Resilience for a Digital Age

Danielle Keats Citron[†] *& Kristen E. Eichensehr*[††]

ABSTRACT

A resilience agenda is an essential part of protecting national security in a digital age. Digital technologies impact nearly all aspects of everyday life, from communications and medical care to electricity and government services. Societal reliance on digital tools should be paired with efforts to secure societal resilience. A resilience agenda involves preparing for, adapting to, withstanding, and recovering from disruptions in ways that advance societal interests, goals, and values. Emphasizing resilience offers several benefits: 1) Resilience is threat agnostic or at least relatively threat neutral; 2) its inward focus emphasizes actions under the control of a targeted country, rather than attempting to change behaviors of external adversaries; and 3) because resilience can address multiple threats simultaneously, it may be less subject to politicization. A resilience strategy is well-suited to address both disruptions to computer systems—whether from cyberattacks or natural disasters—and disruptions to the information environment from disinformation campaigns sowing discord. A resilience agenda is realistic, not defeatist, and fundamentally optimistic in its focus on how society can withstand and move forward from adverse events.

This Article identifies tactics to bolster resilience against digitally enabled threats across three temporal phases: anticipating and preparing for disruptions, adapting to and withstanding disruptions, and recovering from disruptions. The tactics of a resilience strategy across these phases are dynamic and interconnected. Resilience tactics in the preparation phase could include creating redundancies (including low-tech or no-tech redundancies) or "pre-bunking" disinformation campaigns. Actions in the preparation phase help with adapting to and withstanding disruptions when they are ongoing. Forewarning people about cyberattacks can

[†] Jefferson Scholars Foundation Schenck Distinguished Professor in Law, University of Virginia School of Law; Vice President, Cyber Civil Rights Initiative; 2019 MacArthur Fellow.

[††] David H. Ibbeken '71 Research Professor of Law, University of Virginia School of Law; Samuel Willison Visiting Professor of Law, Harvard Law School (2024-25). For helpful comments and conversations, we thank Ryan Calo, Louis Citron, Woodrow Hartzog, Spencer Overton, Richard Re, Shirin Sinnar, Ari Waldman, and John Woods. We are also grateful to participants in *The University of Chicago Legal Forum*'s Symposium on "Reimagining National Security," the Multi-Racial Democracy and AI Panel at the American Association of Law Schools meeting, the University of Pittsburgh's seminar series on the Future of Law in Technology and Governance, and the 7th Annual North American Environment, Energy, and Natural Resources Conference at the University of Houston Law Center, where Eichensehr's keynote address explored some of the points in this piece. For excellent research assistance, we thank Samantha Blond, Alexander Chen, Toluwani Ojuola, and librarian extraordinaire Kate Boudouris, and thanks to the editors of *The University of Chicago Legal Forum* for great suggestions and careful editing.

ensure they do not panic when crucial services cease to function. More persistent and recurrent threats like disinformation campaigns may require structural adaptations, like privacy law reform, to curb the exploitation of personal data that can be used for democracy-damaging disinformation. Recovering from disruptions draws on steps taken earlier. Resilience tactics in the recovery phase could include reverting to manual controls and turning to pre-positioned hardware stockpiles that enable continuity of operations after cyberattacks, as well as supporting and protecting journalists and researchers subjected to intimidating online abuse. These are just possibilities—a resilience strategy is ours to imagine and pursue, and doing so is a crucial step to strengthen national security for a digital age.

I. INTRODUCTION

Electricity, water services, transportation, social media, and countless other daily activities depend upon, or are connected to, networked technologies.[1] Digital tools shape relationships, democratic institutions, and individual well-being.[2] It is difficult to imagine life in the 21st century without digital technologies.

At the same time, our digital dependence poses vulnerabilities that must be addressed,[3] including ones that implicate national security. Consider these pressing national security concerns. Cyberattacks can stop society in its tracks. State-sponsored hackers have crippled computer systems essential for medical care, electricity, and shipping operations.[4] In July 2024, a flawed update to a product used to protect

[1] *See, e.g.*, THOMAS P. KEENAN, TECHNOCREEP: THE SURRENDER OF PRIVACY AND THE CAPITALIZATION OF INTIMACY 1–18 (2014); Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1 (2004) (exploring the significance of digital technologies on affordances for free speech); Matt Burgess, *The Dangerous Rise of GPS Attacks*, WIRED (Apr. 30, 2024), https://www.wired.com/story/the-dangerous-rise-of-gps-attacks/ [https://perma.cc/6BNH-QCNB] (detailing the effects of GPS jamming and spoofing on aviation and shipping); *Water and Wastewater Cybersecurity*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, https://www.cisa.gov/water [https://perma.cc/WM3F-N64H] ("The Water and Wastewater Sector depends on the digital world . . . ."); WHITE HOUSE, U.S. NATIONAL CYBER STRATEGY 2 (Mar. 2023), https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/8FHY-H99H] ("[F]actories, power grids, and water treatment facilities, among other essential infrastructure, are increasingly shedding old analog control systems and rapidly bringing online digital operational technology . . . .").

[2] *See generally* SIVA VAIDHYANATHAN, THE GOOGLIZATION OF EVERYTHING (AND WHY WE SHOULD WORRY) (2012). This has been true for all transformative technologies. *See* LANGDON WINNER, THE WHALE AND THE REACTOR (1986) (exploring the role of technologies in transforming social and political affordances and altering political and moral meaning).

[3] *See, e.g.*, NICHOLAS CARR, THE GLASS CAGE: AUTOMATION AND US (2014); Linda J. Skitka et al., *Automation Bias and Errors: Are Crews Better Than Individuals?*, 10 INT'L J. AVIATION PSYCH. 85, 86 (2000) (explaining that over-reliance on automated aviation systems could corrode pilots' failsafe skills); Daniel Herman, *The End of High-School English*, ATLANTIC (Dec. 9, 2022), https://www.theatlantic.com/technology/archive/2022/12/openai-chatgpt-writing-high-school-english-essay/672412/ [https://perma.cc/XY7H-4F8K] (warning that widespread adoption of ChatGPT could undermine writing skills).

[4] *See* Dan Bilefsky, *Britain Says North Korea Was Behind Cyberattack on Health Service*, N.Y. TIMES (Oct. 27, 2017), https://www.nytimes.com/2017/10/27/world/europe/uk-ransomware-

against such attacks itself caused a "national digital meltdown," notably crippling flights nationwide.[5]

Add to these risks the fact that states are increasingly using online disinformation to exacerbate political discord.[6] Foreign governments have targeted the United States with disinformation campaigns on social media, including using "A.I. tools" to sow unrest in the United States.[7] For example, in the wake of devastating fires in Maui, Hawaii, China launched a disinformation campaign on social media asserting that "[t]he disaster was not natural . . . but was the result of a secret 'weather weapon' being tested by the United States."[8] To bolster the plausibility of this claim, posts included photographs seemingly generated by "artificial intelligence programs, making them among the first to use these new tools to bolster the aura of authenticity of a disinformation campaign."[9] Russia has used similar tactics. In the midst of the 2024 election season, the U.S. Department of Justice accused the Russian government of "malign influence efforts targeting the 2024 U.S. presidential election," including the use of "'AI-generated false narratives on social media.'"[10]

In this challenging era, societal reliance on digital technologies should be paired with a societal resilience strategy. Resilience has wide-ranging meanings and applications.[11] In the cybersecurity context, the

hack-north-korea.html [https://perma.cc/J6KG-NZSS] (discussing North Korea's WannaCry ransomware operation that affected Britain's National Health Service); Andy Greenberg, *Sandworm Hackers Caused Another Blackout in Ukraine—During a Missile Strike*, WIRED (Nov. 9, 2023), https://www.wired.com/story/sandworm-ukraine-third-blackout-cyberattack/ [https://perma.cc/36SG-H7ZU] (discussing Russian government hackers' history of causing electricity blackouts in Ukraine); Andy Greenberg, *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*, WIRED (Aug. 22, 2018), https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [https://perma.cc/LK6F-FLA8] (discussing the effect of Russia's NotPetya cyber operation on the Maersk shipping company).

[5] David E. Sanger, *What Happened to Digital Resilience?*, N.Y. TIMES (July 19, 2024), https://www.nytimes.com/2024/07/19/us/politics/crowdstrike-outage.html [https://perma.cc/K3QD-CSFT] (describing the aftermath of a flawed update to Crowdstrike software).

[6] *See, e.g.*, *Combating Foreign Influence*, FBI, https://www.fbi.gov/investigate/counterintelligence/foreign-influence [https://perma.cc/Z6F8-UWHX] (explaining that the FBI investigates foreign influence operations that "spread disinformation, sow discord, and, ultimately, undermine confidence in democratic institutions and values," often by "us[ing] false personas and fabricated stories on social media to discredit U.S. individuals and institutions").

[7] David E. Sanger & Steven Lee Myers, *China Sows Disinformation About Hawaii Fires Using New Techniques*, N.Y. TIMES (Sept. 11, 2023), https://www.nytimes.com/2023/09/11/us/politics/china-disinformation-ai.html [https://perma.cc/QXL7-DENN].

[8] *Id.*

[9] *Id.*

[10] Press Release, U.S. Dep't of Justice, Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere (Sept. 4, 2024), https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence [https://perma.cc/WMB6-KCLJ] (quoting Deputy Attorney General Lisa Monaco).

[11] *See infra* Part II.A.

National Institute of Standards and Technology (NIST) describes "cyber resiliency" as "[t]he ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[12] Resilience has also been invoked to refer to the capacity to ignore and disregard disinformation.[13]

This Article explores the descriptive meaning and normative significance of resilience for the protection of national security against digitally-enabled threats. Government officials, commentators, and others have been invoking the idea of resilience with increasing frequency, but with insufficient explanation of its theoretical grounding. We hope to change that, and to start a discussion, for us, about the role that law, markets, and social norms could play in fostering resilience.

Foregrounding resilience as a national security strategy offers several benefits. First, resilience strategies are relatively threat-neutral or threat-agnostic, enabling them to tackle varied threats and threat actors. Second, bolstering resilience is internally focused, and thus implementation is easier than classic deterrence strategies that rely on changing the behavior of external actors. Because a resilience agenda looks inward, it is ours to imagine and design. It enables us to articulate the interests, goals, and commitments our society believes deserve reinforcement. Third, in an era of deep political divisions about nearly everything, including the nature, magnitude, and even existence of some national security threats, focusing on resilience may provide a way to decrease polarization with respect to investing in and improving our security posture.

