The Journal of Civic Information

Volume 6 | Number 1 June 2024

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

The Journal of Civic Information is an interdisciplinary peer-reviewed open-access online journal published by the Brechner Center for Freedom of Information through the Public Knowledge Project and is supported by the University of Florida College of Journalism and Communications.

Contact:
David Cuillier, Ph.D.
cuillierd@ufl.edu

DOI: https://doi.org/10.32473/joci.6.1

Table of Contents

Editor's Note

Legal Analysis

JCI Editorial Board

The Journal of Civic Information

Volume 6 | Number 1 June 2024

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Editor's Note: Welcoming New Journal Associate Editors

David Cuillier, Ph.D., Editor and Publisher, *University of Florida* *

The *Journal of Civic Information* welcomes two new associate editors to improve the reach and impact in scholarship toward a more informed world. The positions are new, with an eye to increase submissions, readership, and depth. The selections, through a committee of editorial board members, followed an open search and interview process.

Dr. A.Jay Wagner

Dr. Wagner is an associate professor of journalism and media studies in Marquette University's Diederich College of Communication. His research focuses on access to government information, publishing in *Government Information Quarterly*, *Administration & Society*, *Journalism*, *Journal of Civic Information*, *University of Florida Journal of Law & Public Policy*, *Quinnipiac Law Review*. His scholarship has received awards from the Association for Education in Journalism and Mass Communication, National Communication Association, and the National Freedom of Information Coalition.

He received his doctorate in mass communication from Indiana University in 2016. He holds a bachelor's degree from the University of Dayton and a master's from DePaul University. He has served on the FOIA Advisory Committee under the National Archives and Records Administration, acted as an expert witness in federal FOIA cases, and been a panelist for a recent Government Accountability Office report on reducing FOIA backlogs. Dr. Wagner worked professionally as a journalist for several years before pursuing a doctorate and has also worked in media rights advocacy, including time at the International Press Institute and the McCormick Foundation.

Dr. Ahmed Alrawi

Dr. Alrawi completed his doctorate this spring at the Donald P. Bellisario College of Communications at Pennsylvania State University and is embarking on a post-doc position at the University of Virginia's Karsh Institute of Democracy. He holds a bachelor's degree from the College of Communications at Al-Mansour University in Baghdad, Iraq, with a major in computer communication engineering. Additionally, he earned another bachelor's degree in telecommunications before attaining his master's degree in media studies, both from Bellisario College.

Dr. Alrawi's research interests span two main areas: (1) Surveillance, Privacy, & the Implications of ICTs, and (2) Broadband Platform Policy and Deployment. His research goal is to comprehensively understand the theoretical, methodological, and empirical aspects that shape the adoption, use, and impact of digital platforms and ICTs. Moreover, his research seeks to draw attention to contemporary issues within the communication and media sectors, advocating for appropriate regulations and policies to benefit the public. Dr. Alrawi's work has been published in the *Journal of information policy*, *Journalism & Mass Communication Quarterly*, *Mass Communication and Society*, *Surveillance & Society*, *and Touro Law Review*.

Fluent in Arabic, Turkish, and English, Alrawi is also conversant in French. He has received numerous awards, including the Sidney and Helen Friedman Scholarship Endowed Award and the Graduate School Endowment Award, among others.

I am thrilled to have Drs. Wagner and Alrawi join the journal team. They represent broad interdisciplinary expertise across various citation styles and publication types, which is essential for the expansive issues concerning civic information. They will be assisting with editing, pagination, managing submissions, and outreach. We welcome suggestions for improving the journal to provide an outlet for research on information that helps citizens throughout the world be more informed about their communities and government.

DOI: 10.32473/joci.6.1.136683
** Send correspondence about this article to David Cuillier, Director of the University of Florida College of Journalism and Communications Joseph L. Brechner Freedom of Information Project, cuillierd@ufl.edu.*

The Journal of Civic Information

Volume 6 | Number 1 June 2024

Journal homepage: https://journals.flvc.org/civic/ ISSN (online): 2641-970X

Critical Shrinking: The Perils of Opaque and Undefined Critical Infrastructure Policy in American Communications

Benjamin W. Cramer *

Article Information

Received: January 5, 2024

Accepted: April 7, 2024

Published: June 27, 2024

Keywords

Regulatory language
Statutory language
Transparency
Policy
Communications
National security
Critical infrastructure

Abstract

This article analyzes American regulations, legislation, and executive orders that address the matter of critical infrastructure, primarily in communications. The article conducts policy-oriented research into the relevant government documents, plus theoretical research on the framing of geopolitical disputes and the transparency of regulatory actions. This article argues that existing definitions of critical infrastructure are indistinct and tautological, while they perennially get mixed up with national security. The article concludes that a distinct American policy definition should be formulated at a government-wide level and observed by all relevant agencies, as has been achieved to a certain extent by the European Union, as opposed to the current pattern of relying on myriad government agencies to announce vague and unworkable definitions of the term. Otherwise, the United States will be unable to effectively address threats to critical infrastructure, from malicious actors or from international market trends.

* Benjamin W. Cramer, Ph.D., is a teaching professor in Telecommunications and Media Industries at the Donald P. Bellisario College of Communications at Pennsylvania State University. Please send correspondence about this article to Dr. Cramer at bwc124@psu.edu.

To cite in Bluebook: Benjamin W. Cramer, *Critical Shrinking: The Perils of Opaque and Undefined Critical Infrastructure Policy in American Communications*, 6 J. CIVIC INFO. 1, 1-26 (2024).
To cite in APA: Cramer, B. W. (2024). Critical shrinking: The perils of opaque and undefine critical infrastructure policy in American communications. *Journal of Civic Information, 6*(1), 1-26.

DOI: 10.32473/joci.6.1.135040

I. Introduction

This article will analyze American regulations, legislation, and executive orders that address the matter of "critical infrastructure," starting with the general usage of that term in matters such as national security and financial policy, and eventually focusing on communications networks. The article will conduct policy-oriented research into the relevant American government documents, plus more theoretical research on the framing of geopolitical disputes and the transparency of the resulting regulatory actions.

In American law, the first notable use of the term "critical infrastructure" was in the USA PATRIOT Act of 2001,[1] which was a direct response to terrorist attacks. In parallel with the related term "national security," critical infrastructure started its regulatory life with a fairly precise security-oriented definition that has become much less distinct in the ensuing years. Communications networks first enjoyed extra attention as critical infrastructure during the Obama Administration, alongside new conceptions of such networks as vital to national security. This trend was exacerbated by the Trump Administration, which added those conceptions to retaliatory trade policies, particularly with rival nations such as China. Regardless, the definition of critical infrastructure, including telecom-related uses of the term, remains elusive as a matter of law.

Importantly, the United States promotes the goal of protecting critical infrastructure but with few enforceable policies in place to do so. Meanwhile, most of the nation's telecom network infrastructure is owned by private firms, for which the profit motive supersedes policy concerns. In contrast, other countries have distinct policies in place that enable government oversight of critical infrastructure, with a developed and distinct definition of the term. This may cause the United States to fall behind in its ability to react to everything from high-tech market trends to terrorist cyberattacks.[2]

This article will analyze the causes and effects of America's indistinct policy definition of critical infrastructure, along with the political framing of associated geopolitical disputes and threats. Via an analysis of statutory and regulatory language,[3] this article will argue that existing definitions of critical infrastructure are indistinct, tautological, and self-referencing; while they perennially get mixed up with the related but different matter of national security. Upon comparing America's patterns with how the European Union and China have handled definitions of critical infrastructure and policies designed to protect it, this article ultimately argues that the much-needed distinct policy definition requires concrete proposals for designing and protecting that infrastructure rather than relying on myriad government agencies to announce vague and unworkable definitions of the term.

---

[1] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). While colloquially known as simply the Patriot Act, the statute's full title is an acronym for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism." The shorter form of the name will be used here for brevity.

[2] *See* David W. Opderbeck, *Huawei, Internet Governance, and IEEPA Reform*, 47 OHIO NORTHERN U. L. REV. 165, 221 (2021).

[3] This article primarily analyzes each statute or regulation's meaning on its face plus interpretations that can be gleaned from comparisons with similar documents and legislative history. This technique is often used by judges and legal scholars. For the theoretical underpinnings of this method, *see* Congressional Research Service, *Statutory Interpretation: Theories, Tools, and Trends*, report (Mar. 10, 2023), https://crsreports.congress.gov/product/pdf/R/R45153.

II. From antiterrorism to critical networks

The American conception of critical infrastructure, though not necessarily under that terminology, can be traced back to the early years of the Cold War between the United States and the Soviet Union when military leaders sought to identify transportation and communications systems that must remain operational in the event of a nuclear attack.[4] The general concept changed little over the ensuing decades, even as the Cold War faded from history in the 1990s.

The first newsworthy use of the specific term "critical infrastructure" by the U.S. government was in reaction to the terrorist attacks of September 11, 2001. The term has since been used in many statutes and regulations for systems in which disruption by enemies could cause major hardships for the United States, though with a noticeable lack of precision. Critical infrastructure tends to be vaguely and inconsistently defined in American law, and often in conjunction with its equally vague counterpart "national security."[5] Despite its dramatic nature, the term "national security" has been used in so many American statutes and regulations, usually without a distinct definition, that it has become practically useless as a measure of citizen protection or governmental progress.[6]

This article will argue that the same may be true of the somewhat less dramatic "critical infrastructure," though the effects may be nearly as significant, at least for communications networks. This article will eventually focus on communications, but other industries were deemed to be "critical" in the wake of the 9/11 attacks. The fact that communications and other sectors were added to the collection over time illustrates the inconsistent and unworkable definition of the term.

The most prominent federal statute passed in reaction to the attacks, the Patriot Act,[7] outlined a fairly manageable list of industry segments that needed immediate upgrades and protection against future attacks. Tellingly, the House Committee on Transportation and Infrastructure played a large role in drafting the statute's language.[8] Transportation featured prominently, with attacks on mass transit and delivery systems now categorized as terrorist acts to be prosecuted thusly.[9] The only other industry to receive noteworthy mention in the Patriot Act was communications, but all of the provisions surrounding that industry involved the pervasive and well-researched electronic surveillance that is outside the scope of this article.[10] There was no

---

[4] *See* AYNE KOKAS, TRAFFICKING DATA: HOW CHINA IS WINNING THE BATTLE FOR DIGITAL SOVEREIGNTY 76-77 (2022). In telecommunications during this period, government policy on networks remaining operational as critical systems was simplified by the fact that AT&T was the telephone monopoly, and in return was subjected to various types of government oversight. *See* Adam D. Thierer, *Unnatural Monopoly: Critical Moments in the Development of the Bell System Monopoly*, 14 CATO J. 267, 275-276 (1994).

