, 2024.
[79] Tero Koskinen, Mediapooli briefing, NDU/ES field study, April 19, 2024.
[80] Nordic Policy Centre, “Media Literacy Education in Finland,” The Australia Institute, November 12, 2020.
[81] Salomaa, Saara and Palsa, Lauri, “Media literacy in Finland: National media education policy,” Ministry of Education and Culture, December 16, 2019.
[82] Jenny Gross, “How Finland Is Teaching a Generation to Spot Misinformation,” *The NYTs*, January 10, 2023.
[83] The Listening Post, “Inside Finland’s incredible education system,” Al Jazeera, podcast, January 22, 2024.
[84] Jenny Gross, “How Finland Is Teaching a Generation to Spot Misinformation,” *The New York Times*, January 10, 2023.
[85] David J. Cord, “Educated Decisions: Finnish Media Literacy Deters Disinformation,” Ministry of Foreign Affairs, June 2022.
[86] Nordic Policy Centre, “Media Literacy Education in Finland,” The Australia Institute, November 12, 2020.
[87] The Listening Post, “Inside Finland’s incredible education system,” Al Jazeera, podcast, January 22, 2024.

Case Study 4: Estonia Collaborative Approach



Integrating media literacy into the educational curriculum is a national priority and critical to national security

The Ministry of Foreign Affairs, the Ministry of Education, and over 30 NGOs collaboratively develop media literacy curricula for middle school, high school, and university students

High school programs include lessons in national defense

Highly digital society with 99% of government services online, all citizens assigned a unique electronic identification number at birth, facilitating secure and efficient online interactions

This robust digital framework, coupled with the continuous threat of Russian disinformation campaigns and cyberattacks, underscores the critical need for comprehensive media literacy to safeguard the population and maintain the integrity of Estonia's digital and democratic infrastructure.

In Estonia, integrating media literacy into the educational curriculum is a national priority, reflecting its strategic importance to national defense. The Ministry of Foreign Affairs, Education, and over 30 NGOs collaboratively develop media literacy curricula for middle school, high school, and university students, with high school programs also including lessons in national defense lessons.[88] As a highly digital society with 99% of government services online, Estonia assigns a unique electronic identification number to all citizens at birth, facilitating secure and efficient online interactions. This robust digital framework, coupled with the continuous threat of Russian disinformation, underscores the critical need for comprehensive media literacy to safeguard the population and maintain the integrity of Estonia's digital and democratic infrastructure. [89]

Line of Effort 2: Regulation and Governance

National Strategy and Oversight

National Security Memorandum (NSM)-22, released on April 30, 2024, designates the DHS Secretary acting through the Director of CISA as "National Coordinator" for Critical Infrastructure Security and Resilience.[90] However, CISA must be resourced appropriately to fulfill duties, responsibilities, and authorities adequately.

Secure-By-Design Law for Critical Infrastructure

The United States should mandate that all companies identified by DHS/CISA as operating

[88] Estonia Ministry of Defense, Information System Authority briefing, NDU/ES field study, April 16, 2024.

[89] e-Estonia Briefing Center, "We have built a digital society, and we can show you how," briefing, NDU/ES field study, April 16, 2024.

[90] The White House, "National Security Memorandum on Critical Infrastructure Security and Resilience," last modified April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

“critical infrastructure” implement SBD principles. This law would require the elimination of default passwords, enforcement of multi-factor authentication, and mandatory password resets upon system activation. Additionally, these companies must report all attempted cyberattacks to CISA and the FBI. This regulation aims to eliminate outdated security practices and bolster the resilience of critical infrastructures against cyber threats.

Incentives for Strengthening Cybersecurity

Use tax incentives, grants, and regulatory requirements to encourage private sector participation in improving infrastructure resilience.

