
Communicating Safety

Open Access Teaching Case Developed for the Tech for Humanity Pathways Minor

Funded by the Andrew Mellon Foundation

Developed by Dr. Katie Walkup

Background

What counts as infrastructure? While some definitions limit infrastructure to designed objects, other conceptualizations expand infrastructure to the networks of humans and technologies that design those objects. The debate carries implications for funding; limiting infrastructure's definition also limits the potential to fund projects addressing education, healthcare, and climate change, to name a few. The debate over infrastructure's definitions also limits our understanding of the groups who are harmed by failing infrastructures, and the ways that infrastructure both causes and compounds inequalities for those groups. Public awareness and media coverage of infrastructure exacerbates this issue; focusing on the tragedy of the incident and the necessity of an investigation into its events limits attention on holding actors accountable for redressing the issue, or of addressing the issue before it becomes a tragedy. This case study explores the issue of infrastructure's definition, entanglement of human and non-human actors, and the communication of resiliency to concerned publics. To do this, the case examines issues of cybersecurity, inadequate and failing infrastructure, precarity, and risk in the 2021 hack of a drinking water system in Oldsmar, FL.

In this case, the hacking of a water treatment plant exposes the concerning inadequacies of critical infrastructure. Investigation reveals that although redundancies in the water treatment plant's system succeeded in preventing further harm, the system was not resilient to cyber intrusion. Further information regarding enhanced security practices adopted by the facility in the wake of the incident has not been forthcoming, leaving stakeholders uncertain about the

safety of the water supply. The case raises questions about risk communication and the public's right to access information about the safety of critical resources.

Focus Questions

- 1) In your opinion, what counts as infrastructure? Why is there so much disagreement over the definition of the term?
- 2) Why are vulnerable groups more likely to be impacted by failing infrastructure? Can you think of any examples where vulnerable groups were exposed to failing or inadequate infrastructural resources?
- 3) Infrastructure is designed to be unnoticed, facilitating our daily activities, like driving to work or school, turning on a tap for water, flipping a light switch, etc. Why do you think we only notice infrastructure when it fails? How does this lack of attention lead to lack of funding?

Case Study

On February 5, 2021, hackers accessed the operating system of a water treatment plant in Oldsmar, FL. They were able to increase the concentration of lye in the city's water to toxic levels—fortunately, the plant was able to identify and correct the problem before the city's drinking water was compromised (Robles and Perlroth, 2021). Media outlets were quick to connect this incident to other cybersecurity threats regarding critical infrastructure, including a hacker gaining remote access to a San Francisco water facility in January 2021 (See Dowd, 2021, for example). Or, as Barrett (2021) reports for *Wired*, in 2019, an ex-employee of a Kansas water system was allegedly able to interfere with the process for disinfecting the water supply, potentially impacting residents living in eight counties. Yet after the initial media coverage over the Oldsmar incident, and related incidents, public officials have offered little information on the measures put in place to prevent such an action from recurring.

How the Hack Succeeded

In the Oldsmar case, media coverage agrees that the access point for the hack was through an unused remote-access program that remained on the plant's computers and was still able to be logged into (i.e., Lyngaas, 2021). A joint report authored by the FBI, DHS, U.S. Secret Service, and the Pinellas County Sheriff's Office (2021) goes into more detail, noting that in addition to this old remote-access program, all computers used by water plant personnel were connected

to the water treatment system and used the 32-bit version of the (no longer supported) Windows 7 operating system. Further, all computers shared the same password for remote access and appeared to be connected directly to the internet without any type of firewall protection installed (n.p.).

Given these technical inadequacies, an article in *The Economist* (2021) compares the Oldsmar attack to “the equivalent of jimmying open a loose window” (n.p.). Interestingly, most media coverage of the case focuses on a larger narrative about lack of funding for critical infrastructural resources, rather than the actual lack of cybersecurity at the water plant itself.

What Counts as Infrastructure

This case coincides with a larger public and increasingly partisan debate about what resources comprise infrastructure. For some, infrastructure only constitutes roads and bridges. Others define infrastructure more broadly; resources integral to supporting life, like healthcare, mitigating climate change, or in this case, ensuring the safety of the nation’s water supplies. Infrastructure’s definition has always been subject to interpretation. As *The Atlantic’s* Peter A. Shulman (2021) writes, the Eisenhower administration borrowed the French term to mean any resource necessary for warfare. After this coining, what Shulman (2021) calls infrastructure’s “metaphorical utility” was applied to “housing, hospitals, schools, public services, functional legal systems, and governmental bureaucracies” (n.p.). The narrowing of infrastructure to mean only roads, bridges, or other objects is a more recent linguistic phenomenon. Shulman (2021) notes that focusing on infrastructure’s physical components ignores its socioeconomic necessities. Using the narrower definition of infrastructure in the Oldsmar case would have addressed the computers using unsupported operating systems and perhaps the lack of a firewall. This narrow definition of infrastructure would not have addressed the education needed for the water treatment plant operators to understand why they should restrict remote access programs and strengthen password security, two recommendations made by the FBI, DHS, U.S. Secret Service, and Pinellas County Sheriff’s Office (2021) after the incident.

