



# Understanding Cyberinfrastructure Adoption: The Effect of Social Norms and Culture

Natalie Shanaa, Leora Kalili, Morgan Venn, JJ Wu and Kerk Kee

COM 329: Capacity Building in Organizations, in Fall 2018– Chapman University; Orange, CA



## Introduction

Cyberinfrastructure (CI) is a word that is used often but lacks an exact definition. The US National Science Foundation (NSF) refers to this term as an information technology system that has advanced and powerful capabilities. Margaret Leinen, head of NSF's Geosciences, had once said that cyberinfrastructure will "expand the horizons of what scientist can study and understand". People are always computing, they use cyber infrastructure for research that supports advanced acquisition, storage, management, data integration, and many more. But, how does one adopt cyberinfrastructure and in what ways do social norms and cultural values drive people to adopt and use cyber infrastructure? This project looks at how norms and values influence people's attitudes and actions towards cyber infrastructure. One can see people using cyber infrastructure for capacity building purposes in order to help prosper their organization. Cyberinfrastructure main purpose is to tackle problems in all science and engineering disciplines and is vital for an organization's longitudinal success.

## Literature Review

Cyberinfrastructure is brought into businesses for capacity building purposes to help the organization grow and prosper. It is appealing due to its big, collaborative, and leading-edge lure as well as its quick speed to get the task done fast yet efficiently (Participant 3, Page 8). Along with the fast work pace, social norms and cultural values play a role in compelling one to use cyberinfrastructure. Since people want the development of science to be more open, cyber infrastructure allows people to work collaboratively while still improving technology. This current study seeks to understand how and why people incorporate and use cyberinfrastructure. Knowing what cyberinfrastructure is and following how it drives people to adopt the idea of cyberinfrastructure leads to our questions: RQ1: How does one adopt cyberinfrastructure? RQ2: In what ways does social norms and cultural values drive people to incorporate and use cyberinfrastructure?

## Methodology

This poster analyzes occurrences of social norms and cultural values influencing cyberinfrastructure by coding 20 transcripts conducted with domain scientists, technologists, and administrators involved in XSEDE (Extreme Science and Engineering Discovery Environment, the largest supercomputing consortium in the US). Following a semi-structured protocol, interviews were conducted by phone and some in-person. The participants were from a diverse range of institutions, and organizations all with some expertise in cyberinfrastructure from around the United States. We then identified key social norms and cultural values that influence organizations towards adopting cyberinfrastructure. By applying the grounded theory coding techniques, we analyzed the interviews that resulted in the findings presented in this poster.

## Findings

Throughout the coding process, three common themes were found within:

Strategies	Culture	Social Norms
<p>Cyber infrastructure refers to computing systems, advanced data reports, and how it links communities, environments, and people. As explained by data analyst (Participant 9) the material objects that make up cyberinfrastructure would be the high-performance computing cluster which allows one to do research. Little by little people are becoming more aware and are adapting to the idea of incorporating cyberinfrastructure. Strategically in order to adopt cyber infrastructure you need funders and GAPS.</p> <p>The most important part of all organizations are funders. As mentioned in previous tools; you need an array of funders from different backgrounds and with different mentalities to support your nonprofit and overall goal. If you do not have somebody fulling your organization/idea, then you can't keep infrastructure going and the materials, maintenance, repair and replacement costs won't be there. Also they are important because they are ones who provide money and resources in order to get your project off the ground. Moreover, without money and funding one will be unable to access technology.</p> <p>Secondly, GAPS is very important for one to be able to strategically adopt cyber infrastructure. GAPS is the mentality that each researcher and coworker each holds their own objectives and goals. We are able to build even stronger connections and collaborations across all areas by taking up a team-based approach. It's GAPS that further lead to collaboration between institution leaders and students further promoting a successful institution with a clear vision in mind for great change.</p>	<p>Slowly the common ideology and culture is revolved around behavioral practices. Specifically, data organizational skills and background knowledge of the topic at hand, further allowing research interaction.</p> <p>Culturally you need to do a lot of good work in order to produce a lot of human capital. In other words you need diversity. As explained by Participant 7, the goal is to do a lot of good work and produce a lot of human capital for advanced computing. He explained that one does not simply adopt existing tool even though one pride themselves of spreadsheets but rather work with others further bringing the organization together. One must be able to work with technologists and hire interns to develop tools that they use in order to further allow a wide spread of knowledge from not only people who have been in the business forever but millennials as well.</p> <p>Cultures tend to adapt as technology advances. In these advanced countries, it is unheard of for a company not to have built their own secure network. The whole culture adapts to the trend of having a secure network because if they don't, they are considered weak and penetrable. In other words, they have a higher chance of getting hacked with a weak security system. The most technologically advanced cities in the world are Seoul, Hong Kong, Tokyo, San Francisco, and Sweden. All of the companies in these cities are competing against each other. Now imagine if one of them had a weak security system compared to the rest. The more technologically advanced companies would be able to break through the weak companies cyber walls and steal their information for their own personal growth. They might even go as far as to publish their information as their own. This is why security is important and it is crucial to be as technologically advanced as your competitors.</p>	<p>One of the main social norms that help adopt cyberinfrastructure is the ability to visualize components as well as any sort of kind of desktop or sensor networks since a lot of data streams collected from things like social media. Data sharing is a very important factor as it encompasses ideologies. Such factor can actually enhance your cyber infrastructure because it makes everyone be on the same page and agree on the same policies. You're working environment is a community so having everyone be on the same page and share and agree on the same policies and data enhances your organizational growth and cyber infrastructure.</p> <p>People innately need to compartmentalize: which means to separate into isolated compartments or categories, and this is done with technology. "We do a lot of sharing, but we also have compartmentalization. And that compartmentalization comes out of that people want to have ownership of their data and be able to do their work before others can, you know, do similar kinds of work" (Participant 13, Page 2). People's perceptions about security tends to drive cyber infrastructure. In many cases, people who hold valuable information avoid using iCloud due to security reasons. Many also speculate on the security level of Google for storing personal information. Although it is a fast and easy way to store and share information, some think that a password protected website isn't sufficient. This is a viable claim because hackers with the right skillset may be able to break through the security walls. These skeptical people use other methods for storing information such as a personal computer and hard drive. Most companies even hire a professional IT person to create a stronger security network.</p> <p>A social value held by a majority of the world is the fostering and advancement of education. With the improvement of technology, people are now able to work collaboratively with like-minded individuals on projects and research. Allen Lee explains how "People should be able to build on each other's work." (Participant 9, Page 3) and that new developments in cyber infrastructure are allowing this to occur. In fact, cyber infrastructure is the hardware that drives the development of coding, an example of a free, widely used technology that anyone can develop and share. Yet more importantly, "this kind of technology has a huge potential for revolutionizing undergraduate education" (Participant 8, Page 3). Will explains that cyberinfrastructure technology allows students to visualize what our eyes can't naturally see such as electromagnetic fields. In virtual space students can act with the electro-magnetic fields and therefore gain a greater understanding.</p>

## Conclusion

From analyzing transcripts of interviews conducted with technologists, scientists and administrators, we were able to identify a strategy and some key cultural values and social norms that influence the adoption of cyberinfrastructure. From using a strategy that focuses on funding and a strong mentality that relies on GAPS, collaboration amongst institutions and people are more likely to be successful. When it comes to cultural values, establishing a culture of sharing and strong security is vital to making sure cyberinfrastructure can be adopted and implemented securely. When it comes to social norms, we were able to notice similarities of importance when it came to successfully incorporating cyberinfrastructure. All organizations require strong policies and even more when it comes to cyberinfrastructure as honest and secure collaboration is needed for it to succeed.

## References

Corbin, J. M., & Strauss, A. (1990). *Basics of qualitative research: Grounded theory procedures and techniques*. Thousand Oaks, CA, US: Sage Publications, Inc.

Kerk, K. F. (2017). *Adoption and diffusion*. In C. Scott, & L. Lewis (Eds.), *International encyclopedia of organizational communication*. Hoboken, NJ: Wiley-Blackwell.

Kee, K. F., & Schrock, A. S. (in press). *Best social and organizational practices of successful science gateways and cyberinfrastructure projects*. Future Generations Computer Systems McKinsey, Venture Philanthropy Partners (2001). *Effective Capacity Assessment for Non-Profit Organizations*. [http://www.vppartners.org/sites/default/files/reports/full\\_rpt.pdf](http://www.vppartners.org/sites/default/files/reports/full_rpt.pdf)

McKinsey, Venture Philanthropy Partners (2001). *Effective Capacity Assessment for Non-Profit Organizations*. [http://www.vppartners.org/sites/default/files/reports/full\\_rpt.pdf](http://www.vppartners.org/sites/default/files/reports/full_rpt.pdf)