[5] *See* Benjamin W. Cramer, *Entity of the State: The Transparency of Restricting Telecommunications Firms as Threats to America's National Security*, 4 NOTRE DAME J. OF EMERGING TECHNOLOGIES 56, 66-67 (2023).

[6] *See* J. Benton Heath, *The New National Security Challenge to the Economic Order*, 129 YALE L.J. 1020, 1047-1050 (2020).

[7] Pub. L. No. 107-56, 115 Stat. 272 (2001).

[8] *See H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, https://www.congress.gov/bill/107th-congress/house-bill/3162/text.

[9] Pub. L. No. 107-56 at § 801.

[10] *Id.* at §§ 201-225. These sections of the Patriot Act make up an entire distinct section called "Title II – Enhanced Surveillance Procedures." For introductions to this topic as presented in the text of the Patriot Act, *see* Laurie Thomas Lee, *The USA Patriot Act and Telecommunications: Privacy under Attack*, 29 RUTGERS COMPUTER & TECH. L.J. 371, 379-399 (2003); Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHICAGO L. REV. 287, 295-305 (2008).

mention at the time about communications networks being the targets of terrorist attacks; that possibility did not become a serious concern for lawmakers until the following decade, as will be covered in the next section below.

Though they were only mentioned very briefly in the Patriot Act,[11] power and water utilities were the first major industrial sector instructed by policymakers to shore up security after the 9/11 attacks, in the interest of maintaining infrastructure that could be tempting targets for terrorists.[12] The antiterrorism conception of risks to utilities later expanded to delivery networks, with fossil fuel pipelines and related transport or storage facilities being advanced as possible targets needing extra protection. Energy was mentioned briefly in the Patriot Act,[13] but more specific delivery network facilities and their susceptibility to villainous attacks were gradually added to later conceptions of critical infrastructure in other statutes and agency regulations.[14]

This was the beginning of an expansion of the term "critical infrastructure" from a precise collection of likely terrorist targets to an inconsistent and unworkable pile of disparate industry segments that may be essential to the functioning of American society but may also be headed by parties trying to cultivate government funding or other attention by claiming that their systems are indeed "critical." Communications networks, for purposes other than collecting surveillance data, were eventually added to this framework, but with little instruction on how they can be protected, for what reason, and by whom. As this article will argue, simply saying that something is "critical" means little without a more precise definition of the term and a plan to address risks. These tricky details tend to be forgotten in the political drama of calling for protection and fighting against future attacks. The definition of "critical infrastructure" has been politicized and expanded to the point of vagueness and uncertainty. This can, in fact, lead to less protection of those crucial systems and can reduce their competitiveness on the world stage.

III. More is less: Attempting to define critical infrastructure in federal policy

A national effort to protect critical infrastructure predated the 9/11 terrorist attacks by three years, and the non-emergency rationale of that period is noticeable, as is the fact that the concept received little attention at the time. In 1998, President Bill Clinton issued Presidential Directive PDD-63, positioning infrastructure protection as necessary for economic strength and quality of life.[15] This directive advanced a loose definition of critical infrastructure as "those physical and cyber-based systems essential to the minimum operations of the economy and government." It did not attempt to list *all* relevant industrial sectors, noting that they "include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services." The directive states its goal as preventing "non-traditional attacks on our infrastructure

[11] Pub. L. No. 107-56 at § 1016(b)(2).
[12] *See* Don Byrne, *Preparedness Standards Can Have Positive Effect on Utilities*, 28 CLIMATE AND ENERGY 21, 21-22 (May 2012).
[13] Pub. L. No. 107-56 at § 1016(b)(2).
[14] *See* Benjamin W. Cramer, *Envirodemic: Unconstitutional Restrictions on Environmental Protests from the Attacks of 2001 to the Struggles of 2020*, 14 L. J. SOCIAL JUST. 79, 81 (2021).
[15] *See* The White House, *Presidential Decision Directive/NSC-63* (May 22, 1998), https://irp.fas.org/offdocs/pdd/pdd-63.htm. An entity called the President's National Security Telecommunications Advisory Committee had existed since 1982, but its responsibilities were expanded significantly in the post-9/11 era of greater focus on national security. EXEC. ORDER NO. 12,382, 47 F.R. 40531 (1982); amended by EXEC. ORDER NO. 13,285, 68 F.R. 10619 (2003).

and information systems [that] may be capable of significantly harming both our military power and our economy."[16]

Clinton's directive also attempted to set up a public-private partnership structure to identify risks.[17] Such efforts were to be overseen by a newly designated official known as the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism.[18] There has been some criticism of the public-private partnership structure, which may allow the participating companies to advance their own importance to national security and then claim to need government funding to prevent attacks on their infrastructure.[19] The wish for public-private partnerships, but with few instructions on setting them up, would also bedevil later efforts to shore up critical infrastructure systems via statutory requirements and advisory recommendations, particularly in telecommunications, as will be seen below.[20]

A. Post-9/11 statutes

The first major American statute to include a specific focus on protecting critical infrastructure was the Patriot Act, which was passed rapidly after the 9/11 attacks. The statute's many requirements for security, surveillance, and infrastructure protection were almost uniformly described as necessary to protect Americans from further attacks.[21] Extra protection for critical infrastructure in the statute initially took the form of criminal prosecution for property damage committed by terrorists.[22] Critical infrastructure itself was defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[23] This original definition has been repeated with just a few minor variations in most of the subsequent statutes and regulations dealing with critical infrastructure, despite orders from two presidents to make it more distinct.

The Patriot Act made no further effort to define critical infrastructure or any particular industry sectors or networks that it may contain, except for some mentions of transportation systems. The statute instead reinforced the need to protect such systems at the higher level, with rhetorical proclamations like, "A continuous national effort is required to ensure the reliable provision of cyber and physical infrastructure services critical to maintaining the national defense, continuity of government, economic prosperity, and quality of life in the United States."[24] Note

[16] *Presidential Decision Directive/NSC-63* at § I.
[17] *Id.* at §§ IV, VI.
[18] *Id.* at § VI, ¶ 3. The first person to assume this role was national security expert Richard A. Clarke.
[19] *See* Elisa Williams, *Climate of Fear*, FORBES (Feb. 4, 2002), https://www.forbes.com/forbes/2002/0204/064.html?sh=77f886335222.
[20] *See infra* notes 66-68 and accompanying text.
[21] This was the general explanation from the Department of Justice, which was assigned to enforce the terrorism-related bills passed by Congress in the post-9/11 period. *See* United States Department of Justice, *Preserving Life and Liberty*, https://www.justice.gov/archive/ll/archive.htm.
[22] *See* Rebecca K. Smith, *Ecoterrorism: A Critical Analysis of the Vilification of Radical Environmental Activists as Terrorists*, 38 ENVIRONMENTAL L. 537, 570 (2008); Will Potter, *Sentinel Species: The Criminalization of Animal Rights Activists as "Terrorists," and What It Means for Civil Liberties in Trump's America*, 95 DENVER L. REV. 877, 879-882 (2018). Note that beyond foreign Islamists, in late 2001 there was widespread condemnation of environmental activists, with American politicians often describing them as "terrorists", and this has been documented as an influence on the statutory language of the Patriot Act. *See also* Cramer, *Envirodemic*, *supra* note 14, at 80-81.
[23] Pub. L. No. 107-56, § 1016(e).
[24] *Id.* at § 1016(a)(3).

that this statement does not extend beyond the wide adjectives "cyber" and "physical," which could be seen as a sign of flexibility but which also engendered inconsistency and uncertainty in later statutes and regulations. The statute also called for "a public-private partnership involving corporate and non-governmental organizations,"[25] but with no instructions on who should be invited and what they should accomplish.

In the decades since the Patriot Act, specific networks such as telecommunications and utilities have been added to the running definition of critical infrastructure; conversely, so have many other types of installations, hence making the term less and less distinct. Starting in the post-9/11 period, critical infrastructure has usually been mentioned alongside national security in federal policy documents. While the use of two different terms should imply that they are distinct concepts, the definition of critical infrastructure has never quite been differentiated from more prevalent but nearly as indistinct definitions of national security.

Critical infrastructure appears in the Homeland Security Act of 2002,[26] a more procedural statute written to implement many of the specific goals of the Patriot Act while setting up the operations and responsibilities of the then-new Department of Homeland Security. The Homeland Security Act added criminal terrorism charges to offenses that are "potentially destructive of critical infrastructure or key resources."[27] In turn, the term critical infrastructure was defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government."[28] Once it went into operation, the Department of Homeland Security identified 18 industrial sectors that fall partially or completely within critical infrastructure, including one denoted as "Information Technology and Telecommunications."[29]

The Homeland Security Act concocted the additional term "critical infrastructure information" as something useful for determining when the department should jump into action, such as "any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation."[30] The statute also defined the threat of "actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems)."[31] This was the first precise mention of communications-oriented infrastructure as a matter of national security in a federal statute. However, the act added no precision to the high-level definition of critical infrastructure itself from the previous year's Patriot Act.