If ensuring resilience is a crucial national security goal, then how can it be pursued? This Article identifies essential components of a resilience strategy, focusing on the ability to anticipate and prevent disruptions, to adapt to and withstand harm, and to recover from shocks, all in line with clearly articulated societal interests, goals, and values. The remainder of this Article proceeds as follows. Part II describes the recent expansion in conceptions of national security and the ways in which digital dependence exacerbates security risks. Part III defines resilience and explains the advantages for national security of focusing on resilience as a complement to other strategies like deterrence. Part IV highlights various tactics that would help operationalize a resilience strategy for the good of national security. Part V concludes by offering cautions about what a focus on resilience should *not* entail.

[12] *Cyber Resiliency*, NAT'L INST. STANDARDS & TECH., COMPUT. SEC. RES. CTR., https://csrc.nist.gov/glossary/term/cyber_resiliency [https://perma.cc/CB9Y-7JVR].

[13] Edda Humprecht et al., *The Sharing of Disinformation in Cross-National Comparison: Analyzing Patterns of Resilience*, 26 INFO., COMMC'N & SOC'Y 1342, 1344–45 (2023).

II. THE NEW AGE OF NATIONAL SECURITY THREATS AND DIGITAL DEPENDENCIES

The past few years have witnessed a reframing in how the U.S. government conceptualizes national security.[14] Consider the 2024 *Annual Threat Assessment of the U.S. Intelligence Community*.[15] This document, prepared by the Office of the Director of National Intelligence, included sections on China, Russia, Iran, North Korea, and "Global Terrorism."[16] But it also addressed "environmental change and extreme weather"; "health security"; "disruptive technology"; and "digital authoritarianism and transnational repression."[17] The list of threats placed under the umbrella of national security is long and growing.

Many national security threats can be tied, at least in part, to the growing dependence on digital technologies. In some cases, digital technologies enable threats; in others, they exacerbate vulnerabilities. In still others, disinformation campaigns and dependence on social media more generally can deepen societal divisions and make it more difficult to reach agreement on how to address other problems.[18]

The national security complications caused by digital dependence manifest at the national, enterprise, and individual levels, with frequent crossovers between them. Consider some of the technology-related risks facing public and private institutions. Storing data electronically means that espionage can lead to the exfiltration of vast quantities of information from public and private sector databases.[19] The hack of the U.S. Office of Personnel Management resulted in the compromise of more than 22 million individuals' records,[20] and the 2017

[14] *See, e.g.*, Kristen E. Eichensehr & Cathy Hwang, Essay, *National Security Creep in Corporate Transactions*, 123 COLUM. L. REV. 549, 556–60 (2023) (discussing how the concept of national security has expanded in recent years).

[15] OFF. OF THE DIR. OF NAT'L INTELL., ANNUAL THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY (Feb. 5, 2024).

[16] *Id.* at 7–23, 38–39.

[17] *Id.* at 30–31, 33–34 (capitalization omitted).

[18] Disinformation campaigns can be so successful that people reject "the knowability of information altogether." Stephan Lewandowsky & Sander van der Linden, *Countering Misinformation and Fake News Through Inoculation and Prebunking*, 32 EURO. REV. SOC. PSYCH. 348, 353 (2021); *see also* Bobby Chesney & Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1778–79 (2019) (exploring how well-timed deep fake video or audio of political candidates on the eve of an election could change election outcomes). Robert Chesney and one of us (Citron) have described the weaponization of decrying actual truths as the "Liar's Dividend." Chesney & Citron, *supra*, at 1785.

[19] *See, e.g.*, Dustin Volz, *More SolarWinds Hack Victims Yet to be Publicly Identified, Tech Executives Say*, WALL ST. J. (Feb. 23, 2021, 7:50 PM), https://www.wsj.com/articles/senate-panel-probes-solarwinds-hack-to-learn-how-big-how-broad-hit-was-11614086918 [https://perma.cc/U33R-YUX7] (discussing the broad scope of the hacking enabled by the compromise of SolarWinds).

[20] Ellen Nakashima, *Hacks of OPM Databases Compromised 22.1 Million People, Federal*

breach of Equifax, a credit reporting company, compromised the records of 147.9 million U.S. citizens.[21] In addition, dependence on digital records and networked systems has left businesses vulnerable to ransomware attacks, including ones that have impacted medical care.[22] A ransomware attack on Colonial Pipeline in 2021 led to a days-long shutdown of a major pipeline along the U.S. East Coast, causing "panic buying" at gas stations.[23] Moreover, the widespread adoption of social media has made public discourse vulnerable to malign foreign information operations.[24] The 2024 *Annual Threat Assessment* warned in particular that foreign states are "growing more sophisticated in digital influence operations that try to affect foreign publics' views, sway voters' perspectives, shift policies, and create social and political upheaval."[25]

Other threats target individuals.[26] So long as there have been networked communications, there has been cyber harassment, which has disproportionately impacted women and minorities.[27] Female politicians have been harassed by cyber mobs that discredit and terrorize them.[28] Journalists have faced a storm of destructive abuse.[29] For

Authorities Say, WASH. POST (July 9, 2015, 8:33 PM), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/ [https://perma.cc/DG5M-GTBM].

[21] Brian Barrett, *How 4 Chinese Hackers Allegedly Took Down Equifax*, WIRED (Feb. 10, 2020, 12:52 PM), https://www.wired.com/story/equifax-hack-china/ [https://perma.cc/S9KY-VSSG].

[22] *See, e.g.*, Rebecca Carballo, *Ransomware Attack Disrupts Health Care Services in at Least Three States*, N.Y. TIMES (Aug. 5, 2023), https://www.nytimes.com/2023/08/05/us/cyberattack-hospitals-california.html [https://perma.cc/AK84-LVHC].

[23] *See, e.g.*, Michael D. Shear et al., *Colonial Pipeline Paid Roughly $5 Million in Ransom to Hackers*, N.Y. TIMES (June 7, 2021), https://www.nytimes.com/2021/05/13/us/politics/biden-colonial-pipeline-ransomware.html [https://perma.cc/HW6J-TDG3].

[24] *See, e.g.*, MAREK N. POSARD ET AL., FROM CONSENSUS TO CONFLICT: UNDERSTANDING FOREIGN MEASURES TARGETING U.S. ELECTIONS, RAND CORP. RESEARCH REPORT (2020), https://www.rand.org/pubs/research_reports/RRA704-1.html [https://perma.cc/ETM2-7Y3T]; U.S. DEP'T OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 14–35, https://www.documentcloud.org/documents/5955118-The-Mueller-Report [https://perma.cc/83K8-UNFP] (detailing "Russian 'Active Measures' Social Media Campaign" conducted primarily by the Internet Research Agency).

[25] OFF. OF THE DIR. OF NAT'L INTEL., *supra* note 15, at 31 (emphasis omitted).

[26] *Id.* ("Foreign states are advancing digital and physical means to repress individual critics and diaspora communities abroad, including in the United States . . . ."); *see also* SARAH SOBIERAJ, CREDIBLE THREAT: ATTACKS AGAINST WOMEN ONLINE AND THE FUTURE OF DEMOCRACY (2020).

[27] DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE 13–15 (2014); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 85 (2009).

[28] NINA JANKOWICZ ET AL., MALIGN CREATIVITY: HOW GENDER, SEX, AND LIES ARE WEAPONIZED AGAINST WOMEN ONLINE, WILSON CENTER (Jan. 2021) (studying online abuse involving gendered and sexualized disinformation targeting ten U.S. female politicians).

[29] MICHELLE FERRIER, ATTACKS AND HARASSMENT: THE IMPACT ON FEMALE JOURNALISTS AND THEIR REPORTING (Sept. 2018), https://www.iwmf.org/wp-content/uploads/2018/09/Attacks-and-Harassment.pdf [https://perma.cc/R27Q-CQCX]; ANTI-DEFAMATION LEAGUE'S TASK FORCE ON HARASSMENT AND JOURNALISM, ANTI-SEMITIC TARGETING OF JOURNALISTS DURING THE 2016 PRESIDENTIAL CAMPAIGN (Oct. 19, 2016), https://www.adl.org/sites/default/files/documents/assets/

example, after profiling Melania Trump in *GQ* magazine in 2016, Julia Ioffe received a tsunami of antisemitic and misogynistic threats for her allegedly unfavorable coverage.[30] In the lead up to the 2020 U.S. presidential election, ***Russia Today*** (*RT*) attacked *New York Times* journalist Nicole Perlroth after she tweeted about "the Russian Internet Research Agency's well-documented strategy of targeting Black voters in an attempt to suppress Black turnout in the 2016 election."[31] *RT*'s articles described Perlroth as racist and stupid, sparking abuse on Twitter and fringe American outlets.[32] The online attacks impacted Perlroth's mental health and relationships.[33] She noted, "there's no clear way to respond to it, except silence."[34]

These are not isolated examples. Cyber harassment is a weapon of choice for authoritarian regimes to target critics. Pro-Kremlin trolls relentlessly attacked Finnish journalist Jessikka Aro after she began investigating the Russian Internet Research Agency's online influence campaigns.[35] Serbian political analyst Jelena Milić, who studies Russian influence operations in the Balkans, faced continuous online abuse.[36] Anonymous posters called her "'a whore paid by NATO'" and fantasized about her death.[37] Her employer received messages accusing Milić of being a criminal, and its website crashed after multiple distributed denial-of-service attacks.[38] Indian journalist Rana Ayyub was targeted with a deepfake sex video after she appeared on BBC and criticized the Modi regime's human rights abuses of the minority Muslim community (to which she belongs).[39] For months, Ayyub faced misogynistic and anti-Muslim abuse, including rape and death threats, doxing, and texts asking for her rates for sex.[40] Although these incidents

pdf/press-center/CR_4862_Journalism-Task-Force_v2.pdf [https://perma.cc/F5GP-DXDH].

[30] Lauren Gambino, *Journalist Who Profiled Melania Trump Hit with Barrage of Antisemitic Abuse*, GUARDIAN (Apr. 28, 2016, 9:57 PM), https://www.theguardian.com/us-news/2016/apr/28/julia-ioffe-journalist-melania-trump-antisemitic-abuse [https://perma.cc/QSA7-22AD].

[31] JANKOWICZ ET AL., *supra* note 28, at 34.

[32] *Id.* at 34–37.

[33] *Id.*

[34] *Id.* at 41.

[35] JESSIKKA ARO, PUTIN'S TROLLS: ON THE FRONTLINES OF RUSSIA'S INFORMATION WAR AGAINST THE WORLD 9–21, 81, 185–89 (2022) (explaining the pro-Kremlin cyber campaign against her that included, among other tactics, a phone call with the sound of gun fire, online smears accusing her of being "a NATO lobbyist," and Facebook comments fantasizing about raping her).

[36] *Id.* at 195–98.

[37] *Id.* at 195–96.