Much like the roads and bridges that facilitate movement without being objects of attention themselves, infrastructure facilitates everyday life without being observed. This lack of observation has consequences for how much funding critical resources receive. This lack of funding intersects with the precarity of the population impacted by the failing. Failing or inadequate infrastructures are more likely to impact vulnerable groups. As rhetorical scholars

Johnson and Johnson (2020) write in an overview of precarity studies, those impacted by precarious infrastructure are most likely to include people of color, those with disabilities, women, LGBTQIAA+ individuals, and immigrants, as well as the elderly and displaced (n.p.). Johnson and Johnson (2020) note that “an investigation of precarity, then, is an investigation into uneven distributions of risk, exclusion, and exploitation that reproduce inequality” (n.p.). These infrastructural inequalities compound, as Shivaram and Tomer (2018) demonstrate for the *Brookings Institution*: they provide several examples of failing infrastructure impacting these populations, including inadequately designed roads resulting in increased pedestrian fatalities, increasing numbers of contamination in public water supplies, and built environments vulnerable to the impacts of climate change.

Focus Questions

- 4) What types of images are brought to mind when you hear words like “cybersecurity,” “hacking,” or “cyberthreat”? Do these images match the story of the Oldsmar case?
- 5) Describe some of the human and technological actors in the Oldsmar case. Where did each actor go wrong? Are there some failures where you can’t decide what is human error and what is technological error?
- 6) What type of infrastructural repairs would have been needed to stop the Oldsmar hack from happening? Would these repairs have been recognized under the narrower “roads and bridges” definition of infrastructure?
- 7) Why do you think that most media (both national and local) coverage of the incident did not encompass the actual results of the federally-authored report? Do you think that there might have been more coverage if the infrastructural failures had been more technological in nature?
- 8) Do you think the jointly-authored report is specific enough about the failures at the Oldsmar water treatment plant? Are you concerned that other water resources will be made vulnerable by this information? Does the public have a right to know this information?

Themes from the Case Study

Theme 1: Infrastructure and Precarity

Failing or inadequate infrastructure creates and reinforces precarity. Tragedy after tragedy shows how vulnerable groups are most likely to be exposed to and harmed by infrastructural inequality: levee failures during Hurricane Katrina in 2005, flammable building material used to construct affordable housing in the Grenfell Tower fire in London in 2017, the Flint water crisis, and recently, the Texas electrical grid inadequately designed to withstand cold weather (Steffy, 2021). These tragedies all lay bare the necessity of funding for even the narrowest definition of what counts as infrastructure. The debate over the definition of infrastructure distracts from the discussion regarding whom infrastructure serves.

Discussion Questions

- 1) If you saw two people arguing over what counted as infrastructure, how would you redirect their attention to focus on the human costs of inadequate or failing infrastructure?
- 2) Do you think infrastructure contributes to systemic inequality or systemic racism? If so, how would you describe the issue to someone who did not understand the role of infrastructure in producing inequality?

Theme 2: Risk Communication

Tragedies caused by infrastructure failings create headlines and help us understand the invisible or unobserved systems that facilitate daily life. As Johnson and Johnson (2016) write about infrastructural mechanisms, generally their “workings appear stable and absolute if they appear at all” (n.p.). Only a system glitch can render infrastructures available for scrutiny (n.p.); but the headlines that accompany glitches also create uncertainty. Walsh and Walker (2016) find that “individual perception of uncertainty is powerfully connected to risk perception” (p. 76). The uncertainty surrounding a glitch becomes a risk, resulting in calls for investigation. Yet in this case, addressing the uncertainty surrounding the vulnerabilities of the Oldsmar facility and numerous other water systems only addresses part of the risk. The calls for investigation present an easier goal than addressing the nation’s risky water supply and may distract public attention from efforts to implement the latter objective.

Discussion Questions

- 1) Can you think of any other tragedies that seemed to end with a call for investigation? Was the investigation ever completed? What were its findings? While the investigation was being completed, did the actor allegedly at fault for the tragedy seem to make an effort to prevent subsequent tragedy, or did they seem to wait for the investigation to be completed?
- 2) Should infrastructures be invisible or unnoticeable? What are the affordances and consequences of their invisible design?

Theme 3: Cybersecurity and Resilience

In 2018, the Environmental Protection Agency (EPA) required national drinking water systems serving more than 3300 people to develop or update risk and resilience assessments as well as emergency response plans by a series of staggered due dates in 2021. The final deadline for drinking water systems to submit emergency response plans was December 31st, 2021 (United States Environmental Protection Agency, 2021). Risk and Resilience Assessments include guidelines on system monitoring practices, so the managers of drinking water systems should be aware of their vulnerability to “malevolent acts,” as they are termed by the EPA. Yet, protocols like risk assessments may not be able to solve issues of cybersecurity. For example, the January 2021 COVID-19 relief plan included \$10 billion to address cybersecurity, with a \$9 billion investment in the Cybersecurity and Infrastructure Security Agency (CISA) (Miller, 2021). Critical infrastructure requires investment, but which agencies provide that investment is, as this case has demonstrated, a contentious debate.