Also in 2002, Congress passed a statute focused on information and reporting. The Critical Infrastructure Information Act ordered the Department of Homeland Security to coordinate the management of information about critical infrastructure amongst various government departments

[25] *Id*. at § 1016(c)(2).
[26] Pub. L. No. 107-296, 116 Stat. 2135 (2002).
[27] *Id*. at § 2(15)(A)(i).
[28] *Id*. at § 101(4).
[29] *See* Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS)*, report (Feb. 26, 2020), https://crsreports.congress.gov/product/pdf/RL/RL33388, at 17. For the full list of 18 sectors, *see also* Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Sectors*, http://www.dhs.gov/critical-infrastructure-sectors.
[30] Pub. L. No. 107-296, at § 212(3)(C).
[31] *Id*. at § 212(3)(A).

and agencies.[32] Such information included the risks faced by critical infrastructure installations and their abilities to resist those risks.[33] One pertinent provision of this statute instructed the government to manage any such information that had been provided voluntarily by the public, and the resulting documents would be shielded from disclosure via the Freedom of Information Act or other processes through which interested citizens could request access. The same was true for state and local government documents.[34] Ironically, this expanded the types of information that are relevant for the protection of critical infrastructure but made that same knowledge more secretive. As will be discussed in a later section, policymakers often fall into the trap of keeping a topic secret while trying to convince the citizenry of that same topic's importance, and this typically allows those policymakers to avoid accountability for inconsistent definitions and poor planning.[35]

B. A voluntary national plan

The enormity of coordinating infrastructure protection among a multitude of federal, state, and local departments required not just far-reaching statutes but presidential orders and the creation of specialist agencies as well. President George W. Bush issued Presidential Directive HSPD-7 in 2003 to reinforce the need for protection. However, this directive merely repeated the basic definition of critical infrastructure from the Patriot Act and added the trite "Critical infrastructure and key resources provide the essential services that underpin American society."[36] Given the political milieu of the time, and concerns about terrorism that had not been present in Clinton's 1998 directive on the same general topic, Bush's directive emphasized that, "Terrorists seek to destroy, incapacitate, or exploit critical infrastructure and key resources across the United States to threaten national security, cause mass casualties, weaken our economy, and damage public morale and confidence."[37] This directive instructed the Secretary of Homeland Security to establish uniform policies for the protection of critical infrastructure for purposes of national security;[38] that effort began almost immediately but has thus far resulted in little more than voluntary workshops and advisory documents.

In 2006, Homeland Security solidified multiple presidential directives and the goals of the post-9/11 statutes by formulating the National Infrastructure Protection Plan (NIPP), which in turn sought to coordinate the efforts of government agencies and the private sector during an emergency. That plan was updated in 2009 and 2013.[39] The most recent version of the plan uses the term critical infrastructure hundreds of times but with a disarming lack of precision, introducing the concept as simply "those assets, systems, and networks that underpin American society."[40] The 2013 report gives the impression of expanding the definition a bit with "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or

---

[32] 6 U.S.C. §§ 671-674 (2002).
[33] *Id*. at § 671(3).
[34] *Id*. *See also* Freedom of Information Act, 5 U.S.C. § 552 (1966).
[35] *See infra* notes 140-143 and accompanying text.
[36] *See* Office of the President of the United States, *Homeland Security Presidential Directive 7* (Dec 17, 2003), https://www.cisa.gov/news-events/directives/homeland-security-presidential-directive-7, at ¶ 4.
[37] *Id*. at ¶ 2.
[38] *Id*. at ¶¶ 12-15.
[39] *See* Cybersecurity and Infrastructure Security Agency, *2013 National Infrastructure Protection Plan*, https://www.cisa.gov/resources-tools/resources/2013-national-infrastructure-protection-plan.
[40] *See* United States Department of Homeland Security, *NIPP 2013: Partnering for Critical Infrastructure Security and Resilience*, report (2013), https://www.cisa.gov/sites/default/files/2022-11/national-infrastructure-protection-plan-2013-508.pdf, at 1.

destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[41] This definition is indeed longer than in the previous plans; unfortunately it is copied straight from the Patriot Act[42] which itself inspired the Presidential Directive that ordered these same policymakers to come up with a more workable definition.

Exemplary sentences in the NIPP illustrate the lack of a precise definition, and an unproven assumption that everyone should be able to decipher that definition via sheer repetition and tautology. Such sentences include: "The national effort to strengthen critical infrastructure security and resilience depends on the ability of public and private critical infrastructure owners and operators to make risk-informed decisions when allocating limited resources in both steady-state and crisis operations,"[43] and "Effective risk management requires an understanding of the criticality of assets, systems, and networks, as well as the associated dependencies and interdependencies of critical infrastructure,"[44] among many others.

The expansive and uncertain definition of the concept is further illustrated by the apparent risks faced by critical infrastructure, which the department lists as acts of terrorism, pandemics, extreme weather, accidents or technical failures, or cyber threats.[45] The plan does become a bit more precise on the matter of telecommunications, stating that, "Growing interdependencies across critical infrastructure systems, particularly reliance on information and communications technologies, have increased the potential vulnerabilities to physical and cyber threats and potential consequences resulting from the compromise of underlying systems or networks."[46] Regardless of its definitional precision or lack thereof, it is important to note that the NIPP is an advisory document that only encourages voluntary compliance,[47] and not a policy that has been put into effect with full funding and enforcement. The plan also called for public-private partnerships; this resulted in meetings and more advisory documents, but no settled policy.

C. Financial security statutes

Another effect of the 9/11 attacks was the suspicion that foreign terrorists may try to infiltrate the American economy via strategic transactions that could destabilize financial networks and the American economy at large.[48] This possibility was addressed in the Foreign Investment and National Security Act of 2007,[49] which has its own definitions of "critical infrastructure" and "critical technologies" as things that need to be protected from financial manipulation in the interests of national security. The statute defines critical infrastructure as "assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets

[41] *Id*. at 7.
[42] Pub. L. No. 107-56, § 1016(e).
[43] *See* Department of Homeland Security, *NIPP 2013*, *supra* note 39, at 1.
[44] *Id.* at 2.
[45] *Id.* at 8.
[46] *Id*. The report later recommends that such networks be used to coordinate critical infrastructure protection operations by various government agencies and partners in private industry, in addition to being protected in their own right. *Id.* at 13.
[47] *Id.* at 10.
[48] This category of risk eventually evolved into government efforts to prevent cyberattacks on financial systems. *See e.g. FBI Strategy Addresses Evolving Cyber Threat*, FBI NEWS (Sept. 16, 2020), https://www.fbi.gov/news/stories/wray-announces-fbi-cyber-strategy-at-cisa-summit-091620.
[49] Pub. L. No. 110–49, 121 Stat. 246 (2007).

would have a debilitating impact on national security."[50] Note how this definition of critical infrastructure is still tied with national security in a fashion that avoids definition of the protection that critical infrastructure really needs beyond threats to national security. The statute's curious terminology is exemplified by an unashamedly tautological definition of the related term "critical technologies" as "critical technology, critical components, or critical technology items essential to national defense."[51]

The Foreign Investment and National Security Act granted new enforcement powers to the Committee on Foreign Investment in the United States (CFIUS),[52] which is made up of high-ranking federal officials and has the authority to cancel attempts by foreign parties to invest in or acquire American businesses.[53] Regardless of neglecting to define critical infrastructure succinctly, the statute instructed CFIUS to conduct detailed investigations of any proposed foreign investment in an American company that was associated with the concept.[54] In the years since, the CFIUS regularly describes its investigations as focused on national security risks with lesser focus on critical infrastructure, and with no further definition for either concept, which contributes to running accusations that the committee is nontransparent and unaccountable.[55] This is another manifestation of inconsistent terminology leading to little utility for citizens who may wish to review the conduct of government agencies in determining whether critical infrastructure is truly being protected.

D. Telecommunications and cyber networks

Old directives on matters of critical infrastructure from Bill Clinton and George W. Bush were superseded by Presidential Directive PDD-21 from President Barack Obama in 2013. This document expanded the definition of critical infrastructure somewhat as including "distributed networks, varied organizational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations."[56] This new directive reflected that era's increasing appreciation of the importance of computerized networks, outlining some enhanced plans for sharper coordination among government agencies and private businesses, with a plan to focus on research and development in the search for defense strategies,[57] but with no further attempts to refine the basic terminology.

That same year, Obama added enforcement powers on the matter of cybersecurity for critical infrastructure via an executive order that required sharing of relevant information among

[50] *Id*. at § 2(a)(6).
[51] *Id*. at § 2(a)(7).
[52] *Id*. at § 3(k)(1).
[53] The CFIUS had originally been authorized by an Executive Order in 1975, but its responsibilities were not codified until this statute in 2007. EXEC. ORDER NO. 11,858, 3 C.F.R. § 990 (1975). The committee consists of the Secretary of State, Secretary of the Treasury, Secretary of Defense, Secretary of Commerce, United States Trade Representative, Chairman of the Council of Economic Advisers, Attorney General, and Director of the Office of Management and Budget.
[54] Pub. L. No. 110–49 at § 7(b)(2)(F).
[55] *See* Ioannis Kokkoris, *Assessment of National Security Concerns in the Acquisition of U.S. and U.K. Assets*, 12 J. OF NATL. SECURITY L. & POLICY. 349, 374 (2022).
[56] *See* Office of the President of the United States, *Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience* (Feb. 12, 2013), https://www.cisa.gov/sites/default/files/2023-01/ppd-21-critical-infrastructure-and-resilience-508_0.pdf, at 1.
[57] *Id*. at 6-8.

agencies,[58] and instructed the National Institute of Standards and Technology (NIST) to develop a framework that could be adopted by business and industry.[59] Beyond its basic definition of critical infrastructure, repeated from previous statutes and regulations, Obama's executive order instructed various federal agencies to collaborate on finding a viable definition of the term by identifying vulnerable infrastructure and by "apply[ing] consistent, objective criteria in identifying such critical infrastructure."[60] This appears to have never happened comprehensively and succinctly, as the subsequent policy definitions described below will show.