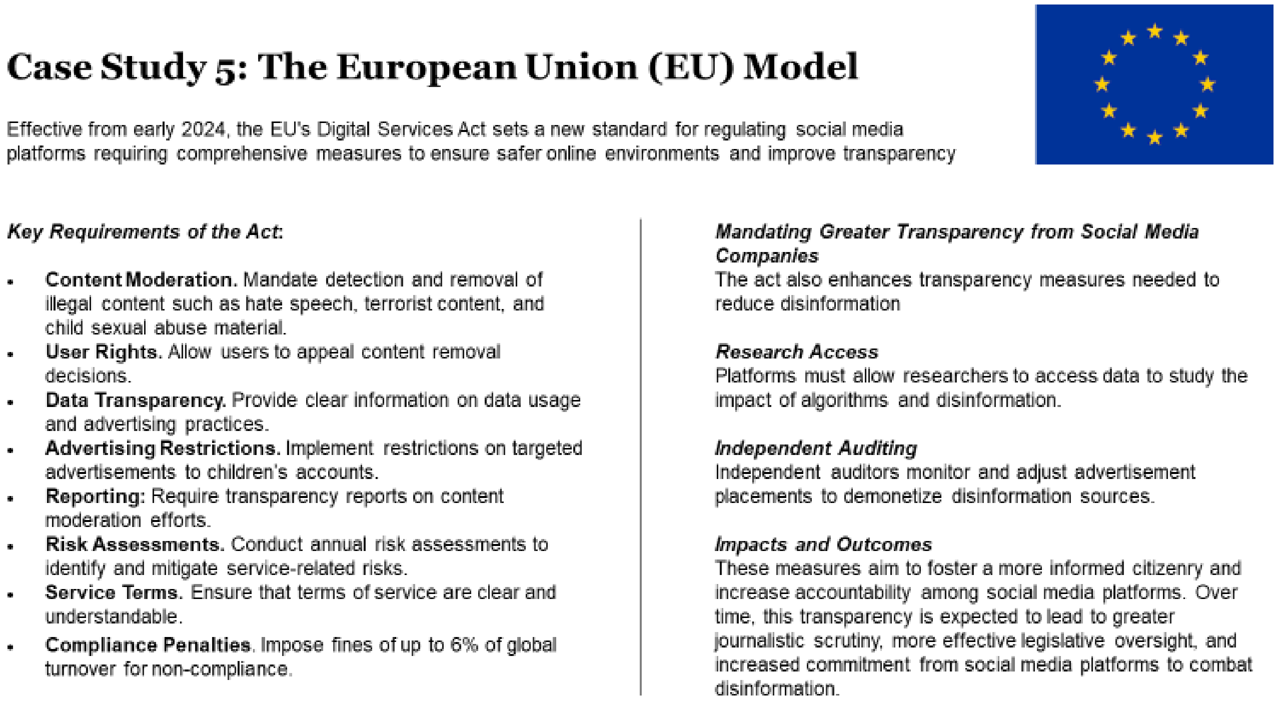
Sector-Specific Cybersecurity Standards

Develop tailored cybersecurity standards for each sector, facilitated by the designated SRMA in collaboration with DHS/CISA and industry leaders.

Implement credible and sensible regulations in the United States similar to the EU model.

Though social media is a relatively recent technological advancement, U.S. legislative measures for this sector still need to be developed. Current regulatory perspectives are primarily shaped by Section 230 of the Communications Decency Act of 1996, stipulating that an "interactive computer service" cannot be treated as the publisher or speaker of third-party content. This provision shields platforms from legal liability for user-generated content, with specific exceptions for copyright violations and breaches of federal criminal law.[91] However, as originally conceived, Section 230 is increasingly seen as inadequate for addressing the complexities and challenges of today's digital and social media landscape.

[91] Valerie C. Brannon and Eric N. Holmes, “Section 230: An Overview,” accessed April 24, 2024, https://crsreports.congress.gov/product/pdf/R/R46751.



Case Study 5: The European Union (EU) Model

Effective from early 2024, the EU's Digital Services Act sets a new standard for regulating social media platforms requiring comprehensive measures to ensure safer online environments and improve transparency

***Key Requirements of the Act*:**

- **Content Moderation.** Mandate detection and removal of illegal content such as hate speech, terrorist content, and child sexual abuse material.
- **User Rights.** Allow users to appeal content removal decisions.
- **Data Transparency.** Provide clear information on data usage and advertising practices.
- **Advertising Restrictions.** Implement restrictions on targeted advertisements to children's accounts.
- **Reporting:** Require transparency reports on content moderation efforts.
- **Risk Assessments.** Conduct annual risk assessments to identify and mitigate service-related risks.
- **Service Terms.** Ensure that terms of service are clear and understandable.
- **Compliance Penalties**. Impose fines of up to 6% of global turnover for non-compliance.