[38] *Id.* at 197–98.

[39] Rana Ayyub, Opinion, *In India, Journalists Face Slut-Shaming and Rape Threats*, N.Y. TIMES (May 22, 2018), https://www.nytimes.com/2018/05/22/opinion/india-journalists-slut-shaming-rape.html [https://perma.cc/G644-U7HK].

[40] *See id.*; *Rana Ayyub: Misinformation Threatens to be the New 'True Information'*, NOBEL PEACE PRIZE BLOG (May 2023), https://www.nobelprize.org/rana-ayyub-misinformation-threatens-

targeted individual journalists, they have had broader societal and security implications. Digital tools allow targeting across borders and at scale, and online harassment silences journalists, public figures, and other critics, thereby reshaping the digital public sphere and the information available there.

Digital technologies enable and exacerbate vulnerabilities for governments, companies, communities, and individuals, posing risks for national security. Now to discuss what resilience offers to protect national security in a digital age.

III. RESILIENCE AS A STRATEGIC IMPERATIVE

In the face of national security threats tied to digital technologies, U.S. government officials are increasingly calling for resilience strategies. In a blog post in August 2023, Jen Easterly, Director of the Cybersecurity and Infrastructure Security Agency (CISA), wrote with a Ukrainian cybersecurity official about "The Power of Resilience" and lessons the United States can learn from Ukraine.[41] They said that the United States must "take a page out of Ukraine's cyber playbook and build its resiliency now."[42] In a March 2024 speech, Federal Trade Commission Chair Lina Khan bluntly declared that "we have a resiliency problem in America," citing cybersecurity and defense industry examples in arguing against consolidation of companies and in favor of competition.[43] The Biden administration's National Cybersecurity Strategy, mentions "resilience," "resiliency," or "resilient" sixty-eight times.[44] But what does resilience mean and what does it add?

to-be-the-new-true-information/ [https://perma.cc/KUD6-WRVC]; DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY: PROTECTING DIGNITY, IDENTITY, AND LOVE IN THE DIGITAL AGE 56 (2022) (discussing interviews with Ayyub about her experience facing online abuse spearheaded by the Modi regime to stop her from writing).

[41] Jen Easterly & Victor Zhora, *The Power of Resilience: What America Can Learn from Our Partners in Ukraine*, CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY (Aug. 9, 2023), https://www.cisa.gov/news-events/news/power-resilience [https://perma.cc/YF4Z-XWPH].

[42] *Id.*

[43] U.S. Fed. Trade Comm'n, Remarks by Chair Lina M. Khan as Prepared for Delivery, Carnegie Endowment for Int'l Peace 2–3 (Mar. 13, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2024.03.13-chair-khan-remarks-at-the-carnegie-endowment-for-intl-peace.pdf [https://perma.cc/P4M5-KZZ4].

[44] WHITE HOUSE, *supra* note 1; *see also* WHITE HOUSE, FACT SHEET; BIDEN-HARRIS ADMINISTRATION ANNOUNCES NEW NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE (Apr. 30, 2024), https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/30/fact-sheet-biden-harris-administration-announces-new-national-security-memorandum-on-critical-infrastructure/ [https://perma.cc/9V7Z-ENSW] ("Resilience, particularly for our most sensitive assets and systems, is the cornerstone of homeland defense and security."); PRESIDENT'S COUNCIL OF ADVISORS ON SCI. AND TECH., REPORT TO THE PRESIDENT: STRATEGY FOR CYBER-PHYSICAL RESILIENCE: FORTIFYING OUR CRITICAL INFRASTRUCTURE FOR A DIGITAL WORLD (2024), https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf [https://perma.cc/MTG3-U2HY] [hereinafter PCAST Report]

This Part aims to put descriptive and theoretical meat on the bones of these invocations of resilience. It defines the concept of resilience, drawing on sociology, engineering, and human rights literature, and it then identifies several benefits that a resilience strategy offers.[45]

A. What Resilience Means

Resilience is a wide-ranging concept. In its broadest sense, resilience captures the ability of "people, communities, corporations, and countries . . . to absorb and adapt to changes."[46] Addressing threats to critical infrastructure, the Obama administration's Presidential Policy Directive 21 (PPD-21) in 2013 defined "resilience" as "the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions" including "deliberate attacks, accidents, or naturally occurring threats or incidents."[47] Its 2024 replacement, National Security Memorandum 22 (NSM-22), similarly defines "resilience" as "the ability to prepare for threats and hazards, adapt to changing conditions, and withstand and recover rapidly from adverse conditions and disruptions."[48]

(offering concrete recommendations for improving the resilience of cyber-physical systems).

[45] To be sure, we are not the first to discuss resilience and technological challenges. *See, e.g.*, Derek E. Bambauer, *Ghost in the Network*, 162 U. PA. L. REV. 1011 (2014) (drawing on "normal accident theory" to argue for focusing on mitigating the effects of cyberoperations and identifying disaggregation of data and heterogeneity of software and hardware as resilience strategies that governments should employ in key industries); Gary E. Marchant & Yvonne A. Stevens, *Resilience: A New Tool in the Risk Governance Toolbox for Emerging Technologies*, 51 U.C. DAVIS L. REV. 233 (2017) (discussing the role of resilience in governing emerging technologies, particularly consumer products). We add to the existing literature, however, a broader frame. We consider resilience as not just a technological issue, but rather a societal one. We draw insight from scholarly discussions related to specific contexts and concerns and then widen the aperture to a whole of national security approach. *See infra* notes 53–58 and accompanying text discussing insights from specific fields like systems design, safety engineering, and human rights.

[46] Anthea Roberts, *From Risk to Resilience: How Economies Can Thrive in a World of Threats*, 102 FOREIGN AFFAIRS 123, 127 (2023); *see also* THE NATIONAL ACADEMIES, DISASTER RESILIENCE: A NATIONAL IMPERATIVE 1 (2012), https://nap.nationalacademies.org/read/13457/chapter/2 [https://perma.cc/W8B9-3K9Z] ("[R]esilience is the ability to prepare and plan for, absorb, recover from, and more successfully adapt to adverse events" (emphasis omitted)); Timothy Malloy, *Re-Imagining Risk: The Role of Resilience and Prevention*, 22 NEV. L.J. 145, 177–78 (2021) (collecting "leading definitions" of "resilience" from a variety of contexts).

[47] WHITE HOUSE, PPD-21, CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [https://perma.cc/5Q4G-32FT].

[48] WHITE HOUSE, NSM-22, NATIONAL SECURITY MEMORANDUM ON CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE (Apr. 30, 2024), https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/ [https://perma.cc/64DX-TGRZ]. The Memorandum defines "all threats, all hazards" broadly to include "a threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of Government, social, or economic activities," including but "not limited to: natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, supply chain disruptions to degrade critical infrastructure, and disruptive or destructive activity targeting critical

Scholars have understood resilience as the "capacity of a system to deal with harm" and "a strategy to ensure a 'soft landing' after a significant external shock or disruption causes damage."[49] On this view, "resilience strategies seek to minimize the severity or duration of unanticipated harm once an adverse event or outcome has occurred."[50]

Definitions of *cyber* resilience focus more specifically on withstanding harms to computer systems. For example, according to the U.S. Pacific Northwest National Laboratory, "cyber resilience" concerns the "ability to weather adverse events in a computing environment."[51] Companies have similarly described cyber resilience as requiring "proactively manag[ing] risks, threats, vulnerabilities and the effects on critical information and supporting assets."[52]

These explanations are an important start. But our societal commitments and ambitions should be in the foreground of understanding resilience. A resilience agenda should be shaped by a clear understanding of the interests, goals, and values at stake. What should be protected from harm, and what counts as disruption or harm? Definitions of resilience have embedded within them value questions that often fly under the radar.

One can, however, find some definitions of resilience that are more explicit about societal interests, goals, and values. For instance, the engineering system-design literature understands resilience as the "capacity of a system to absorb disturbance," to adapt and transform to "retain essentially the same function, structure, [and] identity," and to *ensure that stakeholders' "values, aspirations, and goals" are met.*[53] Societal commitments are also in the foreground of definitions of "information resilience." Human rights advocates describe information resilience as "fortifying the truth."[54] This includes sharing "trustworthy video of human rights violations that did indeed *happen*."[55] As disinformation expert and Co-Founder and CEO of The American Sunlight Project Nina Jankowicz has explained, information resilience involves

infrastructure." *Id.*

[49] Marchant & Stevens, *supra* note 45, at 247.

[50] *Id.* at 248.

[51] *Cyber Resilience*, PAC. NW. NAT'L LAB'Y, https://www.pnnl.gov/explainer-articles/cyber-resilience [https://perma.cc/WSL5-NUAT].

[52] *What Is Cyber Resilience?*, IBM, https://www.ibm.com/topics/cyber-resilience [https://perma.cc/V7SC-79WT].

[53] DAVID G. HENDRY & BATYA FRIEDMAN, RESILIENCE GRAMMAR: A VALUE SENSITIVE DESIGN METHOD FOR RESILIENCE THINKING 4, 6 (2023) (emphasis added), https://digitalcommons.law.uw.edu/techlab/21/ [https://perma.cc/9WEW-RJ45].

[54] Sam Gregory, *Fortify the Truth: How to Defend Human Rights in an Age of Deepfakes and Generative AI*, 15 J. HUM. RTS. PRAC. 702, 703 (2023).

[55] *Id.* (emphasis in original); *see also* Humprecht, *supra* note 13, at 1344 (defining resilience as disregarding and ignoring disinformation).

ensuring that: (1) truthful information can compete with disinformation, (2) algorithms amplify authentic images, knowledge, and truthful information, and (3) women and minorities can live, work, and express themselves free from online abuse.[56]

Employing the notion of resilience in the national security arena embeds values implicitly, and those invoking resilience should, we think, be more explicit going forward about these embedded values. In articulating the values and interests that resilience protects, a resilience agenda should center on institutional behavior more so than individual action. We have seen the failure of policies that lean too heavily on individuals, such as the notice-and-choice regime that has failed to protect privacy in the United States.[57] In the safety-engineering literature, critics have raised concerns that resilience efforts could put too much responsibility on the allegedly autonomous "resilient *subject*" (in that context, the individual worker).[58] While a resilience strategy necessarily involves individuals, it should focus primarily on governmental, corporate, and other institutions to preserve, reinvent, and protect societal goals, interests, and values from disruption. We will return to this concern in Part V, but the next section addresses the advantages of focusing on resilience.

B. What Resilience Adds

Focusing on resilience as a national security imperative has three main advantages: resilience strategies are threat-neutral or at least relatively threat-agnostic; bolstering resilience is an inwardly focused strategy that does not depend on changing the behavior of external threat actors; and focusing on resilience may decrease politicization or polarization with respect to improving national security. We address each in turn.