Per the requirement in Obama's 2013 executive order, the NIST published its own plan the following year, with another attempt to conceptualize critical infrastructure in the form of advice to businesses and organizations on assessing cybersecurity risks to their properties and operations.[61] The NIST advised organizations on strategies to achieve economic security via technological and scientific standards, and took on cybersecurity protocols during this period.[62] The institute advised all relevant businesses and organizations to implement its guidelines, but with no working definition of critical infrastructure beyond that given in Obama's executive order.[63] The definition or structure of the desired public-private partnerships also remained vague and idealistic, resting upon pronouncements like "The critical infrastructure community includes public and private owners and operators, and other entities with a role in securing the Nation's infrastructure."[64] The NIST plan was immediately criticized for its idealistic goals which would be prohibitively expensive to implement, and relatively few organizations have formally adopted them.[65]

Researchers have found that simply recommending public-private partnerships is not necessarily good governance. For those partnerships to be effective and influential, they must be designed with a strategy that includes distinct goals and known participants invited from industry and civil society, and what they are expected to accomplish.[66] Poor planning and definition often doom public-private partnerships to obscurity, with their outcomes relegated to advisory documents and uninfluential recommendations for idealistic projects.[67] When corporate leaders

---

[58] *See* EXEC. ORDER NO. 13,636, 78 Fed. Reg. 11,737 (Feb. 12, 2013), at § 4.
[59] *Id.* at § 7.
[60] *Id.* at § 9(a).
[61] *See* National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, report (Feb. 12, 2014), https://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.
[62] *See* Hamed Taherdoost, *Understanding Cybersecurity Frameworks and Information Security Standards – A Review and Comprehensive Overview*, 11 ELECTRONICS 2181, 2189-2190 (2022).
[63] *See* National Institute of Standards and Technology, supra note 61, at 3.
[64] *Id.*
[65] *See* Dimensional Research, *Trends in Security Framework Adoption: A Survey of IT and Security Professionals*, white paper (March 2016), http://www.tenable.com/press-releases/nist-cybersecurity-framework-adoption-linked-to-higher-security-confidence-according. According to Dimensional Research, 70% of the businesses and organizations surveyed for the study found the NIST recommendations to have merit, but less than 50% planned to implement them due to high implementation costs and unclear benchmarks. *See Id.*
[66] *See* Derick W. Brinkerhoff & Jennifer M. Brinkerhoff, *Public-Private Partnerships: Perspectives on Purposes, Publicness, and Good Governance*, 31 PUBLIC ADMIN. & DEV. 2, 3-4 (2011). American citizens have long had an ambivalent and skeptical attitude toward public-private partnerships, despite their regular promotion by policymakers, reflecting shifting levels of trust in government and the business sector. *See generally* Eric J. Boyer and David M. Van Slyke, *Citizen Attitudes Towards Public–Private Partnerships*, 49 AM. REV. PUB. ADMIN. 259 (Apr. 2019).
[67] *See generally* Lena Brogaard & Ole Helby Petersen, *Public-Private Partnerships (PPPs) in Development Policy: Exploring the Concept and Practice*, 2018 DEVELOPMENT POLICY REV. 729-730 (Sept. 2018). On the matter of poor planning and uninfluential recommendations, *see* Alexsander Yandra, Bunga Chintia Utami & Khuriyatul Husna, *Distortion of Government Policy Orientation in Public-Private Partnership (PPP)*, 4 POLICY & GOVERNANCE REV.

are invited, such partnerships tend to take on a corporate structure and end up reflecting the goals of the companies that have contributed.[68] This repeats the pattern of critical infrastructure being defined by private operators seeking government funds and other special favors, which does not necessarily correspond to national security goals.[69]

The politics of protecting critical infrastructure became more contentious, if not more distinct, after Obama left office. This is especially true for telecommunications networks, given increasing awareness of their crucial impact on economic and social health.[70] President Donald Trump's apparent interest in infrastructure (critical or otherwise) and its effects on national security resulted in several new statutes focused on the concept during his administration and that of his successor Joe Biden. In 2018, Trump signed into law the Cybersecurity and Infrastructure Security Agency Act,[71] which created a new office within the Department of Homeland Security called the Cybersecurity and Infrastructure Security Agency (CISA). That agency's mission statement readily adopts the term critical infrastructure, announcing that the CISA "provides guidance to support state, local, and industry partners in identifying critical infrastructure needed to maintain the functions Americans depend on daily."[72]

The CISA was instructed to coordinate the protection of various industrial sectors that had been named in the National Infrastructure Protection Plan back in 2013.[73] The new agency lists 17 industrial sectors, two of which are Information Technology and Communications, as deserving of protection because their "assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[74] This definition is once again copied directly from the Patriot Act.[75] Also, recall that Communications and Information Technology were previously combined into one sector by the Department of Homeland Security, and there are other inconsistencies between that department's list of 18 sectors and its new child agency's 17 sectors.[76]

In its sector-specific report focused on Communications, the CISA divided that sector into Broadcast, Cable, Satellite, Wireless, and Wireline components;[77] though it relies on rather

---

40, 45 (2020); Anika Guevara, PUBLIC-PRIVATE PARTNERSHIPS: AN INNOVATIVE SOLUTION FOR A DECLINING INFRASTRUCTURE, 47 THE URBAN LAWYER 309, 324 (2015).

[68] *See* Gudrid Weihe, *Public-Private Partnerships: Addressing a Nebulous Concept*, conference paper, 10th International Research Symposium on Public Management, Glasgow, Scotland (2006), https://research.cbs.dk/files/59064824/ppp_approaches_guri_16.pdf, at 9.

[69] *See* KOKAS, *supra* note 4, at 25.

[70] *See* Cramer, *Entity of the State*, *supra* note 5, at 65.

[71] Pub. L. No. 115-278, 132 Stat. 4168 (2018).

[72] *See* Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Security and Resilience," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

[73] *See supra* note 39 and accompanying text.

[74] *See* Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[75] Pub. L. No. 107-56, § 1016(e).

[76] *See supra* note 29 and accompanying text. The inconsistencies between the two agencies include a sector called "National Monuments and Icons" which is only addressed by Homeland Security and not by CISA, while the reverse is true for a sector called "Government Facilities". Homeland Security lists "Telecommunications" while CISA lists the less distinct "Communications", with different definitions of the networks and media types involved as well as their various interconnections.

[77] *See* United States Department of Homeland Security, *Communications Sector-Specific Plan: An Annex to the NIPP 2013*, report (2015), https://www.cisa.gov/sites/default/files/publications/nipp-ssp-communications-2015-508.pdf, at 6-7.

shallow definitions of the sector like "provid[ing] products and services that support the efficient operation of today's global information-based society," and rests on the fact that this sector is useful for other sectors.[78] The government's penchant for circular reasoning can also be seen in the statement "Virtually every element of modern life is now dependent on cyber infrastructure. As a result, our Nation's economic and national security relies on the security of the assets and operations of critical communications infrastructure."[79]

In the corresponding sector-specific report focused on Information Technology, one can find similarly high-level definitions like "[this sector] provides products and services that support the efficient operation of today's global information-based society."[80] Later, there is some more specificity but another lapse into circular reasoning with "products and services that support the efficient operation of today's global information-based society and are integral to the operations and services provided by other critical infrastructure Sectors."[81] These sector-specific documents then largely repeat the concerns of the original National Infrastructure Protection Plan advanced by the Department of Homeland Security.[82]

Influenced by both America's growing awareness of the importance of telecommunications networks and political rhetoric on economic or security threats from China,[83] Trump issued an executive order in 2019 barring any American telecom service company from importing equipment from foreign firms that have been deemed threats to national security.[84] While most of the executive order dwells on real or imagined threats, and instructs a wide variety of federal officials on how to determine the nature of those threats, the order mentions critical infrastructure several times. For example, an import transaction can be forbidden by the government if it "poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States."[85] Trump's order does not attempt to define critical infrastructure and refers the reader to Obama's 2013 order on the same topic, and cites a section of that older order that merely instructed various federal agencies to collaborate on finding a definition of that same term.[86]

Given the prevalence of, and public concerns about, cyberattacks and other hacking exploits against corporate systems in the preceding years, Congress passed a new statute in 2022 that required companies to report such incidents to the government within 72 hours.[87] The precisely titled Cyber Incident Reporting for Critical Infrastructure Act[88] focused on industrial sectors that had been designated as critical infrastructure by President Obama in his 2013 directive. Those included telecommunications and information technology, among several others. The new statute

---

[78] *Id.* at 3.
[79] *Id.*
[80] *See* United States Department of Homeland Security, *Information Technology Sector-Specific Plan: An Annex to the NIPP 2013*, report (2016), https://www.cisa.gov/sites/default/files/2023-01/nipp-ssp-information-technology-2016-508%20%281%29.pdf, at 1.
[81] *Id.* at 2.
[82] *See supra* note 39 and accompanying text.
[83] See KOKAS, *supra* note 4, at 81.
[84] *See* EXEC. ORDER NO. 13,873, 84 Fed. Reg. 22,689 (May 15, 2019).
[85] *Id.* at § 1(B).
[86] *Id.* at § 5(b). The reference to Obama's order is to EXEC. ORDER NO. 13,636 at § 9; see also *supra* note 58 and accompanying text.
[87] *See* Michael T. Borgia, "The Cyber Incident Reporting for Critical Infrastructure Act of 2022: An Overview," blog post, Davis Wright Tremaine LLP (May 18, 2022), https://www.dwt.com/blogs/privacy--security-law-blog/2022/05/cyber-incident-reporting-act-2022.
[88] Pub. L. No. 117-103, 136 Stat. 59, § 101 *et seq.* (2022).

required the Cybersecurity and Infrastructure Security Agency to manage such information for entities that are likely to be targeted by malicious actors, and for which disruptions would cause damage to national security, public health, or the economy.[89]

For present purposes, the key addition of this statute is that the CISA, which had previously been an office to coordinate information and build partnerships with private industry, now had enforcement powers (usually in the form of administrative sanctions) against companies that failed to report such information in a timely fashion.[90] This is the first notable statutory requirement for enforcement against malicious actors in the critical infrastructure sphere since the Homeland Security Act of 2002, perhaps illustrating the ineffective recommendations for voluntary cooperation in all the intervening plans and directives.

The various statutes addressing critical infrastructure in recent years, though not necessarily refining its definition, have also enabled federal agencies to address new issues that arose during the COVID-19 pandemic, such as disruptions to the supply chain for needed telecom network equipment,[91] and maintaining emergency communications systems,[92] with the attendant regulatory documents continuing to mention critical infrastructure frequently but pointing back to the usual older documents for vague definitions of the term. Despite frequent calls for various public-private partnerships and for government agencies to develop a working definition of such infrastructure, the original bare-bones definition from the Patriot Act in 2001 continues to be used into the 2020s.

E. Federal trade and foreign investment regulations

The Trump Administration's trade wars with competing nations have resulted in some of the most viable definitions of critical infrastructure, but those have not yet moved beyond the esoteric realm of export/import restrictions, which themselves have also become entangled with vague conceptions of national security. Back in the 1980s, the Reagan Administration objected to the drift in foreign investment reviews from pure international trade and finance into the realm of national security concerns.[93] This objection did not turn out to be influential, because the opposite has happened with frequent references to both national security and critical infrastructure in financial and trade regulations.