Mandating Greater Transparency from Social Media Companies
The act also enhances transparency measures needed to reduce disinformation

Research Access
Platforms must allow researchers to access data to study the impact of algorithms and disinformation.

Independent Auditing
Independent auditors monitor and adjust advertisement placements to demonetize disinformation sources.

Impacts and Outcomes
These measures aim to foster a more informed citizenry and increase accountability among social media platforms. Over time, this transparency is expected to lead to greater journalistic scrutiny, more effective legislative oversight, and increased commitment from social media platforms to combat disinformation.

Case Study 5: The European Union Model

Enacted in 2022 and effective from early 2024, the EU's Digital Services Act sets a new standard for regulating social media platforms. This legislation requires comprehensive measures to ensure safer online environments and improve transparency, which could serve as a model for the United States.

***Key Requirements of the Act*:**

- **Content Moderation.** Mandate detection and removal of illegal content such as hate speech, terrorist content, and child sexual abuse material.
- **User Rights.** Allow users to appeal content removal decisions.
- **Data Transparency.** Provide clear information on data usage and advertising practices.
- **Advertising Restrictions.** Implement restrictions on targeted advertisements to children's accounts.
- **Reporting:** Require transparency reports on content moderation efforts.
- **Risk Assessments.** Conduct annual risk assessments to identify and mitigate service-related risks.
- **Service Terms.** Ensure that terms of service are clear and understandable.
- **Compliance Penalties**. Impose fines of up to 6% of global turnover for non-compliance.[92]

[92] "A Guide to the Digital Services Act, the EU's New Law to Rein in Big Tech," Algorithm Watch, updated August 22, 2023, https://algorithmwatch.org/en/dsa-explained.

Mandating Greater Transparency from Social Media Companies

The act also enhances transparency measures needed to reduce disinformation:

> ***Research Access.*** Platforms must allow researchers to access data to study the impact of algorithms and disinformation.
>
> ***Independent Auditing.*** Independent auditors monitor and adjust advertisement placements to demonetize disinformation sources.[93]
>
> ***Impacts and Outcomes.*** These measures aim to foster a more informed citizenry and increase accountability among social media platforms. Over time, this transparency is expected to lead to greater journalistic scrutiny, more effective legislative oversight, and increased commitment from social media platforms to combat disinformation.

Implement Watermarking Systems for AI-Generated Content

In consultation with the most prominent U.S. generative AI companies, Congress should pass legislation mandating watermarking of AI-generated content to combat disinformation. Watermarking involves embedding information into AI outputs that allow users to understand if the content is synthetic and verify its authenticity.[94] There is comprehensive academic and industry support for this approach.[95] Snapchat has already embedded watermarks into all of its AI-generated content.[96] The Biden Administration laid the groundwork for this effort with an executive order requiring the Commerce Department to develop "science-backed standards and techniques for:

- authenticating content and tracking its provenance
- labeling synthetic content, such as watermarking; [and]
- detecting synthetic content."[97]

***Impact*:** By enforcing watermarking, the production and spread of AI-generated deepfakes and disinformation can be significantly curtailed, enhancing digital media trust and security.

[93] "Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act) (Text with EEA Relevance)," 277 OJ L § (2022), http://data.europa.eu/eli/reg/2022/2065/oj/eng; Brooke Tanner, "EU Code of Practice on Disinformation," Brookings, August 5, 2022, https://www.brookings.edu/articles/eu-code-of-practice-on-disinformation/.

[94] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

[95] Tate Ryan-Mosley and Melissa Heikkila, "Three Things to Know about the White House's Executive Order on AI," MIT Technology Review, October 30, 2023, https://www.technologyreview.com/2023/10/30/1082678/three-things-to-know-about-the-white-houses-executive-order-on-ai/.