1. Threat neutrality

First to the notion that specific threats do not drive a resilience agenda. Tactics that strengthen an institution's resilience against one kind of threat can cross-apply to other kinds of threats. Consider an

[56] Zoom Interview with Nina Jankowicz, Co-Founder and CEO, American Sunlight Project (Dec. 13, 2023) (notes on file with authors). *See generally* NINA JANKOWICZ, HOW TO LOSE THE INFORMATION WAR: RUSSIA, FAKE NEWS, AND THE FUTURE OF CONFLICT (2020); NINA JANKOWICZ, HOW TO BE A WOMAN ONLINE: SURVIVING ABUSE AND HARASSMENT AND HOW TO FIGHT BACK (2022).

[57] *See generally* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880 (2013).

[58] Erik Mygind du Plessis & Bjarne Vandeskog, *Other Stories of Resilient Safety Management in the Norwegian Offshore Sector: Resilience Engineering, Bullshit and the De-Politicization of Danger*, 36 SCANDINAVIAN J. MNGMT. 1, 9 (2020) (emphasis added).

example. Just before Russia's full-scale invasion of Ukraine in February 2022, Ukraine's parliament amended existing data protection laws to allow critical data to be stored in the cloud.[59] With the help of major Western companies, the Ukrainian government quickly moved crucial government databases into the cloud and out of the country.[60] Backup copies of governmental information now reside in servers located in friendly countries, notably Poland.[61] Russian attacks on sites storing data in Ukraine have not destroyed the Ukrainian government's functionality because the country secured another way to access crucial information.[62] To be sure, that resiliency tactic responded to a very particular physical and cyber threat from Russia. But more generally, the tactic of creating cloud backups of critical governmental data in different physical locations creates resilience that protects against disruption from a whole variety of threats, from fires and floods to armed conflict and cyberattacks.[63]

Resilience strategies also protect against the same or similar threats from *different* actors. In other words, they can be attribution-neutral: resilience measures that allow institutions to recover quickly from intrusions by states will also allow them to recover quickly from intrusions by non-state actors.[64] The same is true for efforts to ensure the integrity of democratic discourse and free speech values. Tactics designed to promote truthful information and to de-amplify disinformation apply to governments trying to sow discord *and* to private actors seeking attention that generates advertising income.[65]

[59] MICROSOFT, DEFENDING UKRAINE: EARLY LESSONS FROM THE CYBER WAR 5 (June 22, 2022), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK [https://perma.cc/5TFS-HW5A].

[60] *Id.* (describing the effort as one to "'evacuate' critical government data outside the country and into data centers across Europe"); *see also Safeguarding Ukraine's Data to Preserve Its Present and Build Its Future*, AMAZON (Apr. 14, 2023), https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-and-build-its-future [https://perma.cc/9HCU-VPD8] (describing Amazon's role in migrating Ukrainian government and private sector data to the cloud).

[61] Catherine Stupp, *Ukraine Has Begun Moving Sensitive Data Outside Its Borders*, WALL ST. J. (June 14, 2022, 5:30 AM), https://www.wsj.com/articles/ukraine-has-begun-moving-sensitive-data-outside-its-borders-11655199002 [https://perma.cc/LS5N-PS7D].

[62] *Id.*

[63] *Cf.* MICROSOFT, *supra* note 59, at 5 (explaining that "[o]ne reason" Russian "kinetic and cyberattacks [against Ukraine] have had limited operational impact is because digital operations and data have been disbursed into the public cloud").

[64] *Cf.* Joseph S. Nye, Jr., *Deterrence in Cyberspace*, PROJECT SYNDICATE (June 3, 2019), https://www.project-syndicate.org/commentary/deterrence-in-cyberspace-persistent-engagement-by-joseph-s-nye-2019-06 [https://perma.cc/WB2M-P5EH] ("[W]hile attribution is crucial for punishment, it is not important for deterrence by denial or entanglement.").

[65] *See* Claire Atkin, *Are Your Ads Funding Disinformation?*, HARV. BUS. REV. (Aug. 21, 2023), https://hbr.org/2023/08/are-your-ads-funding-disinformation [https://perma.cc/YDL5-64B3] (describing how brands are contributing to the disinformation economy and how personal data "enables propagandists to develop detailed user profiles that help them target people who are

Moreover, a threat-neutral approach helps to prevent the distorting effect of focusing on specific threats or attackers. Having a particular threat or attacker in mind can skew or narrow resiliency measures. For instance, efforts focused on curtailing the spread of deepfake audio and video might not address cheap fakes or other low-tech distortion of video, audio, and images.[66]

2. Inward focus

The second benefit of focusing on resilience is its inward focus. This differs from traditional deterrence strategies, which aim to change the incentives and behavior of external actors.[67] In traditional discussions of deterrence (sometimes described as deterrence by punishment), deterrence is understood to work because it threatens a tit-for-tat: if State A attacks State B, then State B will respond with equal or greater force, and anticipating that possibility, State A will refrain from attacking in the first place.[68] This deterrence-by-punishment model looks outward and aims to change the behavior of adversaries.[69] Doing so effectively, however, is a tall order. Using threats or promises of consequences to change someone else's decision-making calculus is difficult to calibrate and ultimately may not be possible.

By contrast, efforts to bolster resilience focus on changing the behavior of the governments, entities, and individuals that may be targeted, putting countries and their stakeholders in the driver's seat and in charge of *their own* behavior. A resilience approach asks stakeholders within a country to consider their priorities, goals, and values and to ask themselves what institutions, activities, and entities need adapting, backing up, or shoring up (and which do not). For instance,

susceptible to lies and bigotry").

[66] *Cf.* Robert Chesney et al., *All's Clear for Deepfakes: Think Again*, LAWFARE (May 11, 2020, 4:19 PM), https://www.lawfaremedia.org/article/alls-clear-deepfakes-think-again [https://perma.cc/ 46JM-4EB3] (noting in the context of discussing deep fakes that although "major platforms like Facebook and Twitter have banned some manner of digital forgeries[,] . . . [f]akes . . . have to be judged fraudulent in a particular way that contravenes the policy").

[67] *See, e.g.*, ALEXANDER L. GEORGE & RICHARD SMOKE, DETERRENCE IN AMERICAN FOREIGN POLICY: THEORY AND PRACTICE 11 (1974) ("In its most general form, deterrence is simply the persuasion of one's opponent that the costs and/or risks of a given course of action he might take outweigh its benefits.").

[68] *See generally* Robert Jervis, *Deterrence Theory Revisited*, 31 WORLD POLITICS 289, 291–92 (1979) (describing work on deterrence that "uses the game of Chicken as an analogy in situations in which the first choice of both sides is to stand firm, but in which both prefer retreating and letting the other side win to a mutually disastrous confrontation" and noting "the paradoxical nature of deterrence in which each side hopes to gain security, not by being able to protect itself, but by threatening to inflict unacceptable damage on the other").

[69] *See, e.g.*, THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 9 (1960) ("Deterrence . . . is concerned with persuading a potential enemy that he should in his own interest avoid certain courses of activity.").

expressive freedoms in a democracy depend upon a healthy digital public sphere where people can search for truth, access knowledge, and learn about political and cultural reality.[70] A resilience agenda would assess the digital public sphere that we have, rather than one that we wish that we had.[71] It would enable society to adapt to the changes to public conversation and interaction in ways that ensure that our expressive traditions can "survive the translation to the digital age."[72]

The inward focus of a resilience approach presses governments, entities, and communities to assess their priorities, ambitions, and values. This process might lead to revision or updating of commitments, or perhaps to a reinforcement of existing priorities. Either way, a resilience agenda would require stakeholders to revisit priorities, goals, and values on an ongoing basis.[73]

No doubt, decision-making in a democratic society is often difficult and drawn out.[74] Not everything can be protected, and hard choices must be made about the allocation of limited resources and the tradeoffs necessary to free certain resources for projects. Lawmakers can "fall victim to short-termism," preventing them from "supporting politically unpopular short-term sacrifices to make longer-term progress."[75] Acknowledging that fact does not suggest its inevitability, but rather highlights it as an ongoing challenge that must be managed. And indeed, it can be managed. For example, recent years have seen progress in data privacy legislative efforts to mandate corporate sacrifices for long-term societal gain. State lawmakers have strengthened privacy laws in

[70] Jack M. Balkin, *To Reform Social Media, Reform Informational Capitalism*, *in* SOCIAL MEDIA, FREEDOM OF SPEECH AND THE FUTURE OF OUR DEMOCRACY 101, 102 (Lee Bollinger & Geoffrey R. Stone, eds. 2022); CITRON, HATE CRIMES IN CYBERSPACE, *supra* note 27, at 190–221.

[71] *Cf.* Danielle Keats Citron & Neil M. Richards, *Four Principles for Digital Expression (You Won't Believe #3!)*, 95 WASH. U. L. REV. 1353, 1357 (2018).

[72] *Id.* at 1385.

[73] Checking back on priorities, goals, and values can be legally required via expiration dates. We see this, for example in the sunset provision of Section 702 of the Foreign Intelligence Surveillance Act. *See* Caroline Lynch, *The Virtue of Sunsets?*, LAWFARE (Feb. 28, 2017, 9:00 AM), https://www.lawfaremedia.org/article/virtue-sunsets [https://perma.cc/JE56-7K7W]; *see also* Ashley Deeks & Kristen E. Eichensehr, *Frictionless Government and Foreign Relations*, 110 VA. L. REV. (forthcoming 2024) (manuscript at 47), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727989 [https://perma.cc/ASP4-J5SR] (discussing sunset clauses as a type of "policy off-ramp" that prompts debate). The exact cadence of periodic re-evaluations will depend on the actors involved and the particular issues.

[74] Of this, we do not dismiss the difficulty involved. Long-standing efforts to pass a federal bill to criminalize nonconsensual disclosure of intimate images and Section 230 reform illustrate the point. *See* CITRON, FIGHT FOR PRIVACY, *supra* note 40, at 140–44, 149–55; Danielle Keats Citron, *How to Fix Section 230*, 103 B.U. L. REV. 713 (2023).

[75] FRANCES Z. BROWN, GOVERNANCE FOR RESILIENCE: HOW CAN STATES PREPARE FOR THE NEXT CRISIS?, CARNEGIE ENDOWMENT FOR INT'L PEACE 4–5 (2022), https://carnegie-production-assets.s3.amazonaws.com/static/files/Brown_Governance_for_Resilience_final.pdf [https://perma.cc/2E5P-Q3JZ].

modest yet important ways.[76] Even at the federal level, a comprehensive data privacy law has not yet been adopted, but it has drawn bipartisan support at the committee level.[77] Obstacles will remain, as ever, but a resilience approach focuses attention on choices *internal* to our political system about our collective well-being and goals, rather than trying to change the calculus of an adversary intending to cause harm.