The first appearance of national security in the realm of trade regulations was in a 1975 executive order from President Gerald Ford, establishing the aforementioned Committee on Foreign Investment in the United States (CFIUS), which reviews the impact of foreign investments in American companies.[94] National security is also a primary topic in the Export Administration Act of 1979, which governs the review of exports by the Department of Commerce.[95] A partial

[89] *See* Borgia, *supra* note 87.
[90] Pub. L. No. 117-103, § 2244.
[91] *See* Federal Communications Commission, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, Notice of Proposed Rulemaking, WC Docket No. 18-89, 85 F.R. 48134 (Aug. 10, 2020); United States Department of Commerce, *Securing the Information and Communications Technology and Services Supply Chain*, interim final rule, Docket No. 210113-0009, 86 F.R. 4909 (Jan. 19, 2021).
[92] *See* Cybersecurity and Infrastructure Security Agency, *Agency Information Collection Activities: Telecommunications Service Priority System*, Notice of Proposed Rulemaking, Docket No. CISA-2023-0008, 88 F.R. 21203 (Apr. 10, 2023).
[93] *See* Congressional Research Service, *The Committee on Foreign Investment in the United States*, *supra* note 29, at 7.
[94] EXEC. ORDER NO. 11,858, 3 C.F.R. § 990 (1975). *See also supra* note 53 and accompanying text.
[95] 50 U.S.C. §§ 2401-2420; *see particularly* § 2404.

update to that statute, the Export Control Reform Act of 2018,[96] adds telecommunications networks to the effort to protect national security via export controls, characterizing such networks as "emerging and foundational technologies that… are essential to the national security of the United States."[97]

Meanwhile, the responsibilities of the CFIUS are currently codified in several different statutes, one of which features another tautological definition of the problem the committee is supposed to address: "The term 'national security' shall be construed so as to include those issues relating to 'homeland security,' including its application to critical infrastructure,"[98] which in turn includes "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[99] The reader may recognize this definition as once again copied directly from the Patriot Act.[100] Here, national security requires protecting critical infrastructure, and critical infrastructure is something with impacts for national security. This may be the most in-depth description of either term in any federal trade statute, regardless of its indistinctness.[101]

Perhaps the most extensive appearance of critical infrastructure in a finance-oriented statute is in the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2018,[102] which is the latest statute to govern the operations of the CFIUS. This statute received bipartisan support given recent evidence that nations sometimes invest in the private companies of rival nations as a tactic for gaining economic power or infiltrating security networks.[103] State-owned enterprises in non-capitalist or semi-Communist countries are believed to be involved in such tactics to an increasing extent.[104] For the first time, a government agency was instructed to consider critical infrastructure at a level of importance and specificity similar to that for national security.[105] The CFIUS was previously a rather obscure information management office, but the 2018 statute gave it additional investigative responsibilities and the ability to inform national security officials of solicitations from foreign investors who may be interested in gaining access to American technology and infrastructure for suspicious reasons.[106] The CFIUS can prohibit the transfer of funds earmarked for such transactions or impose sanctions on parties that entered into suspicious transactions that have been completed.[107] The committee can also advise the President to forbid any merger of a foreign firm with an American firm if it would "result in foreign control of any United States business."[108]

---

[96] 50 U.S.C. §§ 4811-4852 (2018).
[97] *Id*. at § 4817(a)(1).
[98] This text is from a 1988 addendum, known as the Exon-Florio Amendment, to the Defense Production Act. 50 U.S.C. § 4565(a)(1).
[99] *Id*. at § 4565(a)(5).
[100] Pub. L. No. 107-56, § 1016(e).
[101] *See* Cramer, *Entity of the State*, *supra* note 5, at 75.
[102] Pub. L. No. 115-232, 132 Stat. 1636, § 1701 *et seq.* (2018).
[103] *See* Harry G. Broadman, *CFIUS under Biden Just Got Tougher*, FORBES, Sept. 30, 2022, https://www.forbes.com/sites/harrybroadman/2022/09/30/cfius-under-biden-just-got-tougher/?sh=7d18c05d1a49.
[104] *See* Congressional Research Service, *The Committee on Foreign Investment in the United States*, *supra* note 29, at 6.
[105] *See* KOKAS, *supra* note 4, at 31.
[106] *See* Olivia Rosenzweig, *The Political Underpinnings of U.S. Foreign Investment Policy*, THE REGULATORY REVIEW, Oct. 5, 2022, https://www.theregreview.org/2022/10/05/rosenzweig-the-political-underpinnings-of-u-s-foreign-investment-policy/.
[107] Pub. L. No. 115-232, § 1718(4)(A).
[108] *Id*. at § 1702(a)(4)(B)(i).

The CFIUS has also been instructed to take action against any transaction that would enable foreign influence or control over critical infrastructure in telecommunications, with the agency's regulations defining that term as any "telecommunications service or information service" as defined in the Communications Act of 1934, plus any public Internet exchange point, any undersea cable, and any data center.[109] This may seem like a powerful incentive to focus on foreign financial shenanigans designed to disrupt telecom networks, but the citation to the Communications Act instructs the CFIUS to oversee everything in the realm of modern communications. Whether this is workable for a relatively small committee remains to be seen.

The FIRRMA statute includes several requirements related to critical infrastructure, but once again rests upon the running political definition of the term from the Patriot Act with no appreciable enhancements: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[110] The statute also addresses suspicious activity, requiring action against transactions from any country "that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect United States leadership in areas related to national security;"[111] while action should be taken when such parties seek to invest in any American company that "owns, operates, manufactures, supplies, or services critical infrastructure,"[112] or provides knowledge and information thereof.[113] Once again the definition of critical infrastructure descends into tautological references to infrastructure that happens to be critical, with the usual inability to separate the concept from national security. The statute also contains no instructions on how to determine if a given infrastructure system could be targeted by suspicious financial players.

Interestingly, the FIRRMA statute acknowledges that the term critical infrastructure suffers from an indistinct definition, with the provision "Any definition of 'critical infrastructure' established under any provision of law other than this section shall not be determinative for purposes of this section."[114] In other words, different government agencies are expected to have their own definitions of the term, and the operations of the CFIUS will hopefully not be disrupted by the uncertainty of others. Hence, different federal agencies and departments are expecting each other to succinctly define the term, and to date none of them have done so.

The difficulty, or perhaps bureaucratic confusion, of defining critical infrastructure can be seen in a regulatory order from the Department of the Treasury, the Secretary of which is a member of the CFIUS.[115] That order lists a whopping 28 industrial sectors that qualify as critical, six of which are associated with telecommunications and/or information technology.[116] The Treasury

---

[109] 31 C.F.R. § 800, Appendix A, ¶ i. *See also* Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064 (1934) at § 3(a)(2).

[110] Pub. L. No. 115-232 at § 1703(5). The FIRRMA statute also uses the term *critical technology*, which is largely defined in the interests of military defense. *Id.* at § 1703(6). The Patriot Act definition of *critical infrastructure* is found at Pub. L. No. 107-56, § 1016(e).

[111] Pub. L. No. 115-232 at § 1702(c)(1).

[112] *Id*. at § 1703(4)(B)(iii)(I).

[113] *Id*. at § 1703(4)(D)(ii)(I)(cc).

[114] *Id*. at § 1703(4)(B)(vi).

[115] *See* United States Department of the Treasury, *The Committee on Foreign Investment in the United States (CFIUS)*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius.

[116] *See* United States Department of the Treasury, *Treasury Releases Final Regulations to Reform National Security Reviews for Certain Foreign Investments and Other Transactions in the United States*, press release (Jan. 13, 2020), https://home.treasury.gov/news/press-releases/sm872.

Department's list of sectors tilts largely toward utilities and the military,[117] making it more specific than the corresponding lists from the Department of Homeland Security but also with many more entries. Thus, more and more industrial sectors are being added to the definition of critical infrastructure by more and more government agencies, but the core term itself remains elusive.

F. State statutes

During the post-9/11 period, individual states aligned themselves with the nationwide goals of the Patriot Act, and its focus on preventing terrorist attacks on critical infrastructure, by instituting their own efforts to shore up energy and transportation systems. Also reflecting national trends, those efforts were usually accompanied by policies that prevented citizens from reviewing their effectiveness,[118] given the prevailing national attitude about the sensitive nature of national security-related efforts.[119]

However, since about 2015, the states have diverged significantly from the federal perception of critical infrastructure. Per recent political trends with impacts at the local level, the protection of critical infrastructure is also being addressed by states, but with a definition that does not comport with federal statutes in either terminology or spirit. In the states, meddling with critical infrastructure is becoming a matter of criminal prosecution, and primarily for American citizens. Whereas federal agencies keep adding more and more industrial sectors to critical infrastructure, the states are moving in the opposite direction, with fewer sectors but expanding lists of supposedly crucial items within those sectors. This further illustrates the perils of inconsistent definitions of a matter that policymakers at various levels are trying to address with a certain sense of urgency.

A wave of popular protests against large fossil fuel pipeline projects in the mid-2010s resulted in a plethora of state statutes that sought to prosecute environmental protesters who damaged or disrupted critical infrastructure, which in turn was usually described as fossil fuel installations and occasionally other types of networks like telecommunications or electrical service.[120] Many of those state statutes are adapted directly from model legislation concocted by the American Legislative Exchange Council (ALEC), a think tank funded by corporations and industrial consortia. Among other lobbying activities, ALEC writes model legislation under a theme of free market principles and states' rights, and these models are often presented to state lawmakers alongside lobbying efforts to pass them for the benefit of industry.[121]

The six sectors affiliated with telecommunications and/or information technology are titled Internet protocol or telecommunications service; Certain internet exchange points; Submarine cable systems; Submarine cable landing systems; Data center at a submarine landing facility; and Satellite or satellite systems servicing the Department of Defense. The Treasury Department's list also includes "Technology providers in the Significant Service Provider Program" but it is unclear in the document which type of *provider* to which this prefers.

[117] *See* Congressional Research Service, *The Committee on Foreign Investment in the United States*, *supra* note 29, at 16-17.

[118] *See* Reporters Committee for Freedom of the Press, *Homeland Security and Anti-Terrorism Measures*, https://www.rcfp.org/open-government-sections/l-homeland-security-and-anti-terrorism-measures/.

[119] *See infra* notes 132-137 and accompanying text.

[120] *See* Cramer, *Envirodemic*, *supra* note 14, at 85-86.