[96] "Generative AI on Snapchat," Snapchat Support, 2024, https://help.snapchat.com/hc/en-us/articles/25494876770580-Generative-AI-on-Snapchat.

[97] The White House, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," October 30, 2023, https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/.

Figure 8: AI-generated content on Snapchat includes a Snap Ghost with a sparkles watermark.

Increase measures to protect against economic espionage (IP protection)

Visa Policy Enhancement

The U.S. government can reassess visa policy to more carefully vet PRC nationals who seek to travel to the United States to work or study. PRC nationals are already subjected to extra scrutiny when traveling to the United States, especially if they involve sensitive fields of study, research, or discussion. While the Technology Alert List is comprehensive, and the processing of visa applicants whose work related to those categories must be carefully balanced, and the U.S. government must still balance the need to protect national security and IP with the need to let the U.S. economy grow and the U.S. academic, research, and trade ecosystem flourish.[98] Fine-tuning this system of visa application scrutiny is a policy option to mitigate economic espionage.

Policy options:

1. Reassess visa policy to more carefully vet PRC nationals
2. Companies make decisions independent of U.S. government policy
3. Monitor employee travel more carefully
4. Global Magnitsky Act for IP theft
5. Prioritize work with allies and partners

Figure 9: Policy Options - IP Protections

IP Protection Legislation

Policymakers might also consider some version of a Global Magnitsky Act to counter Chinese IP theft. The Global Magnitsky Act, enacted in April 2016, was created to "impose sanctions

[98] Boston University Global Programs, International Students & Scholars Office, "Technology Alert List, From the U.S. Department of State, August 2022," https://www.bu.edu/isso/files/pdf/tal.pdf

concerning foreign persons responsible for gross violations of internationally recognized human rights, …"[99] The Act has been employed to sanction over 650 foreign government officials responsible for human rights abuses.[100] A similar Congressional act about economic espionage may deter some of the IP theft driven by CCP officials. Just as the decisions around sanctioning foreign officials under the Global Magnitsky Act have been painstaking and thoughtful, naming CCP officials to be sanctioned under a similar act aimed at economic espionage would have to be carefully considered and coordinated across multiple U.S. government agencies.

Line of Effort 3: Engagement and Collaboration

Improve International Cooperation on Cyber Attribution

Enhance international cooperation for global cyber forensics and attribution collaboration to address malign cyber activity. This expanded effort could unite international partners further to improve the speed and accuracy of cyberattack attribution through a dedicated task force that rapidly and accurately identifies cyber threats. The partnership can allow for more focused development and standardization of forensic methodologies and tools that can be employed universally across national boundaries. Additionally, better implementation of Cyber Confidence-Building Measures (CCBMs), which are addressed in the 2022 National Cyber Strategy, can further develop these collaborative relationships through policy exchanges, joint exercises, and continuing to expect the UN's previous work better to define norms for state behavior in cyberspace to enhance transparency and trust with international partners. These measures should include shared strategies for responding to cyber incidents and reinforcing mutual commitments against cyber threats.

International Cooperation to Deter Espionage

In conjunction with efforts to enhance cyber forensic capabilities and threat attribution, engage with allies and partners to develop coordinated responses to economic espionage. This includes using sanctions and other diplomatic measures as deterrence strategies, aiming for a unified stance against intellectual property theft, and securing trade secrets. Such collaboration targets the perpetrators and encourages reconsidering strategies by nations known for IP theft, like China.

Enhanced Cyber Threat Intelligence Sharing

Strengthen intelligence sharing between government and private sectors, supported by legislative measures.