Notably, decisions to bolster resilience might *indirectly* change adversaries' calculations about the utility of attacks. For this reason, commentators and institutions sometimes describe resilience as part of "deterrence by denial."[78] For example, the U.S. Cyberspace Solarium Commission argued that the United States "should prioritize deterrence by denial," including by "increasing the defense and security of cyberspace through resilience and public- and private-sector collaboration," because "[a] resilient nation deters adversaries by denying them the gains they seek from attacking the United States."[79]

3. Avoiding politicization

A final benefit of foregrounding resilience as a national security strategy is its potential for avoiding politicization. In an era of deep political divisions about nearly everything, including the nature, magnitude, and even existence of some national security threats, focusing on resilience may provide a way to decrease polarization about investing in and improving the country's security posture.[80] Because resilience

[76] Colorado and California are standouts in their efforts to adopt comprehensive data protection regimes. *See* Lothar Determann et al., *Comparing the Colorado Privacy Act with the California Consumer Privacy Act*, CONNECT ON TECH (Oct. 21, 2022), https://www.connectontech.com/comparing-the-colorado-privacy-act-with-the-california-consumer-privacy-act/ [https://perma.cc/3WQC-AM9M]. The Colorado Privacy Act, for instance, stems the current presumption that all data can be collected, world without end, by requiring meaningful consent before collecting sensitive data, sharing personal data for profiling, and selling personal data. *See Colorado Privacy Act (CPA)*, OFF. OF COLO. ATTORNEY GEN. PHIL WEISER, https://coag.gov/resources/colorado-privacy-act/ [https://perma.cc/9NGA-D9A7].

[77] Danielle Keats Citron & Alison Gocke, *Nancy Pelosi is Blocking Landmark Data Privacy Legislation—for a Good Reason, But There's a Way to Fix It*, SLATE (Sept. 9, 2022, 5:50 AM), https://slate.com/technology/2022/09/nancy-pelosi-data-priavcy-law-adppa.html [https://perma.cc/76Y3-MMG6].

[78] *See, e.g.*, *Deterrence and Defence*, NATO (Oct. 10, 2023), https://www.nato.int/cps/en/natohq/topics_133127.htm [https://perma.cc/G5VM-N4J4] ("Resilience is . . . an important aspect of deterrence by denial: persuading an adversary not to attack by convincing it that an attack will not achieve its intended objectives."); Eric Talbot Jensen, *Cyber Deterrence*, 26 EMORY INT'L L. REV. 773, 813–15 (2012) (discussing resilience as a type of deterrence via denying adversaries the benefit of an attack); MICHAEL J. MAZARR, UNDERSTANDING DETERRENCE, RAND CORP. 2 (2018), https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf [https://perma.cc/Q9LV-G3P2] ("Deterrence by denial represents, in effect, simply the application of an intention and effort to defend some commitment.").

[79] U.S. CYBERSPACE SOLARIUM COMM'N REPORT 32–33 (2020), https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view [https://perma.cc/TA4J-HDCH].

[80] du Plessis & Vandeskog, *supra* note 58, at 8–9 (addressing the argument that resilience

strategies improve national security vis-à-vis a range of threats, there need not be agreement among political factions or between government and the private sector on the *precise* nature of the threat or the identity of an attacker.

For example, agreement on the most likely perpetrator or most likely kind of cyberoperation is not necessary to support a resilience strategy that prioritizes cloud backups of data. The same is true for resilience strategies aimed at reinforcing the health of public discourse. A resilience strategy that tackles disinformation is not premised on concerns about *specific* kinds of lies or the *identities* of the liars.

* * *

As a counterpoint to these benefits, one might wonder whether focusing on resilience is defeatist. After all, resilience strategies take as a starting premise that bad things—whether cyberattacks or disinformation campaigns—will happen and, to a certain extent, will succeed. Resilience acknowledges that other strategies focused on protecting institutions and preventing bad behavior will fail some of the time, as they have to date, and asks what then? In our view, this approach is not defeatist, but realistic.[81] It is proactive and democracy enhancing.

Fundamentally, resilience is an agenda of optimism rather than of doom. Emphasizing resilience is not mutually exclusive with other efforts to deter adversaries from engaging in malign behavior or efforts to bolster defenses to prevent cyber intrusions from succeeding. These tactics, taken together, would be mutually reinforcing.[82] But resilience is, in our view, optimistic because it does not calculate the final score at the time of a successful attack or disruption, but rather looks forward to minimizing harm, speeding recovery, and redesigning institutions in line with society's priorities. CISA Director Jen Easterly, writing with Ukrainian cybersecurity official Victor Zhora, described resilience as "[d]oing the work up front to prepare for a disruption, anticipating that it will in fact happen, and exercising not just for response but with a deliberate focus on continuity and recovery, improving the ability to operate in a degraded state and significantly reducing downtime when an

contributes to an "exclusion of the political" and noting that while the data is not sufficient to conclude that this is the case, it certainly suggests that the way the resilience term is used by industry actors has de-politicizing potential).

[81] *See* PCAST Report, *supra* note 44, at 12 (urging a "shift from a futile quest for absolute invulnerability to a more realistic strategy of resiliency in which we control the impacts of failures").

[82] *See, e.g.*, U.S. CYBERSPACE SOLARIUM COMM'N, *supra* note 79, at 24–26 (proposing "layered cyber deterrence" as a model to combine different deterrent strategies).

incident occurs."[83] The ability to continue functioning after cyber operations distinguishes the current digital domain from the nuclear deterrence paradigm, which sought to achieve *no* use of nuclear weapons.[84] The digital domain likely cannot aim for the same absolute prohibition of bad acts, but bolstering resilience to digital threats also shows that such a goal is not necessary.

IV. HOW TO BUILD RESILIENCE

If resilience for the digital age is the goal, how then can we achieve it? This Part begins with two important acknowledgements about the role of law and technology. Then, it explores key features of a resilience agenda.

A. Initial Acknowledgments

Before turning to the components of a resilience agenda, we start with two initial acknowledgments. First, laws, regulations, and governments more generally have critical roles to play in articulating, shaping, and fostering resilience. This is true for investments in cybersecurity and other responses to widely dispersed harms like disinformation.

Consider the ways in which governments might mandate, nudge, or otherwise incentivize businesses, which generally focus on efficiency and maximizing shareholder profits, to invest in resilience strategies with long horizons and long-term payoffs.[85] With regard to some strategies, governments may need to assess and alter their own behavior, which might result in legal changes, regulations, or shifting market demand. The governments we have in mind are not just the U.S. federal government, charged most prominently with managing national security issues, but also state and local governments in the United States that provide critical functions, like courts and emergency response systems, that have fallen prey to cyber-related disruptions.[86] Issues related

[83] Easterly & Zhora, *supra* note 41.

[84] *See, e.g.*, Nye, *supra* note 64 (distinguishing nuclear deterrence from cyber deterrence because "where nuclear weapons are concerned, the aim is total prevention," whereas "[d]eterrence in cyberspace is more like crime: governments can only imperfectly prevent it").

[85] *See, e.g.*, Roberts, *supra* note 46, at 124; *see also* PCAST Report, *supra* note 44, at 20 (noting that while "[i]ncreased cyber-physical resilience is usually fully aligned with commercial goals[,] . . . there need to be checks and balances—laws or regulations—to create the incentives to build resiliency that may slip in the face of occasional short-term thinking").

[86] *See, e.g.*, John Hanna, *Top Official Says Kansas Courts Need at Least $2.6 Million to Recover from Cyberattack*, ASSOC. PRESS (Jan. 16, 2024), https://apnews.com/article/kansas-courts-cyberattack-hack-computers-costs-c8cbea12c2b8d0589d9490e81772e660 [https://perma.cc/3CYK-2Z8H] (reporting that Russian ransomware group caused a weeks-long disruption to state courts); Sean Lyngaas & Alta Spells, *Fulton County Faces Ransomware Attack by 'Financially Motivated Actors,' But County Elections Still on Track*, CNN (Feb. 14, 2024), https://www.cnn.com/2024/02/14/tech/fulton-county-ransomware-attack-financially-motivated-actors/index.html

to building resilience are not just policy questions, but legal ones as well.[87]

Second, debates about improving resilience must avoid the simplistic belief that "technology" is *the* answer or *the* problem, as if technology is something separate from human behavior. Technology is *us*. Human beings build algorithms, data sets, and system architectures.[88] Code embeds the values and choices of code writers.[89] So too with everyday problems: "When you invent the ship, you also invent the shipwreck; when you invent the plane, you invent the plane crash; and when you invent electricity, you invent electrocution . . . Every technology carries its own negativity, which is invented at the same time as technical progress."[90] Digital technologies are neither inevitable nor inevitably good (or bad).[91]

As the suggested tactics of resilience highlighted below make clear, in some cases, additional reliance on technology may help (somewhat paradoxically) mitigate risks from our reliance on technology.[92] In other cases, mitigating risks from digital dependencies may require maintaining non-technological capabilities or at least lower-tech capabilities. The role of technology in resilience is nuanced and should not be treated in a reductionist good-or-bad frame. Now to identify the distinct, yet interrelated, components of a resilience strategy.[93]

[https://perma.cc/QTN7-S2BG] (reporting on disruptions from ransomware in the county that includes Atlanta); Matt Novak, *Ransomware Attack on Dallas Disrupts 911, Court and Water Systems*, FORBES (May 4, 2023, 7:42 PM), https://www.forbes.com/sites/mattnovak/2023/05/04/ransomware-attack-on-dallas-disrupts-911-court-and-water-systems/?sh=71cdbe1f29c6 [https://perma.cc/MAF6-LZYX] (reporting that a Russia-based ransomware group disrupted a variety of government services in Dallas).

[87] *Cf.* Marchant & Stevens, *supra* note 45, at 250 (noting that to date, "law has been slow to integrate resilience strategies").

[88] The literature here is vast and cross cutting. For some highlights, *see* STEPHANIE HARE, TECHNOLOGY IS NOT NEUTRAL: A SHORT GUIDE TO TECHNOLOGY ETHICS (2022); WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018); WINNER, *supra* note 2.

[89] LAWRENCE LESSIG, CODE: VERSION 2.0 110 (2006) ("The . . . change in the code is . . . crafted to reflect choices and values of the coders."); Joel Reidenberg, *Lex Informatica, The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553, 554 (1998).