[121] The ALEC website regularly uses the phrase "limited government, free markets, [and] federalism" to describe its philosophy. *See e.g.* American Legislative Exchange Council, *About ALEC*, https://www.alec.org/about/. For information on the group's ties to lawmakers and industry leaders, *see also* Mike McIntire, *Conservative Nonprofit Acts as a Stealth Business Lobbyist*, N.Y. TIMES (Apr. 21, 2012), http://www.nytimes.com/2012/04/22/us/alec-a-tax-exempt-group-mixes-legislators-and-lobbyists.html?ref=politics&_r=0.

ALEC formulated a generic bill called the Critical Infrastructure Protection Act in 2018,[122] which has since been passed with just minor modifications by several states and targeted at environmental protesters.[123] Some states highlighted the apparent importance of the concept by placing the key term directly in statute titles, such as West Virginia with its Critical Infrastructure Protection Act.[124] There is sufficient evidence that these state statutes are influenced by lobbying from industry,[125] indicating the perils of relying on vested interests to define crucial systems that may or may not need protection from government.

IV. The framing and transparency of critical infrastructure

How policymakers define a term (or not) has an impact on public understanding of the issue at hand. A term that is inconsistently defined but promoted as an important matter of politics and security, as is the case with critical infrastructure in American law, must then be processed via framing strategies performed subconsciously by citizens, or by the media as an intermediary. Such framing strategies may not lead to public understanding, and if not, there are negative impacts on the transparency and accountability of government actions toward the issue in question.

A. Political and news framing

There has been a long tradition of research on the framing of political issues. In essence, how an issue is "framed" by whoever is describing it can influence another person's understanding of that issue. An ordinary person uses mental shortcuts, or "frames," to break down a complex issue into comprehensible parts, but those shortcuts are themselves influenced by the source of the information, be it a peer, teacher, or political leader.[126] The specific phenomenon of news framing by journalists and anchorpersons also has a long research tradition. A news media outlet will explain a complex issue to the audience with its own shortcuts and simplifications, and those arise from explicit or implicit editorial guidelines that are themselves influenced by the political, economic, or personal outlooks of editors and media managers. Another influence is the media outlet's perceptions, right or wrong, of what the audience supposedly wants.[127] Overall, the news media both influences and is influenced by the audience as well as the political milieu in which reporters operate.[128]

---

[122] *See* American Legislative Exchange Council, *Critical Infrastructure Protection Act* (2018), https://www.alec.org/model-policy/critical-infrastructure-protection-act/.

[123] *See* Cramer, *Envirodemic*, *supra* note 24, at 85-86. For a direct comparison of the language in the ALEC draft legislation with that in various state statutes, *see* Gabrielle Colchete & Basav Sen, *Muzzling Dissent: How Corporate Influence over Politics Has Fueled Anti-Protest Law*s, white paper, Institute for Policy Studies (Oct. 2020), https://ips-dc.org/wp-content/uploads/2020/10/Muzzling-Dissent-Anti-Protest-Laws-Report.pdf, at 14-18.

[124] West Virginia Critical Infrastructure Protection Act, H.B. 4615, Reg. Sess. (W.Va. 2020).

[125] *See* Susie Cagle, *"Protesters as Terrorists": Growing Number of States Turn Anti-Pipeline Activism into a Crime*, THE GUARDIAN (July 8, 2019), https://www.theguardian.com/environment/2019/jul/08/wave-of-new-laws-aim-to-stifle-anti-pipeline-protests-activists-say.

[126] *See* Fernando R. Laguarda, *Think of an Elephant? Tweeting as 'Framing' Executive Power*, 8 LEGISLATION & POLICY BRIEF 32, 42-43 (2019).

[127] *See* Claes H. de Vreese, *News Framing: Theory and Typology*, 13 INFO. DESIGN J. 51, 55 (2005).

[128] *See* Dennis Nguyen & Erik Hekman, *A 'New Arms Race'? Framing China and the U.S.A. in A.I. News Reporting: A Comparative Analysis of the Washington Post and South China Morning Post*, 7 GLOBAL MEDIA & CHINA 58, 60-61 (2022).

Meanwhile, there are further framing effects as individuals try to comprehend politicized terms that are both dramatic and indistinct. Psychologists have found evidence that vague terms or poorly defined risks encourage a subconscious reliance on framing strategies to avoid uncertainty. Furthermore, this can lead to a misperception of the importance of the original issue that the person is trying to comprehend.[129] When the vague term carries connotations of importance – such as "critical" in the present discussion – this may cause the person to over-evaluate the importance of the concept despite the vague definition that has been given by leaders.[130]

There has been no previous published research on how critical infrastructure is framed by the media or by politicians. However, lessons can be learned from extensive research on this process for national security. As described herein, statutes and regulations addressing critical infrastructure typically pair that term with national security. The latter generates much more public discussion and media coverage, so the framing of national security is relevant here because of the rhetorical connection and the fact that such framing informs public understanding of policy.

Researchers have found that national security is typically framed simultaneously as both worthy of widespread public concern, and as ineligible for further discussion because it is supposed to remain secret – under the care of trustworthy government officials with no need for anyone to ask questions. This leads to confusion among ordinary people on how to react to perceived threats and whether one can rely upon government officials to do so on behalf of the citizenry; while conceding the secrecy of such operations to the government with little evidence that doing so is justified.[131]

After the 9/11 attacks, researchers found a profound shift in the framing of national security, with the concept often being framed as a zero-sum game in opposition to civil liberties. In other words, if you want national security you must give up civil liberties like privacy, because having both is impossible. That oppositional dichotomy can affect how people interpret the importance of both national security and civil liberties depending on their faith in government protection from threats.[132] American politicians have also been known to frame national security in terms of preventing harm to the public (especially from terrorist attacks) or to the nation's standing in the world, often without evidence that such harms are likely, as a means of deflecting public discussion of the details of military operations.[133]

These effects have also been measured in the behavior of politicians and policymakers themselves, as they may become susceptible to their own framing strategies when deciding on policies related to national security and then explaining them to constituents.[134] This has resulted in severe over-reliance on national security frames by policymakers hyping the importance of their own initiatives, to the point at which national security – once a purely military term – has been

---

[129] *See* Kristine M. Kuhn, *Communicating Uncertainty: Framing Effects on Responses to Vague Probabilities*, 71 ORGANIZATIONAL BEHAVIOR AND HUMAN DECISION PROCESSES 55, 58-60 (1997).

[130] *See* Eyal Gamliel & Hamutal Kreiner, *Applying Fuzzy-Trace Theory to Attribute-Framing Bias: Gist and Verbatim Representations of Quantitative Information*, 46 J. OF EXPERIMENTAL PSYCHOLOGY: LEARNING, MEMORY, AND COGNITION 497, 498-499 (2020).

[131] *See* Marlen Heide & Jean-Patrick Villeneuve, *Framing National Security Secrecy: A Conceptual Review*, 76 INTL. J. 238, 245-248 (2021).

[132] *See* J.C. Barone & Karen Swan, *Effects of Media Framing on Beliefs and Values Concerning Detainees, Civil Liberties, and National Security after 9/11*, 3 J. OF THE RSCH. CTR. FOR EDUCATIONAL TECH. 13, 18-21 (2007).

[133] *See* Matthew Levinger, *A Core National Security Interest: Framing Atrocities Prevention*, 3 POLITICS AND GOVERNANCE 26, 28-29 (2015).

[134] *See* Steven B. Redd & Alex Mintz, *Policy Perspectives on National Security and Foreign Policy Decision Making*, 41 POLICY STUDIES J. 11, 29-30 (2013).

applied to everything from environmental protection to public health to anti-corruption.[135] Politicians with establishmentarian tendencies have also been found susceptible to the influence of framing techniques used by elite constituencies when they discuss national security issues, and those elites are in turn influenced by their particular choices of media outlets; anti-establishmentarian politicians display similar tendencies to adopt the frames of populist social movements.[136] In the words of one legal researcher, "If everything is about national security, nothing is about national security."[137]

One prominent example of this process in telecommunications involves the Chinese equipment companies Huawei and ZTE. Those two firms are often described as threats to American national security, though such threats (usually described in terms of possible surveillance on behalf of their government) have not been definitively proven and the threats have been conflated with trade disputes and American export/import strategy.[138] This type of framing of foreign competition aligns with larger conceptions of national security as being necessary to maintain America's standing on the world stage, with the desired dominance of American firms symbolizing a larger conception of national security.[139] This article argues that the same framing patterns can be seen for critical infrastructure and its ties to the telecommunications sector, for which specific challenges of governmental accountability follow.

B. Transparency and comprehensibility

Government transparency is often attributed to the availability of official agency documents, or the lack thereof. However, there is another conception of transparency that is tougher to conceptualize. Documents may in fact be available but turn out to be useless for the average citizen due to terminology that is incomprehensible or poorly defined, while merely announcing final agency decisions but with no information available on how those decisions were reached.

Researchers have found that vague and non-transparent justifications from government for its own decisions can result in unquestioning trust in those leaders and belief in the wisdom of their decisions.[140] This can encourage politicians to under-explain complex matters to the public.[141] Concrete terminology, in the form of direct references to the observer's experiences and knowledge, is beneficial for that observer's understanding,[142] but is often missing from agency

---

[135] *See* Jacques deLisle, *When Rivalry Goes Viral: COVID-19, U.S.-China Relations, and East Asia*, 65 ORBIS 46, 67 (2021).

[136] *See* David S. Meyer, *Framing National Security: Elite Public Discourse on Nuclear Weapons During the Cold War*, 12 POLITICAL COMMUNICATION 173, 190-191 (1995).

[137] *See* Chad P. Bown, *Export Controls: America's Other National Security Threat*, 30 DUKE J. OF COMPARATIVE & INTL. L. 283, 286 (2020).

[138] *See* Cramer, *Entity of the State*, *supra* note 5, at 73-74.

[139] *Id.* at 72.

[140] *See* Heide & Villeneuve, *supra* note 131, at 248-250. Heide & Villeneuve make this distinction in their examination of the established "elite governance frame" that has been examined by previous researchers.

[141] *See* Simone Chambers, *Behind Closed Doors: Publicity, Secrecy, and the Quality of Deliberation*, 12 J. OF POLITICAL PHILOSOPHY 389, 409-410 (2004).