[99] United States Congress, S.284 - Global Magnitsky Human Rights Accountability Act, April 18, 2026, https://www.congress.gov/bill/114th-congress/senate-bill/284/text

[100] The Federal Register, Global Magnitsky Human Rights Accountability Act Annual Report, February 23, 2024, https://www.federalregister.gov/documents/2024/02/23/2024-03532/global-magnitsky-human-rights-accountability-act-annual-report?_gl=1*1do44oa*_gcl_au*MTc5OTUwNDI3Ni4xNzExNDE1NzUy

Case Study 6: Cooperation in Support of Ukraine

The response in support of Ukraine provides a model for how the international community

Participation from the public and private sectors to bolster the cyber defense efforts of an ally or partner

NATO, the EU, and individual nations, like the United States and the United Kingdom, have provided technical assistance, training, and information sharing to help Ukraine strengthen its cyber security

Public-private partnerships also play an important role in Ukraine, with major technology companies, like Google, Microsoft, and Amazon, collaborating with government agencies to share threat information and develop cybersecurity solutions

The case of Ukraine demonstrates the value of engagement and collaboration in the cyber domain

The response in support of Ukraine provides a model for how the international community, with participation from the public and private sectors, can effectively collaborate to bolster the cyber defense efforts of an ally or partner. NATO, the EU, and individual nations, like the United States and the United Kingdom, have provided technical assistance, training, and information sharing to help Ukraine strengthen its cyber security. Public-private partnerships also play a significant role in Ukraine, with major technology companies, like Google, Microsoft, and Amazon, collaborating with government agencies to share threat information and develop cybersecurity solutions. The case of Ukraine demonstrates the value of engagement and collaboration in the cyber domain.[101]

Line of Effort 4: Targeted Actions

Modernization of Critical Infrastructure

Launch a comprehensive federal initiative to subsidize the modernization of national-essential privately owned critical infrastructure. In coordination with ONCD and DHS/CISA, this initiative should support upgrades to legacy OT/IT systems and enhance cyber hygiene practices at locations deemed critical infrastructure with national implications. Funding will be sourced from the remaining 2021 Infrastructure Investment and Jobs Act appropriations, expanded through existing federal grants to state and local governments, FEMA resiliency programs, and Public-private Partnership Models (P3). The modernization will adhere to Secure-By-Design principles with Zero-Trust Architecture (ZTA), prioritizing continuous verification of all network activities and incorporating multi-factor authentication and encryption. Investments will be prioritized based on the infrastructure's national importance and cross-sector implications, guided by the Sector Risk Management Agency's (SRMA) risk assessment and prioritization model.

[101] Emma Schroeder and Sean Dack, "A Parallel Terrain: Public-Private Defense of the Ukrainian Information Environment," *Atlantic Council* (blog), February 27, 2023, https://www.atlanticcouncil.org/in-depth-research-reports/report/a-parallel-terrain-public-private-defense-of-the-ukrainian-information-environment/.

Cyber Compellence. Implement a cyber compellence strategy using a graduated menu of options to effectively deter malicious cyber actors (MCAs) from engaging in harmful activities against the United States. This strategy involves a range of responses that escalate in severity depending on the nature and severity of the cyber threat:

***Direct Cyber Responses*:**

- **Take aggressive action to compel MCAs from engaging in large-scale disinformation campaigns and cyberattacks against the homeland**. The responses can be graduated; however, MCAs should learn to expect more than a sternly worded letter from diplomatic channels. For in-kind responses to low-level cyberattacks, the US can destroy the hard drives of the offenders. Provided an MCA performs periodic back-ups of their data, they will retain their information and capabilities. If not, then they will temporarily lose their ability to attack.