[90] PAUL VIRILIO, POLITICS OF THE VERY WORST: AN INTERVIEW WITH PHILIPPE PETIT 89 (1999).

[91] *See* HARTZOG, *supra* note 88, at 7; *see also* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1252–53 (2008).

[92] *See, e.g.*, *infra* notes 96–107 (discussing digital redundancies).

[93] These are our preliminary thoughts on resilience strategies. We draw from resilience literature across various fields; our views will continue to evolve as will those strategies. We do not mean to limit ourselves to these components but think that they are a helpful way to begin any resilience analysis, so long as the interests, goals, and values of stakeholders animate the strategies pursued.

B. Components of a Resilience Strategy

As the definitions of resilience in PPD-21 and NSM-22 suggest,[94] resilience is an ongoing strategy that stretches before, during, and after adverse incidents. This Section uses this temporal framing to discuss tactics of resilience across three phases: (1) anticipating and preparing for disruptions; (2) adapting to and withstanding disruptions when they happen; and (3) recovering from them. These tactics overlap by design: for example, preparations made in the anticipation phase will, if done well, prove useful in the withstanding and recovering phases. And lessons from the recovering phase of one disruption will inform future measures—whether through law, market practices, or education efforts—to prepare and adapt, in advance of future disruptions. Throughout, societal interests, goals, and values should inform the shape that resilience tactics take.

1. Anticipation and preparation

For all facets of resilience, the anticipation of threats and preparations to address them are key. What is done *ex ante* to prepare for adverse actions may determine the success of efforts to withstand and recover from incidents *ex post*.

In the field of cybersecurity, one key approach for preparing for digital disruptions is proactively establishing redundancies. Redundancies can take different forms. Some redundancies may be technologically enabled, like ensuring that business data can be recovered from backups in the event that ransomware renders primary business systems nonfunctional.[95] Ukraine's move to migrate crucial government databases to the cloud as a response to Russia's full-scale invasion provides a clear and successful example of redundancies providing resilience.[96] But governments facing less extreme and less immediate threats can benefit from redundancies as a resilience strategy as well.

Consider some governments' practice of creating "data embassies": data centers in other trusted countries that host critical government datasets and have immunities afforded to traditional diplomatic

[94] *See supra* notes 47–48 and accompanying text.

[95] *See, e.g.*, WHITE HOUSE, JOINT STATEMENT OF THE MINISTERS AND REPRESENTATIVES FROM THE COUNTER RANSOMWARE INITIATIVE MEETING OCTOBER 2021 (Oct. 14, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/ [https://perma.cc/A223-ZY3F] (citing "maintaining offline data backups" as a resilience measure in the context of ransomware); Marchant & Stevens, *supra* note 45, at 267 ("Redundancy is a core resilience measure.").

[96] *See supra* notes 59–62 and accompanying text.

facilities.[97] International agreements enable such resilience tactics. Estonia established the world's first data embassy in Luxembourg pursuant to a bilateral international agreement concluded between the two countries in 2017.[98] The agreement notes that it is "in the spirit of the Vienna Convention on Diplomatic Relations," but that Convention "is not sufficient to set a legal framework for the hosting of data and information systems."[99] The countries therefore agreed on particular provisions for Estonian data stored in Luxembourg that replicate traditional diplomatic immunities, including, for example, that the premises of the data embassy "shall be inviolable."[100] Estonia transferred the first datasets in 2019,[101] and the datasets that may ultimately reside at the data embassy include ones pertaining to the courts, treasury, property registries, taxes, identity documents, and national pension insurance.[102] In 2021, Monaco and Luxembourg also signed a bilateral agreement to permit the establishment of an "e-Embassy of Monaco in Luxembourg."[103] Monaco's motivation for establishing a data embassy stemmed not just from the risk of cyberattacks, but also from concerns about natural disasters and the inability to geographically disperse backups within the state's territory, which is "smaller than New York's Central Park."[104]

[97] *See generally E-Embassies in Luxembourg, E-Embassies Ensure IT Security and Diplomatic Protection*, LUXEMBOURG, https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html [https://perma.cc/22PV-7HPY] (explaining that "[d]ata is hosted with guarantees of immunity and privileges similar to those of a traditional embassy because the founding agreements between countries take account of the 1961 Vienna Convention on Diplomatic Relations," but that data embassies represent "a totally new concept in international law: as is the case for actual embassies, the data centres constitute sovereign territory of the country that owns the data." (emphasis omitted)); Thiébaut Meyer, Director, Office of the CISO, *How Digital Embassies Can Strengthen Resiliency with Sovereignty*, GOOGLE CLOUD (Nov. 11, 2022), https://cloud.google.com/blog/products/identity-security/data-embassies-strengthening-resiliency-with-sovereignty [https://perma.cc/5ZPE-LVV2] (discussing "data embassies").

[98] Agreement Between the Republic of Estonia and the Grand Duchy of Luxembourg on the Hosting of Data and Information Systems (2017), https://www.riigiteataja.ee/aktilisa/2280/3201/8002/Lux_Info_Agreement.pdf [https://perma.cc/RHA3-82P3].

[99] *Id.* at Preamble.

[100] *Id.* art. 3.

[101] Yuliya Talmazan, *Data Security Meets Diplomacy: Why Estonia Is Storing Its Data in Luxembourg*, NBC NEWS (June 25, 2019, 11:33 AM), https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171 [https://perma.cc/3ECF-MCHU].

[102] *Factsheet: Data Embassy*, E-ESTONIA, https://https://e-estonia.com/wp-content/uploads/factsheet_data_embassy.pdf [https://perma.cc/3HHJ-HWQW] (lasted visited Aug. 16, 2024).

[103] *The Principality and the Grand Duchy Linked by a New Bilateral Agreement: Pierre Dartout and Xavier Bettel Sign an Agreement to Create an e-Embassy of Monaco in Luxembourg*, GOUVERNEMENT PRINCIER PRINCIPAUTÉ DE MONACO (July 16, 2021), https://en.gouv.mc/Policy-Practice/A-Modern-State/News/The-Principality-and-the-Grand-Duchy-Linked-by-a-New-Bilateral-Agreement-Pierre-Dartout-and-Xavier-Bettel-Sign-an-Agreement-to-Create-an-e-Embassy-of-Monaco-in-Luxembourg [https://perma.cc/TMP3-6VKJ].

[104] Talmazan, *supra* note 101; *see also* GOUVERNEMENT PRINCIER PRINCIPAUTÉ DE MONACO,

Creation of high-tech redundancies to protect against cybersecurity incidents is complicated by the need to ensure that the backups are accessible, but also insulated from the potential threats. For example, data embassies have obvious appeal as a resilience measure to allow countries to withstand and recover quickly from adverse actions, but they also multiply the potential attack surface. Data embassies themselves will surely be a target for malicious actors. In some sense, this is an old challenge. In the wake of the 9/11 attacks, for example, the Federal Reserve, Office of the Comptroller of the Currency, and Securities and Exchange Commission published an "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System."[105] The paper recommended that financial institutions have "geographic diversity between primary and back-up sites for back-office operations and data centers," and while not specifying a minimum distance, recommended that "back-up arrangements should be as far away from the primary site as necessary to avoid being subject to the same set of risks as the primary location" and "should not rely on the same infrastructure components (e.g., transportation, telecommunications, water supply, and electric power) used by the primary site."[106] However, geographic diversity does not necessarily protect against cybersecurity threats that can spread rapidly through global networks.[107] Solving the *usable* redundancy challenge in response to digital threats then is more complicated.

While data embassies and cloud backups are examples of high-tech redundancies, in some cases, anticipated risks may be of such a nature or gravity that redundancy should come in the form of *technology avoidance* or at least avoidance of the same high technology that is typically used and subject to attack. As one of us (Eichensehr) has previously written, "[l]ow-tech redundancy involves deliberate decisions to retain low-tech or no-tech versions of capabilities or nondigital versions of content."[108] One example of low-tech redundancy for critical systems is

supra note 103 (discussing motivations for the e-embassy).

[105] FEDERAL RESERVE SYSTEM, DEP'T OF THE TREASURY, AND SECURITIES & EXCHANGE COMM'N, INTERAGENCY PAPER ON SOUND PRACTICES TO STRENGTHEN THE RESILIENCE OF THE U.S. FINANCIAL SYSTEM (Apr. 7, 2003), https://www.sec.gov/news/studies/34-47638.htm [https://perma.cc/YJM9-88AT].

[106] *Id.*

[107] *See, e.g.*, Greenberg, *The Untold Story of NotPetya*, *supra* note 4 (describing the speed with which NotPetya malware spread around the world).

[108] Kristen E. Eichensehr, *Giving Up on Cybersecurity*, 64 UCLA L. REV. DISC. 320, 323 (2016). A more extreme approach would be to "forego a technological capability" altogether by engaging in "technological regression or arrest," where "[t]echnological regression involves walking back from technological capabilities because of concern about the inability to properly secure the technology" and "[t]echnological arrest . . . captur[es] the deliberate decision not to proceed with developing a technical capacity because of security concerns." *Id.* at 324. That approach may be warranted in certain circumstances, *see id.* at 330–33 (discussing examples of technological regression and

state laws requiring electronic voting machines to produce a paper record or receipt, thereby bolstering the resilience of election outcomes to hacking.[109]

Tactics of anticipation and preparation are also key to tackling malign foreign influence campaigns. We can prepare people to "spot misinformation *techniques* as opposed to just individual instances of misinformation."[110] Such training, often called "pre-bunking," helps individuals recognize patterns of deception and manipulation, so they can resist them.[111] Social psychology research suggests that it is possible to "*preemptively* confer psychological resistance against (malicious) persuasion attempts."[112] Pre-bunking techniques expose people to small doses of disinformation, so they become adept at detecting disinformation and developing cognitive immunity.[113] They help people develop pattern-recognition skills, so efforts to deceive and manipulate fall flat. Introducing "pre-emptive refutations of weakened arguments" can "help build cognitive resistance against future persuasive attempts."[114]

Because specific fake news stories change and evolve at rapid-fire speed, "building immunity against the underlying tactics of misinformation is a more durable strategy" than de-bunking individual falsehoods.[115] While fact-checking can be helpful to combat specific malign falsehoods and inauthentic content, it is difficult to scale, and does not tackle cognitive biases that incline us to believe information that accords with our pre-existing beliefs.[116]

Fact-checking must therefore be combined with efforts to teach people to spot tactics of disinformation so that they are not drawn in. Finland, Estonia, Latvia, Lithuania, and Sweden have long worked on inoculating citizens against disinformation campaigns, because of Russia's proximity and because they have "face[d] a steady barrage of Russian information attacks."[117] In the United States, education efforts to inoculate the public against disinformation have begun. Dozens of

arrest), but the examples highlighted in this Essay involve instances where networking and technological capabilities generally provide significant benefits, making redundancy a more on-point approach.