[142] *See* Anli Xiao, Yan Huang, Denise S. Bortree & Richard D. Waters, *Designing Social Media Fundraising Messages: An Experimental Approach to Understanding How Message Concreteness and Framing Influence Donation Intentions*, 51 NONPROFIT AND VOLUNTARY SECTOR QUARTERLY 832, 834-835 (2022); Claude H. Miller, Lindsay T. Lane, Leslie M. Deatrick, Alice M. Young & Kimberly A. Potts, *Psychological Reactance and Promotional Health Messages: The Effects of Controlling Language, Lexical Concreteness, and the Restoration of Freedom*, 33 HUMAN COMM. RSCH. 219, 225-226 (2007).

documents. Governmental complexity can also be detrimental to public acceptance of policy decisions, and uncertainty over which agency or department is the primary authority on a given issue can damage the usefulness of the resulting official documents.[143]

Recall from the previous sections that four Presidents, officials from at least three different cabinet-level departments, and Congress via a multitude of statutes have contributed inconsistent definitions of critical infrastructure and ever-expanding lists of industry sectors contained within it, and plentiful documents discussing the topic are available. However, quantity does not equal quality. A large quantity of government documents that can be reviewed by the public will not aid with comprehension or believability, if those documents are repetitive, unorganized, or give the impression of poor coordination among higher authorities.[144] This can also lead to an undesirable public focus on big-picture themes and vague ideals, as opposed to in-depth review of the details of real policy actions.[145]

Furthermore, if any policy decisions are made on behalf of a poorly defined term like critical infrastructure, the Administrative Procedure Act would require notifying citizens of how and why such decisions were made.[146] Such documents, even if they exist, are unlikely to be fully informative if they dwell on repetitive and indistinct terminology. Meanwhile, decision-making documents could also qualify for disclosure to citizens under the Freedom of Information Act,[147] though under that statute a given document does not need to be disclosed to a requesting citizen if it qualifies for several exemptions, one of which covers any document that agency personnel deem to be relevant for national security.[148] This could further reduce the transparency and availability of agency documents pertaining to critical infrastructure, which as shown herein is often mentioned in league with national security.

Thus, it can be concluded that the American government talks about protecting critical infrastructure on a regular basis but has depended upon a definition that has become more diffuse over time. Nor has the protection of critical infrastructure at a comprehensive level been codified in a statute, and such processes remain in the realm of nonbinding agreements and non-transparent agency regulatory procedures. As a result, the government says that it protects critical infrastructure on behalf of the people, but there is no practical way for the people to review those efforts and to determine whether they are effective.

V. Network control and critical infrastructure

Whereas the United States has not yet enshrined consistently-defined critical infrastructure protection into law, its biggest competitors in the international telecommunications marketplace have. This section of the article will introduce such efforts in the European Union and China, showing that those polities have at least nailed down a consistent working definition of the term and concrete plans to identify risks and formulate protection strategies.

---

[143] *See* Albert Meijer, *Understanding the Complex Dynamics of Transparency*, 73 PUBLIC ADMIN. REV. 429, 432 (2013).
[144] *See* OMRI BEN-SHAHAR AND CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE 101-106 (2014).
[145] *Id.* at 94-95.
[146] 5 U.S.C. §§ 551-559 (1946).
[147] 5 U.S.C. § 552 (1966).
[148] *Id*. at § 552(b)(1).

A. The European Union

In 2004, the European Council passed a resolution to develop a plan for protecting critical infrastructure, which eventually developed into the European Programme for Critical Infrastructure Protection (EPCIP) two years later.[149] The program is described as an "all-hazards approach" to addressing risks that could affect infrastructure at the Europe-wide level, rather than locally or nationally.[150] All member states of the European Union and the larger European Economic Area are required to incorporate the provisions of the EPCIP into their national laws.[151] The 2006 directive avoided any attempt at a definition of critical infrastructure at first and required the formation of "expert groups" to determine risks and best practices.[152] Unlike in the United States, the expert groups in the EU were able to solidify a Europe-wide definition of critical infrastructure as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions," and this definition appears consistently in all EU documents.[153]

In a noticeable distinction from the United States, the EU originally avoided lengthy lists of industry sectors that may contain critical infrastructure and identified only two such sectors: Energy and Transport. The 2006 directive included a procedure to add more sectors in the future, and predicted that ICT (Information and Communications Technologies) would become a priority later.[154] In a 2013 review of the program, ICT was added to the previously defined Energy sector due to the many interconnections between the two.[155] In another distinction from the United States, all member states of the European Union have a designated representative (known as a "contact point") to oversee local implementation and attend regular European Commission meetings on the topic.[156]

The EU program was updated in 2020, with a change in terminology to "the resilience of critical entities."[157] The terminological change represents a new paradigm with a focus on designing infrastructure to withstand risks from the start, while addressing not just systems but

[149] Commission of the European Communities, Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final.
[150] *Id.* at §§ 2.2-2.3. The term "all-hazards approach" is used regularly by emergency officials around the world and denotes a focus on contingency planning for all parties and acknowledges the possibility of multiple emergencies happening simultaneously.
[151] European Commission, *European Critical Infrastructure*, https://home-affairs.ec.europa.eu/whats-new/european-critical-infrastructure_en.
[152] COM(2006) 786 final at § 4.3.
[153] European Commission, Council Directive on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection, Council Directive 2008/114/EC (Dec. 8, 2008), at art. 2(a). While the United States has a widely used policy definition of *critical infrastructure* that is often copied from the Patriot Act, this article has argued throughout Section III *supra* that this definition is so vague as to have been critiqued by multiple Presidents, while agencies face no requirements on whether to adopt it directly, modify it slightly, or ignore it altogether. The result is both vagueness and inconsistency, which have to a certain extent been avoided by the European Union.
[154] *Id.* at art. 3(3).
[155] European Commission, Commission Staff Working Document on a New Approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures More Secure, SWD(2013) 318 final (Aug. 28, 2013).
[156] Council Directive 2008/114/EC, at art. 10.
[157] European Commission, Directive of the European Parliament and of the Council on the Resilience of Critical Entities, COM(2020) 829 final, 2020/0365 (COD) (Dec. 16, 2020).

their operators as well.[158] By this point in time, the temptation to add more and more industry sectors to what is "critical" had set in; the 2020 update lists ten sectors, one of which is titled Digital Infrastructure.[159] According to researchers, these developments represent a move away from a pure focus on resisting terrorism to addressing other systemic risks like climate change, but they also represent a certain mission creep that complicates matters of oversight and enforcement.[160] The EU most recently updated the program again in 2022, instructing member states to renew their focus on critical entities with war as an additional threat; the new directive contains a direct reference to "Russia's aggression against Ukraine."[161] The directive was rushed into effect after revelations that Russia was suspected of sabotaging cross-Europe natural gas pipelines as a wartime strategy.[162] By this point, digital and telecom-based infrastructure had also received top priority in EU critical infrastructure law, alongside the original energy and transport.[163]

B. China

For decades, China has prioritized the construction and control of infrastructure as a matter of national policy for purposes of economic growth and political power. This is particularly evident in China's construction of transportation, energy, and telecommunications systems in its weaker neighboring countries, which are promoted as a gesture of regional goodwill but are then integrated physically and economically into Chinese networks.[164] This policy focus has been applied to China's own internal infrastructure systems as well, with development being a key component of the nation's economic growth strategy.[165] More recently, China has extended this focus to the particular infrastructure sectors deemed to be "critical" for the nation's political and economic goals.

Unlike in the United States, Chinese policy on critical infrastructure development and protection is codified directly in national law. While China has rules for many different industrial sectors, of interest here is a specific body of regulations focused directly on telecommunications and data security. Those matters are covered by the Cybersecurity Law of 2017;[166] that statute supports the most recent rules on the matter, known as Regulations on the Security and Protection

---

[158] *See* Christer Pursiainen & Eero Kytömaa, *From European Critical Infrastructure Protection to the Resilience of European Critical Entities: What Does It Mean?*, 8 SUSTAINABLE AND RESILIENT INFRASTRUCTURE 85, 87-90 (2023).
[159] COM(2020) 829 final, at 3.
[160] *See* Pursiainen & Kytömaa, *supra* note 158, at 93-94.
[161] European Commission, Directive of the European Parliament and of the Council on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC, EU 2022/2557 (Dec. 14, 2022).
[162] *See* Alexandra Brzozowski & Kira Taylor, *EU Vows to Draw Up Plans to Protect Critical Infrastructure*, EURACTIV (Oct. 5, 2022), https://www.euractiv.com/section/defence-and-security/news/eu-vows-to-draw-up-plans-to-protect-critical-infrastructure/.
[163] *See* Molly Killeen, *EU Commission Seeks Accelerated Defence of Critical Infrastructure*, EURACTIV (Oct. 18, 2022), https://www.euractiv.com/section/digital/news/eu-commission-seeks-accelerated-defence-of-critical-infrastructure/.
[164] *See* Selina Ho, *Infrastructure and Chinese Power*, 96 INTL. AFFAIRS 1461, 1468-1471 (2020).
[165] *See* Pravakar Sahoo, Ranjan Kumar Dash & Geethanjali Nataraj, *Infrastructure Development and Economic Growth in China*, white paper, Institute of Developing Economies (Oct. 2010), https://www.researchgate.net/profile/Pravakar-Sahoo/publication/49175190_Infrastructure_Development_and_Economic_Growth_in_China/links/540431d60cf2c48563b04d61/Infrastructure-Development-and-Economic-Growth-in-China.pdf, at 7-10.
[166] *See* Arendse Huld, *Critical Information Infrastructure in China – New Cybersecurity Regulations*, CHINA BRIEFING (Aug. 30, 2021), https://www.china-briefing.com/news/critical-information-infrastructure-chinas-new-regulations/.

of Critical Information Infrastructure, which were enacted in 2021. This regulatory document defines the topic as (in translation) "important network infrastructure, information systems, etc., in important industries and sectors such as public telecommunications and information services, energy, transportation, water, finance, public services, e-government, national defense, science, technology, and industry, etc., as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people's livelihood, or the public interest."[167]