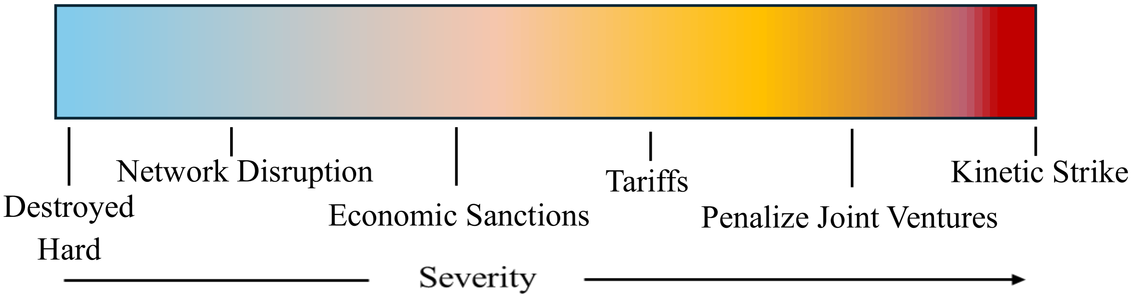


Figure 10: Spectrum of Response Options

- **Next, notify and implement a temporary denial of service on an MCA's internet service provider (ISP).** Commercial buildings and residential neighborhoods are serviced by various ISPs that provide access and maintain the wide-area network. Those networks comprise routers, switches, servers, and firewalls.[102] Each device provides an option to attack that can affect an MCA's access to the internet. The ISP becomes a stakeholder in ensuring its customers are not engaging in illegal cyberspace activities. The ISP likely already has such terms and conditions that customers must agree to, but targeted network degradations by a nation-state further incentivize the desired behavior.

- **The next tier of response options is the use of other national instruments of power.** For example, the US could employ economic responses such as freezing any assets owned by the alleged perpetrators. It could also implement tariffs on goods and services. Additionally, the US could penalize companies that engage in joint ventures with China. There may even be a point where kinetic options are on the table.

[102] "Network Architecture Explained: Understanding the Basics of Modern Networks," Kentipedia, September 11, 2023, https://www.kentik.com/kentipedia/network-architecture/.

The United States needs a broader legal discussion to consider options to compel MCAs to change their behavior.

Advanced Threat Detection Deployment

In response to adversaries utilizing covert LotL tactics that exploit critical infrastructure OT/IT systems, the U.S. government and industry must increase cooperation and focus on adopting advanced detection technologies such as AI/machine learning (ML) models capable of identifying behavioral anomalies in the operation of these systems. This task is complicated by the traditional separation of OT and IT functions and expertise within the industry. To effectively implement these advanced detection technologies, substantial federal investment is necessary to develop these capabilities, train the workforce, and establish ethical and operational guidelines.

Cyber Response Teams (Government and Private Partnerships)

Enhance and expand national and state-level cyber response capabilities through a partnership model involving the National Guard (NG), DHS/CISA, and private sector stakeholders. This initiative aims to bolster U.S. cyber protection forces, enabling more frequent and thorough cybersecurity assessments of critical infrastructures deemed national priorities. Despite existing deployments of NG cyber units in various states, the full potential of this model remains underutilized.[103] Alongside NG enhancements, DHS/CISA should lead the development of sector-specific cyber response teams comprised of industry experts. These teams would work with federal, state, and NG elements to provide localized/regional responses to cyber incidents at private industry locations to augment CISA, which remains under-resourced, ensuring that critical infrastructures receive the necessary support and expertise during threats and recoveries. This integrated approach fortifies the defensive posture of critical infrastructure and builds a resilient framework for public-private collaboration in national cybersecurity efforts.

Comprehensive Cyber Resilience Exercises

Regularly conduct exercises with key public-private sector stakeholders to test and refine disaster response strategies and promote public awareness campaigns focusing on cybersecurity and resilience. Operational plans and wargames must address cyber-attacks. Planners must not white card cyber actions, should select realistic, challenging scenarios, and display capabilities to deter kinetic warfare. There must be integrated deterrence with allies and partners, shared responsibility across the interagency.

Conclusion

Strengthening U.S. cyber capabilities against increasingly sophisticated adversaries leveraging emerging technologies demands a comprehensive, whole-of-society approach. This approach must integrate awareness, education, engagement, collaboration, regulation, governance, and targeted action. Immediate, coordinated efforts are needed to bolster national security, protect democratic

[103] Pomerleau, Mark, Lawmakers Pushing for More Integration of National Guard Reserve Personnel into DoD Cyber Forces." *DefenseScoop*, June 12, 2023. https://defensescoop.com/2023/06/12/lawmakers-pushing-for-more-integration-of-national-guard-reserve-personnel-into-dod-cyber-forces/.

institutions, and maintain U.S. global leadership. Drawing from successful international models, the U.S. must enhance digital literacy, sensibly regulate social media platforms, modernize critical infrastructure, and expand offensive cyber capabilities. The United States can fortify its defenses by uniting government, industry, academia, allies, and citizens to ensure resiliency and a secure, stable, democratic future.