CSAW'22 Policy Competition

Background Paper for Cyber Policy and Strategy for Connected Communities

General Background

The world is integrating digital devices across all aspects of urban and rural infrastructure. This ubiquitous computing infrastructure, commonly known as Internet of Things (IOT), is a universe of devices, that when combined with machine learning and other automated analytics, enable humans to gather, process, store, and analyze data in order to enable users to identify inefficiencies and manage scarce resources with greater care. These are usually referred to as "smart" technologies.

While IOT is largely invisible to the general public, its integration into daily life is increasing modern societies dependence on cyberspace within critical functions. As such, the risk of "smart" technology being disrupted due to poor configuration of malicious activities may increase the likelihood of small systems having a big national security impact.

We use the term "Connected Communities" rather than "Smart Cities" intentionally. Smart City terminology that is popular in the media and in corporate marketing literature overlooks that "smart technologies are being integrated across societies, and not just in urban environments. As such, continuing to reflect on "smart cities" rather than "connected communities' creates a misperception that could create a lag in policy being aligned with the technical realities. The focus of this policy competition is to consider national security concerns across the spectrum of "smart" technologies in the context of the communities within which they are being adapted.

US Teams: National Security Concerns

This sub-topic is designed for students within the US who may be more familiar with US policy, strategy and governance processes. International students are welcome to undertake this sub-topic, but in their presentations, they must align to the US cybersecurity governance ecosystem.

Digital integration of "smart" devices is moving away from linear relationships due to unidentified and unexpected connections, causing each connected community to have its own set of vulnerabilities, in turn leading to its own set of harms for that community. Through the increase of digital integration, the vulnerabilities, risks, and harm being introduced to connected communities is cause for major concerns to local and national security. Teams considering this sub-topic will focus on national security concerns of the integration of "smart" technology across communities. Teams should identify how hyper-connected system-of-systems are integrated into society. Identify how connectivity within and between systems changes the structure of risk and the impact of harm in society.

International Teams: US-China Technological Competition Policy from an International Perspective

This topic is for teams competing internationally. We want to understand trends and drivers and your vantage point of the current US-China technology competition for the global "smart" technology market.

Connected communities are an area of strategic focus for the Chinese government per their 14th Five Year Plan and Made in China 2025. Emerging technologies such as 5G, IOT, AI, encryption, and cloud computing are strategic technologies at the center of great power competition. Within the

connected community concept, we find the convergence of several emerging technologies and national security mission areas presenting new cybersecurity risks. While often challenged by Western countries, China's Made in China 2025 and China Standards 2035 are not only pushing China into the modern age, but making them a global leader of it. Even though the Chinese government is called out for their tactics such as the extreme surveillance of their citizens, the progress that technology companies are making in China is radically changing and benefiting the lives of Chinese citizens. Through actions such as this, China is working towards their goal of becoming the world's economic leader by 2030. Financial reasoning and device efficiency raise challenges for nations in deciding where to purchase "smart" devices from.

Main Research Questions

Competitors must choose **one** subtopic. They must address **all** questions within that subtopic, as listed below.

National Security Concerns

- Chose one critical infrastructure sector (public transport, telecom, energy, agriculture, finance). How are "smart "technologies being integrated?
- In what ways will the cybersecurity picture change for critical infrastructure as "smart" technology proliferates?
- In what ways will cyber resilience be affected by implementation of fully digital ecosystems?
- What are some worthwhile policy solutions to mitigate risk?

US-China Technological Competition Policy from an International Perspective

- Why or why not would your national government, municipal governments or private sectors choose to purchase or not purchase Chinese technological equipment?
- What benefit would your country have in partnering with the US vs. China?
- What risk mitigation measures will your country use to manage risk from potential security risks of Chinese equipment and balance the relationship with the US if desired?

What Needs to be Covered

Between the Policy Brief and Presentation, the bullet points below **must** be addressed.

For both Sub-topics:

- **Funding:** What mechanisms will guarantee long-term funding? What tools, resources, infrastructure, or people need to be funded? How does funding account for expansion and updates?
- **Public-Private Cooperation:** How does your policy incentivize private sector cooperation? What weight should be accorded to private sector considerations during strategic decision making?
- **Short- & Long-Term Goals:** What is the timeframe for your policy? How does your policy assess short- and long-term success in accomplishing its objectives?
- **International Relations:** How will your country prioritize and maintain international relations and interests between the US and China?
- **Privacy Concerns:** How does your policy interact with the privacy laws at local, state, and federal level?

A note to CSAW Competitors

This brief is a starting point for your policies and ideas. It contains things you must address, but scope, definitions, and specific content will come from you. We encourage bold, creative policies that force deep thought and discussion. Leaders from academia, government, and private industry may see your work, and thus we encourage you to prioritize your policies by thinking through their practicality and implementation for a range of stakeholders. Please reach out to the CSAW committee at csaw-policy@nyu.edu with any questions.

Useful References

China Mobile, 2019. “5G Application Scenarios White Paper.” *Smart Cities World.* https://www.smartcitiesworld.net/whitepapers/whitepapers/white-paper-5g-application-scenarios

Cyberspace Solarium Commission, 2020. “Cyberspace Solarium Commission Final Report.” https://www.solarium.gov/report

“The Future of Cities.” *KPMG*, December 3, 2021. https://assets.kpmg/content/dam/kpmg/au/pdf/2021/the-future-of-cities.pdf

Halegoua, Germaine. 2020. “An Introduction to Smart Cities.” In *Smart Cities*, 1-42. Cambridge: MIT Press. https://mitpress.mit.edu/9780262538053/.

Hass, Ryan. 2021. “How China Is Responding to Escalating Strategic Competition with the US.” *Brookings,* March 1, 2021. https://www.brookings.edu/articles/how-china-is-responding-toescalating-strategic-competition-with-the-us/

M. St.John-Green and T. Watson, "Safety and security of the smart city – when our infrastructure goes online," *9th IET International Conference on System Safety and Cyber Security (2014)*, 2014, pp. 1-6, doi: 10.1049/cp.2014.0981.