One key distinction with China's critical infrastructure policy is that it requires those systems and networks to be designed and developed by companies with close ties to the government. This is particularly true in telecommunications and affiliated sectors like smart cities, in which China is an early mover. This directly ties company operations to governmental goals.[168] Notwithstanding western political demonization of the semi-Communist command and control style of current Chinese policy, this is an effective effort to not only protect the nation's own critical infrastructure but also (thanks to integrated international networks) exercise growing influence over the designs and standards of systems used in the United States and elsewhere. For telecommunications in particular, this influence ranges from the economic advantage that may come from setting design standards, to making rival nations wonder if they should be suspicious of Chinese components and protocols, to increasing surveillance and control of data flows.[169] Researchers have also found evidence that the Chinese government has instructed its companies to aggressively seek opportunities to enter other national or regional markets by manufacturing and selling critical infrastructure components.[170]

This process could lead to the destabilization of critical infrastructure in countries that compete with China, including the United States. Previously installed equipment is viewed as a risk that must be replaced at great cost, while the effort to find non-Chinese components can create a level of desperation that leads to rising prices and anticompetitive behavior from manufacturers.[171] An expensive example of this process has already happened in the United States. Due to rising suspicions of security risks, surveillance, and intellectual property theft allegedly perpetrated by the Chinese telecom company Huawei, the Federal Communications Commission has ordered American service providers to remove Huawei components from public networks and replace them with new equipment manufactured in more trustworthy nations. This effort, known colloquially as "rip and replace," was mandated in 2019 and is expected to cost billions of dollars and to take many years.[172] This can be directly attributed to differing policy outlooks on critical infrastructure, particularly America's version which requires private companies that built the infrastructure long ago to play catch-up after the government perceives a new problem.[173] This

---

[167] State Council of the People's Republic of China, Critical Information Infrastructure Security Protection Regulations, No. 745 (2021), at art. 2. The original Chinese version of this regulation can be found at https://www.gov.cn/zhengce/content/202108/17/content_5631671.htm?mc_cid=da5881cf31&mc_eid=a268621911. The translation is from DIGICHINA, https://digichina.stanford.edu/work/translation-critical-information-infrastructure-security-protection-regulations-effective-sept-1-2021/.

[168] *See* KOKAS, *supra* note 4, at 7-8.

[169] *Id.* at 76-77.

[170] *See* Yang Jiang, Aki Tonami & Adam Moe Fejerskov, *China's Overseas Investment in Critical Infrastructure: Nuclear Power and Telecommunications*, white paper, Danish Institute for International Studies (2016), https://www.econstor.eu/bitstream/10419/197634/1/875113524.pdf, at 10.

[171] *See* KOKAS, *supra* note 4, at 84.

[172] *See* Cramer, *Entity of the State*, *supra* note 5, at 85.

[173] *See* KOKAS, *supra* note 4, at 91.

gives a certain amount of power over critical infrastructure to the more forward-looking country with a more distinct policy on the matter, which in this case is China.

C. Comparisons with the United States

The US Department of Homeland Security has noted that "As the Nation's critical infrastructure is largely owned by the private sector, managing risk to enhance security and resilience is a shared priority for industry and government."[174] This may be the American way, but it has led to few tangible results for government-mandated critical infrastructure protection so far. Meanwhile, private corporate owners certainly add expertise and may have the financial incentive to protect their own systems from disruption, but each company's profit motive is unlikely to correspond with national policy goals or even with the motives of other companies attending the same meetings.

In the US, private firms control between 80 and 90 percent of critical infrastructure. Not only is that a very high percentage in its own right, but it is also uncertain due to the vague governmental definition of the term and the tendency of private players to declare their own systems as "critical" in order to attract funding or other government support.[175] There is a related problem for systems that are geared toward consumers and advertised for their benefits in the home. Consumers become less likely to consider the national security implications when they use their favorite devices and networks, but the personal data they generate absolutely has geopolitical consequences.[176] Therefore, rising industry segments like entertainment, personal finance, health care, and smart appliances, all of which are becoming integrated with telecommunications networks and the Internet, face risks similar to those for traditional military and corporate installations.[177]

While other critical systems, especially in the military, have oversight structures and distinct regulations dating back many decades, the same is not true for infrastructure that is dependent on emerging technologies, as is the case for modern telecommunications. This is important because these newer sectors face the same economic and national security risks.[178] This in turn requires a coherent national policy that not only outlines distinct actions to be taken for critical infrastructure protection, but an agreed-upon definition at the highest levels of the American government. Neither of these has yet happened, despite a lot of talk by a plethora of agencies with various levels of connection to the issue.

IIII. Conclusion

Modern military conflicts have increasingly focused on destroying or destabilizing critical infrastructure networks, most notably Russia's attacks on media and telecommunications systems in Ukraine.[179] Protecting such infrastructure requires focused policies to identify such systems and

---

[174] *See* Department of Homeland Security, *NIPP 2013*, *supra* note 39, at 2.
[175] Joel Brenner, *Protecting America's Critical Infrastructure from Cyber Attacks*, speech at Massachusetts Institute of Technology, Internet Policy Research Initiative (Mar. 20, 2017), https://internetpolicy.mit.edu/speech-brenner-infragard-criticalinfra-2017/. *See also* KOKAS, *supra* note 4, at 25.
[176] *See* KOKAS, *supra* note 4, at 76.
[177] *Id.* at 91-92.
[178] *Id.* at 91.
[179] This strategy had been in place since as early as 2014 when pro-Russian separatists sought to secede from Ukraine, and long before Russia launched its organized invasion of the country in 2022. *See* Jack Losh, *Inside Rebel-Held*

the risks they face.[180] As this article has argued, such a focus remains elusive in American policy; as a concept with its own definition and analysis of risks, the country's critical infrastructure remains unprotected from terrorists, invading armies, or even the weather. The United States has unconstructively projected such concerns outward, as critical infrastructure policy, particularly toward China, has been wrapped up in national security arguments posing that country as an economic and/or military threat. This leads to not only tense relations but a shortage of cooperation that could benefit the United States as it strives to identify and protect its own critical infrastructure, including that which is dependent on Chinese components.[181]

Furthermore, this has forced critical infrastructure into the realm of esoteric agency regulations that are valid for their own purposes but have little usefulness as a comprehensive national policy. Unlike the European Union and China, the United States is the only one that does not have critical infrastructure protection codified into law. Instead the US relies on invitational workshops that generate nonbinding resolutions, executive orders targeted at specific and temporary emergencies, and the voluntary framework from the National Institute of Standards and Technology.[182] The US even promotes a gimmicky "Critical Infrastructure Security and Resilience Month" every November.[183] This results in little more than proclamations from leaders to appreciate the issue and the efforts of government agencies that appreciate the same.[184]

Meanwhile, for officials who are tasked with protecting that infrastructure, and concerned citizens overseeing that process, the definition of critical infrastructure has not progressed appreciably beyond the terminology in the 2001 Patriot Act: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[185] The initial reaction to that definition, particularly from President George W. Bush, was to encourage government officials to streamline and solidify that definition,[186] with a similar request from President Barack Obama in 2013.[187] Little noteworthy improvement has happened in the years since.

The United States need not adapt China's semi-Communist command and control strategy toward critical infrastructure, which would be politically impossible. On the contrary, Europe has made more progress on this issue through democratic processes. This article recommends that the United States adapt the strategy of the European Union, which has nailed down a consistent polity-wide definition of critical infrastructure to be used by all governmental and corporate actors, and

---

Ukraine's Palaces of Propaganda, VICE NEWS (Mar. 28, 2016), https://www.vice.com/en/article/neyqa8/inside-rebel-held-ukraines-palaces-of-propaganda.

[180] *See* Carol V. Evans, *Future Warfare: Weaponizing Critical Infrastructure*, 50 THE US ARMY WAR COLLEGE QUARTERLY: PARAMETERS 35, 41-42 (2020).

[181] *See* Andrew Stephen Campion, *From CNOOC to Huawei: Securitization, the China Threat, and Critical Infrastructure*, 28 ASIAN J. OF POLI. SCI. 47, 49-51 (2020).

[182] *See* Jing de Jong-Chen & Bobby O'Brien, *A Comparative Study: The Approach to Critical Infrastructure Protection in the U.S., E.U., and China*, white paper, Wilson Center (Nov. 2017), https://www.wilsoncenter.org/publication/comparative-study-the-approach-to-critical-infrastructure-protection-the-us-eu-and-china, at 9.

[183] *See e.g.* United States Department of Energy, *November is Critical Infrastructure Security and Resilience Month* (Nov. 1, 2019), https://www.energy.gov/oe/articles/november-critical-infrastructure-security-and-resilience-month.

[184] *See e.g.* Office of the President of the United States, *Proclamation 10086—National Cybersecuirty Awareness*, press release (Sept. 30, 2020), https://www.govinfo.gov/content/pkg/DCPD-202000741/pdf/DCPD-202000741.pdf

[185] Pub. L. No. 107-56, § 1016(e).

[186] *See supra* note 38 and accompanying text.

[187] *See supra* note 60 and accompanying text.

has enshrined that definition into law. The EU definition of the term is not necessarily more complex or distinct than the U.S. definition, but it is at least consistent. The EU has also avoided the temptation (until very recently) to crank out longer and longer lists of myriad industrial sectors that qualify as critical. The U.S. should discard all previous agency attempts to list eligible industries, resulting in lists containing up to 28 sectors, and instead rest upon a simpler definition focused on protecting everything equally. Policy should then focus on organizing protection strategies in the event of attacks or natural disasters, while requiring future networks and components to be designed with extra protections from the start. While it may be impossible to not include a list of some industry sectors, the United States should adopt the path originally followed by the EU to keep that list short. As opposed to lengthy lists of industry sectors, the US should focus on system-wide or "all-hazards approach",[188] which treats all infrastructure equally regardless of type or the influence of its corporate managers, and to focus on addressing the weaknesses of current infrastructure and the proactive design of future infrastructure. This in turn could enable a government-wide definition of critical infrastructure to be observed by all relevant federal and state agencies.

Thus far, the United States has fallen behind in such efforts, leaving critical infrastructure, whatever its definition, vulnerable to what may come in the future, while private corporate owners must be convinced to play catch-up if it is even in their financial interests to do so. In the words of researcher Aynne Kokas, an expert on U.S./China trade relations, "In an ideal world, new technologies would spur the development of bespoke protections for their intended users. Instead, amid an illiberal environment for tech sector oversight, users depend on the emergence on new laws and protections, which have been slow to come, have a limited impact, or, in the worst case, never materialize."[189]

[188] *See supra* note 150 for a definition of "all-hazards approach."
[189] *See* KOKAS, *supra* note 4, at 91.