[109] *See id.* at 328–29 (discussing paper backups of electronically cast votes).

[110] Jon Roozenbeek et al., *Prebunking Interventions Based on "Inoculation" Theory Can Reduce Susceptibility to Misinformation Across Cultures*, 1 HARV. KENNEDY SCH. MISINFO. REV. 1, 2 (2020).

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *Id.*

[115] *Id.* (emphasis omitted).

[116] *Id.*; *see also* Chesney & Citron, *supra* note 18, at 1765–68.

[117] P.W. SINGER & EMERSON T. BROOKING, LIKEWAR: THE WEAPONIZATION OF SOCIAL MEDIA 263 (2018).

universities offer courses in advanced critical thinking for the digital age, including, for example, the University of Washington class "Calling Bullshit: Data Reasoning in a Digital World."[118]

The combination of pre-bunking and fact-checking illustrates the interrelated nature of resilience tactics over time: fact-checking efforts that help us bounce back from disinformation campaigns will be more successful if pre-bunking efforts have already trained people to detect and withstand disinformation.

2. Adaptation to and withstanding disruption

Another component of resilience involves adapting to and withstanding disruption. This phase is particularly key for persistent or long-lasting types of disruptions for which there is time to adapt and to continue functioning while disruptions arise, evolve, and continue.

One way to build resilience of this sort is to give people the tools that they need to withstand cyberattacks with the least harm possible. Like pre-bunking with respect to disinformation, we should forewarn communities, entities, and individuals about potential disruptions. For example, just as governments promote awareness and preparedness for earthquakes or tornadoes,[119] awareness campaigns could educate the public about potential disruptions caused by cyberattacks. When such an operation later disrupts electricity or water supplies or renders mapping software unavailable, people would understand what is happening. They would be better equipped to deal with the denial of key services. The advance preparation would help lessen the panic and shock and help individuals, entities, and society adapt to and withstand disruption more easily when it occurs.

Other adaptations should aim to decrease the likelihood of online disinformation campaigns. In the United States, public discourse and education increasingly happens on social media and other tech platforms, whose profits stem from the collection, exploitation, and monetization of our intimate data.[120] Our light regulatory touch to data protection means social media companies can use our personal data to curate feeds that their algorithms predict will garner attention and

[118] *Id.* at 264. No surprise, the University of Washington has the nation's most respected disinformation, media, and tech faculty across the campus. The University of Washington's Tech Policy Lab spearheads some of that work. *See Tech Policy Lab*, UNIV. WASH., https://techpolicylab.uw.edu/ [https://perma.cc/7A9S-GT7G].

[119] *See, e.g.*, *Earthquake Preparedness*, CAL. GOV.'S OFFICE EMERGENCY SERVS., https://www.caloes.ca.gov/office-of-the-director/operations/planning-preparedness-prevention/seismic-hazards/earthquake-preparedness/ [https://perma.cc/P5HA-UGU9]; *Tornadoes*, READY.GOV, https://www.ready.gov/tornadoes [https://perma.cc/T52F-YY5T].

[120] Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Reform*, 2020 U. CHI. LEGAL F. 45 (2020).

produce advertising revenue.[121] This system implicates national security. Social media companies know that people are more likely to click on content that is negative and novel.[122] They promote such content *even when it involves destructive disinformation.*[123] After a Twitter engineer spotted massive Russian botnets in 2015, he was "told to ignore it."[124] The engineer understood why—profits.[125] "They were more concerned with growth numbers than fake and compromised accounts."[126] The lightly-regulated U.S. data marketplace is being weaponized against us. Negative and novel content attracts clicks, likes, and shares, which in turn generate advertising profits.[127] Foreign malign actors take advantage of corporate incentives to spread disinformation far and wide, exacerbating division and undermining trust in government and the press.[128]

These threats are not going away. In response, we need to adapt to the structural changes to our information ecosystem, rather than muddling through and hoping for the best.[129] Searching for political truths is difficult in a sea of lies, outrage, and hate.[130] Learning about politics and culture is challenging amidst a torrent of deepfakes and disinformation.[131] Adaptation requires a "redesign [of] the information architecture that facilitates [the] dissemination" and amplification of truths (not disinformation and other malign campaigns that sow outrage and distrust).[132]

Companies *could* (and should) work on de-amplifying disinformation, such as by decreasing its prominence. Disinformation "spreads via [companies'] services—governed by their legal and software codes."[133] Social media platforms could design their services to prevent the rapid spread of disinformation. As Facebook's chief AI scientist

[121] CITRON, FIGHT FOR PRIVACY, *supra* note 40, at 97–98.

[122] Chesney & Citron, *supra* note 18, at 1765–68.

[123] SINGER & BROOKING, *supra* note 117, at 243.

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] CITRON, FIGHT FOR PRIVACY, *supra* note 40, at 97–98.

[128] Chesney & Citron, *supra* note 18, at 1765–66.

[129] *See* Ryan Calo, *Modeling Through*, 71 DUKE L.J. 1391, 1392, 1398 (2022).

[130] *See* Mary Anne Franks, *The Free Speech Industry*, *in* SOCIAL MEDIA, FREEDOM OF SPEECH AND THE FUTURE OF OUR DEMOCRACY 65, 79–83 (Lee Bollinger & Geoffrey R. Stone, eds. 2022).

[131] *Id.*

[132] *Id.* One of us (Citron) worked closely with a few tech companies interested in doing that in the aftermath of the 2016 election—regrettably, those same companies have walked back those efforts due to new leadership, expense, or having learned the wrong lessons from *Murthy v. Missouri*. Danielle Keats Citron & Jeffrey Stautberg, *Public-Private Partnerships After* Murthy v. Missouri, IND. L.J. (forthcoming 2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4911912 [https://perma.cc/UTQ5-S85E].

[133] SINGER & BROOKING, *supra* note 117, at 269 (emphasis omitted).

acknowledged after the 2016 election, it is "technically possible to stop viral falsehoods," but companies must "manag[e] the 'trade-offs'—finding the right mix of 'filtering and censorship and free expression and decency.'"[134]

Legal intervention is needed since the market is unlikely to move there on its own. There is far too much to say on this topic, so we offer just a few ideas here.[135] Congress should adopt a comprehensive data privacy law that minimizes the intimate data that can be collected, and thus that can be exploited against us. We should set limits on the ability to micro-target advertisements based on people's social and political affinities, as the European Union has asked companies to do.[136] These are a few narrow, but still valuable, legal steps to adapt to our new information environment and threat landscape.

Then too, technology can help us withstand disinformation campaigns. Consider deepfakes—synthetic video and audio that show people doing and saying things that they never did or said.[137] As the nation's expert on image fakery Hany Farid warns, technical experts are increasingly unable to "differentiate between a flawless fake and the real thing."[138] To address those concerns, technologists have been pursuing efforts to authenticate content and to detect fakery.[139] As Farid explains, forensic techniques are "part of a larger ecosystem needed to regain trust in the visual record."[140] Along these lines, the White House's Executive Order 14,110 has directed the Secretary of Commerce to issue a report identifying the potential development of further science-backed standards and techniques, for authenticating content and tracking its provenance; labeling synthetic content; detecting synthetic content; and preventing generative AI from producing child sexual abuse material or producing non-consensual intimate imagery of real individuals (to include intimate digital depictions of the body or body parts of an identifiable individual).[141]

[134] *Id.* at 251.

[135] For more on this, see CITRON, FIGHT FOR PRIVACY, *supra* note 40, at 149–66.

[136] *See* EUROPEAN COMM'N, 2022 STRENGTHENED CODE OF PRACTICE ON DISINFORMATION 9–14 (June 16, 2022), https://ec.europa.eu/newsroom/dae/redirection/document/87585 [https://perma.cc/SE92-S3CJ]; *see also* Julie E. Cohen, *A Systems Approach to Cheap Speech: Flash Trades, Engagement Levers, and Destabilization Attacks*, BALKANIZATION (Apr. 7, 2022), https://balkin.blogspot.com/2022/04/a-systems-approach-to-cheap-speech.html [https://perma.cc/WLF2-4JBL] (discussing legal approaches to microtargeting and disinformation).

[137] Citron & Chesney, *supra* note 18, at 1758.

[138] Hany Farid, *From the Darkroom to Generative AI*, CONTENT AUTHENTICITY INITIATIVE (Aug. 15, 2023), https://contentauthenticity.org/blog/from-the-darkroom-to-generative-ai [https://perma.cc/K79B-GNRH]; *see generally* HANY FARID, FAKE PHOTOS (2019).

[139] *See* Citron & Chesney, *supra* note 18, at 1787.

[140] Farid, *supra* note 138.

[141] Exec. Order 14,110, Safe, Secure, and Trustworthy Development and Use of Artificial

3. Recovery

The final phase of a resilience strategy focuses on recovery: after an adverse event manifests, how can resilience strategies help people, institutions, governments, and society as a whole bounce back faster? Here the groundwork laid in the anticipation and preparation phases can be crucial to the success of the recovery stage.

For example, both governments and companies could stockpile "clean" equipment that could be substituted for equipment compromised or otherwise rendered unusable during a cyberattack.[142] The COVID-19 pandemic brought attention to the U.S. Strategic National Stockpile for responding to public health emergencies.[143] In contemplation of cyberattacks or other disruption of digital systems, Congress could authorize appropriations that would allow stockpiling of computers and other equipment that would be required to restore functionality of electronic government systems.[144]

Businesses might consider obtaining their own hardware stockpiles to speed recovery. In the wake of major hacking incidents, companies now are often left scrambling to acquire replacement products. For example, when North Korean government-linked hackers breached Sony Pictures in 2014, Sony executives were reportedly left to communicate via "[a] handful of old Blackberrys, located in a storage room," and the company paid employees by "haul[ing] out old machines that allowed them to cut physical payroll checks in lieu of electronic direct deposit."[145] When the Russian government's NotPetya malware spread to companies around the world, shipping giant Maersk scrambled to reconstitute its operations by sending "staffers . . . into every available electronics store in Maidenhead and [buying] up piles of new laptops and prepaid Wi-Fi hot spots."[146] To minimize ad hoc scrambling and the unreliability it causes in the recovery phase, companies could and should prepare themselves to be more resilient by acquiring redundant

Intelligence, 88 Fed. Reg. 75,191 (Oct. 30, 2023).

[142] *Cf.* Marchant & Stevens, *supra* note 45, at 268 (describing "stockpil[ing] needed mitigation resources and supplies for when something does go wrong" as a "substantive resilience measure").