Discussion Questions

- 1) Given what you know about the case, what type of risk assessment would you design to ensure that other drinking water systems would not repeat the errors of the Oldsmar facility?
- 2) The creation of CISA implies that infrastructure security should be linked with cybersecurity. Do you agree with the association? Can you think of a different government agency that should handle infrastructural concerns?

Theme 4: Safety and Security

The Oldsmar water plant hack exposed obvious security flaws. In an article for *ProPublica*, Elkind and Gillum (2021) sum them up: lack of firewall, shared passwords, and outdated software (n.p.). However, the messaging regarding incident response has been positive. Elkind and Gillum (2021) quote Oldsmar's mayor, who states, "This is a success story", two weeks after the incident. The mayor may be referring to the redundancies built into the system to prevent an intruder from poisoning the water supply. Yet, a system's successful response to an intrusion is different from a system's ability to prevent the intrusion in the first place. Moreover, the scant media coverage does little to assure Oldsmar residents that the water plant's security flaws have been fixed. On February 8th, the Pinellas County Sheriff stated that "the public was never in danger" (qtd. in "A cyber-attack on an American water plant rattles nerves," 2021). Besides this assurance, little coverage has been devoted to explaining how and why the public was never in danger, and specifically why the public will never be in danger in the future. As an article in *The Economist* quips about these uncertainties, "The residents of Oldsmar may not be so sanguine" (n.p.). Elkind and Gillum (2021) of *ProPublica* note that Oldsmar public authorities have refused to comment on an open investigation.

Discussion Questions

1) If you were a resident impacted by the Oldsmar water plant hack, what information would you want to see from public authorities to be convinced that your water was safe? While commenting further might jeopardize an open investigation, does the public have a right to receive information about events that impact their safety? If so, how much information? What information might be risky to expose?

References

- "A cyber-attack on an American water plant rattles nerves." (2021, February). *The Economist*. Retrieved from: <https://www.economist.com/united-states/2021/02/090a-cyber-attack-on-an-american-water-plant-rattles-nerves>
- Barrett, B. (2021, April). The threat to the water supply is real—and only getting worse. *Wired*. Retrieved from: <https://www.wired.com/story/threat-to-water-supply-is-real-and-only-getting-worse/>
- Cybersecurity & Infrastructure Security Agency. (2021). Additional information about cybersecurity breach in Florida. Massachusetts Department of Environmental Protection.

Retrieved from:

<https://www.mass.gov/service-details/cybersecurity-advisory-for-public-water-suppliers>.

Dowd, K. (2021, June). A hacker gained access to a Bay Area drinking water facility. *SFGate*.

Retrieved from:

<https://sfgate.com/crime/article/sf-bay-area-water-treatment-facility-hack-16260655.php>

Elkind, P., & Gillum, J. (2021, March). America's drinking water is surprisingly easy to poison.

ProPublica. Retrieved from: <https://www.propublica.org/article/hacking-water-systems>

Johnson, N.R., & Johnson, M.A. (2020). Precarious data: Affect, infrastructure, and public education. *Rhetoric Society Quarterly*, 50(5), 368-382.

Johnson, N.R., & Johnson, M.A. (2016). Glitch as infrastructural monster. *Enculturation: A Journal of Rhetoric, Writing, and Culture*. Retrieved from:

<https://enculturation.net/glitch-as-infrastructural-monster>

Lyngaas, S. (2021, February). Florida hack highlights security shortages in US water sector.

CyberScoop. Retrieved from:

<https://www.cyberscoop.com/florida-water-hack-oldsmar-challenges/>

Miller, M. (2021, January). Biden includes over \$10 billion in cyber, IT funds as part of COVID-19 relief proposal. *The Hill*. Retrieved from:

<https://thehill.com/policy/cybersecurity/534323-biden-includes-over-10-billion-in-cyber-it-funds-as-part-of-covid-19>

Robles, F., and Perloth, N. (2021, February). 'Dangerous Stuff': Hackers tried to poison water supply of Florida town. *The New York Times*. Retrieved from:

<https://www.nytimes.com/2021/02/08/us/oldsmar-florida-water-supply-hack.html>

Shivaram, R., and Tomer, A. (2018, May). Do our infrastructure systems put people at risk?

Brookings Institution. Retrieved from:

<https://www.brookings.edu/blog/the-avenue/2018/05/10/do-our-infrastructure-systems-put-people-at-risk/>

Shulman, P. A. (2021, July). What *infrastructure* really means. *The Atlantic*. Retrieved from:

<https://www.theatlantic.com/ideas/archive/2021/07/what-does-infrastructure-mean/619419>

Steffy, L. (2021, June). What is wrong with the Texas grid? *Texas Monthly*. Retrieved from:

<https://www.texasmonthly.com/news-politics/what-is-wrong-with-the-texas-grid>

Walsh, L., & Walker, K.C. (2016). Perspectives on uncertainty for technical communication scholars. *Technical Communication Quarterly*, 25(2), 71-86.