[143] *Strategic National Stockpile*, U.S. DEP'T OF HEALTH & HUM. SERVS. https://aspr.hhs.gov/SNS/Pages/default.aspx [https://perma.cc/HT7T-4TQV].

[144] *See* Jensen, *supra* note 78, at 816 (discussing the need for congressional authorization to permit "purchas[ing] large numbers of computers and other spare systems in case of an attack where spares would be needed").

[145] Michael Cieply & Brooks Barnes, *Sony Cyberattack, First a Nuisance, Swiftly Grew into a Firestorm*, N.Y. TIMES (Dec. 30, 2014), https://www.nytimes.com/2014/12/31/business/media/sony-attack-first-a-nuisance-swiftly-grew-into-a-firestorm-.html [https://perma.cc/7PKK-Q8JU].

[146] Greenberg, *The Untold Story of NotPetya*, *supra* note 4.

tech to be used in emergency situations before they happen. Regulators could foster such planning by asking about it in required disclosures.[147]

Beyond using tech to recover, however, there is also a case to be made for low-tech or no-tech redundancies—preservation of analog capabilities—to foster recovery. Consider the retention (or installation) of manual backup controls for critical infrastructure that can help maintain or restore service in the wake of a cybersecurity incident.[148] Having manual functionality reportedly allowed Ukraine to recover from Russian cyberattacks that knocked out power for several hours in December 2015.[149] Power was restored within a matter of hours, and for months after the incident, operators continued to use the manual controls.[150] Reporting on the Ukraine incident noted that the response was "actually a better outcome than what might occur in the US, . . . since many power grid control systems here don't have manual backup functionality, which means that if attackers were to sabotage automated systems here, it could be much harder for workers to restore power."[151] While automation has many benefits, it also creates vulnerabilities. Maintaining or creating low-tech or no-tech backup systems, and crucially, training employees in advance on how to operate or revert to them in a time of crisis, could bolster resilience by speeding recovery.

What does recovery look like for malign disinformation campaigns? As noted above, fact-checking enterprises can help debunk lies and reduce their spread. But recovery efforts also must include defending the defenders of expressive freedoms—journalists and researchers—against online abuse designed to silence them.[152] As a disinformation researcher explained, the key to "surviving online attacks . . . is having

[147] *Cf.* Securities & Exchange Comm'n, Final Rule, Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 88 Fed. Reg. 51,896 (Aug. 4, 2023) (requiring periodic disclosures about public companies' "processes to assess, identify, and manage material cybersecurity risks, management's role in assessing and managing material cybersecurity risks, and the board of directors' oversight of cybersecurity risks").

[148] *See, e.g.*, Lewis Herrington & Richard Aldrich, *The Future of Cyber-Resilience in an Age of Global Complexity*, 33 POLITICS 299, 305–06 (2013) (discussing retention of analog capabilities to operate critical infrastructure as a resilience mechanism to cyber intrusions and expressing concern that in the United Kingdom, "this unintended but valuable source of resilience will be eroded in the name of cost-cutting and efficiency" through the introduction of digital systems).

[149] Kim Zetter, *Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid*, WIRED (Mar. 3, 2016), https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ [https://perma.cc/A6K5-XCC6]; *see also* CYBERSECURITY & INFRASTRUCTURE SEC. AGENCY, IR-ALERT-H-16-056-01, ICS ALERT: CYBER-ATTACK AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE (2021), https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01 [https://perma.cc/U37U-P37S] (describing the intrusion in detail and noting the attribution to the Russian government).

[150] Zetter, *supra* note 149.

[151] *Id.*

[152] Citron & Richards, *supra* note 71, at 1377–81.

both public and private support."[153] Employers should protect researchers and journalists facing online assaults. Law enforcement must investigate online harassment to deter attackers and to convey to victims that law is on their side.[154]

Regrettably, disinformation researchers have sometimes been abandoned at the very moment that they most needed institutional support. Online trolls and right-wing media outlets attacked Nina Jankowicz in April 2022 after she took the helm of a new group in the Department of Homeland Security called the Disinformation Governance Board.[155] On Sean Hannity's Fox News show, Representative Jim Jordan said that Jankowicz "will come after you" and Hannity accused her of spreading disinformation.[156] Representative Lauren Boebert released a public statement saying Jankowicz was a "Russia hoax espousing radical who is on video singing and asking who she needs to have sex with to become famous and powerful."[157] A cyber-mob campaign followed. Splices of videos taken out of context appeared online suggesting falsely that Jankowicz endorsed the idea that certain people should have the power to edit others' tweets.[158] She was doxed and flooded with threatening emails, texts, and voicemails.[159] Her face was morphed into porn; the deepfake sex videos of her were circulated online.[160] The Biden administration closed the Disinformation Governance Board, and Jankowicz resigned.[161] Jankowicz and her family "were left to face the abuse by themselves—she received no support from her former employer."[162] Law enforcement provided no help, even though federal and state cyber stalking and threat laws might have covered some of the abuse.

[153] ARO, *supra* note 35, at 178.

[154] *See* Danielle Keats Citron, *The Continued (In)visibility of Cyber Gender Abuse*, 133 YALE L.J.F. 333, 343–46 (2023) (showing law enforcement's continued failure to take cyber gender abuse seriously).

[155] Shannon Bond, *She Joined DHS to Fight Disinformation. She Says She Was Halted by . . . Disinformation*, NPR (May 21, 2022, 5:00 AM), https://www.npr.org/2022/05/21/1100438703/dhs-disinformation-board-nina-jankowicz [https://perma.cc/PG77-3UMQ].

[156] Heidi Przybyla, *'A Surreal Experience': Former Biden 'Disinfo' Chief Details Harassment*, POLITICO (Mar. 8, 2023, 4:30 AM), https://www.politico.com/news/2023/03/08/former-biden-disinfo-chief-details-harassment-00085981 [https://perma.cc/U6LT-82HZ].

[157] *Rep. Boebert Introduces Bill to Terminate the Department of Homeland Security's Disinformation Governance Board*, CONGRESSWOMAN LAUREN BOEBERT, https://boebert.house.gov/media/press-releases/rep-boebert-introduces-bill-terminate-department-homeland-securitys-0 [https://perma.cc/8XVK-F2Y2].

[158] Przybyla, *supra* note 156.

[159] *Id.*; Zoom Interview with Nina Jankowicz, *supra* note 56.

[160] Techtonic, *The Deepfake Porn Problem*, ARTICLE 19 (Aug. 21, 2023), https://www.article19.org/resources/techtonic-deepfake-porn-caught-in-the-crosshairs/ [https://perma.cc/XFB4-AFDQ].

[161] Citron, *Continued (In)visibility*, *supra* note 154, at 335.

[162] *Id.*

By contrast, disinformation expert Kate Starbird, a professor at the University of Washington, received crucial support from her employer in the face of online abuse. Starbird has studied online rumors, conspiracy theories, and disinformation for more than a decade.[163] After her lab joined with other researchers to track election rumors, their work was attacked as "censorship."[164] Starbird and her colleagues faced online harassment campaigns and threats.[165] Starbird enjoys support from the University of Washington, as she faces litigation, public records requests, and congressional interviews.[166]

V. CONCLUDING CAUTIONS

While national security most often brings to mind governments, the examples above illustrate that both the vulnerabilities and the need for resilience function not just at the government level, but also with respect to the private sector, civil society, and individual levels. We need a whole-of-society approach that involves social norms, legal reform, and market developments.

At the same time, we also want to sound several notes of caution. Championing resilience should not mean simply devolving responsibility to individuals. Resilience is not a strategy designed just to reinforce individual control, which is impossible in the age of digital behemoths and networks. Individuals, of course, have a role to play, but attempting to force individuals to shoulder the mother lode of responsibility for

[163] Kate Starbird, *UW Misinformation Researchers Will Not Buckle Under Political Attacks*, SEATTLE TIMES (Oct. 6, 2023, 3:07 PM), https://www.seattletimes.com/opinion/uw-misinformation-researchers-will-not-buckle-under-political-attacks/ [https://perma.cc/7WXE-A5Q7].

[164] *Id.*

[165] *Id.* The attacks on Starbird resemble the abuse faced by Jessikka Aro, Rana Ayyub, and others who investigate online influence campaigns and political corruption. *See supra* text and notes.

[166] *Id.* There are other crucial structural reforms that should be pursued to tackle cyber harassment. At the very moment when we are awash in cyber stalking abuse and disinformation, content platforms are stepping back from their efforts at content moderation. Kat Lo, *Elon Musk's Twitter Takeover: Five Takeaways For Content Moderation*, MEEDAN (Nov. 18, 2022), https://meedan.com/post/five-content-moderation-takeaways-from-elon-musks-twitter-takeover [https://perma.cc/RTG3-H3XR] ("Twitter has been rapidly decreasing staffing and capacity for carrying out content moderation actions to prevent misinformation, hate speech, and online abuse."). Content moderation should be brought in house, rather than outsourced through low-paid contracts in countries where minimum pay is appallingly low, and it should be adequately funded. *See* Paul M. Barrett, *It's Past Time to Take Social Media Content Moderation In-House*, JUST SEC. (Jan. 18, 2023), https://www.justsecurity.org/84812/its-past-time-to-take-social-media-content-moderation-in-house/ [https://perma.cc/GJB7-T6TZ]. Law must provide the needed incentives, since the market is not pressing us in this direction. We can and should adopt reforms to Section 230 of the Communications Decency Act, so that legal immunity is not enjoyed by sites that deliberately solicit, encourage, or fail to remove cyber stalking, intimate privacy violations, or digital forgeries and so sites otherwise have duties of care to address such abuse. *See* Citron, *Continued (In)visibility*, *supra* note 154, at 365–66 (discussing draft bill that Citron worked on with Massachusetts Congressman Jake Auchincloss).

resilience is setting us up to fail. This is true for cybersecurity, where individuals are sometimes blamed for falling prey to a phishing email, without also pointing to the failure of training or another institutional action. It is also true for disinformation, where we sometimes blame the person who shares Kremlin-backed posts that tell people that they can vote via text, rather than the platform that amplified the post in the first place. Responsibility for resilience cannot rest solely with individuals; it must lie throughout and across society, with individuals *and* governments *and* non-governmental institutions.

Equity concerns arise as well. The burdens of disruptions do not fall equally, and they often fall disproportionately on communities that are least equipped to bear them. In thinking about how to invest in and plan for resilience, we should consider pooling investments to protect everyone. That means that at least some of the resilience investments must be at the societal and structural levels.

With this Article, we begin a conversation for us about the significance of resilience. We hope to engage with scholars and practitioners across disciplines and areas on this topic. And we hope to see more and more research on resilience strategies for the good of national security.