Cybersecurity Politics in Egypt:

Manipulating Uncertainty

Jaden Walker

CYSE201S

Diwakar Yalpi

2/16/2025

Cybersecurity Politics in Egypt: Manipulating Uncertainty

In today's ever-changing technology world, cybersecurity extends beyond technical defenses by having the potential to influence political strategies and gain societal control. This article focuses on Egypt, exploring how cybersecurity practices serve as tools for both state and non-state actors to manipulate uncertainty, by impacting political processes and citizen engagement.

This article focuses on how cybersecurity practices are employed by actors in Egypt to manipulate the societal and political landscape. The hypothesis that is posed is that both governmental bodies and opposition groups strategically use cybersecurity measures to create ambiguity while aiming to control narratives and influence public perception.

The study employs the qualitative research methodology by utilizing case studies and content analysis. It uses data sources including official government communications, social media content from activist groups, and reports from international watchdog organizations. I like this approach because it allows for a complete perspective, and avoids generalizations from "one side".

The analysis shows that the Egyptian government participates in fear mongering by implementing cybersecurity policies that restrict internet access and monitor online activities. This further creates an environment of uncertainty and fear among citizens because of the lack of connection to the outside world. Conversely, opposition activists use encryption and anonymous communication channels to distribute information aiming to counter state narratives and mobilize support for various causes. The yin-yang of these actions contributes to a dynamic where uncertainty is a deliberate tool used by all parties to achieve political objectives. It also is a replication of almost every country's "civil problems" with an example of the mantra of a cop

killing a black boy. The state media would often times try to hide the footage and put out a general statement, while activist groups aim to directly punish the officer and have the world see what happened.

I found the relation to key concepts discussed in class to be fitting, including the role of information control in social power structures and the use of technology as a means of political influence. It shows how cybersecurity measures can serve both sides of the coin, as instruments of both oppression and resistance, emphasizing the dual-edged nature of technology in societal contexts.

Marginalized groups in Egypt are disproportionately affected by the state's cybersecurity policies. With an example being the government's surveillance and censorship practices which often target these groups by limiting their access to information and platforms for expression. I would argue that it reinforces existing social inequalities and suppresses dissenting voices which further hinders the pursuit of social justice and equity.

This article, "Manipulating Uncertainty: Cybersecurity Politics in Egypt", sheds light on the complex relationship between cybersecurity and political strategy. It underscores the necessity for a nuanced approach to cybersecurity that considers its potential for both empowering and oppressing different societal groups. I would argue that there should be dedicated research exploring strategies to mitigate the negative impacts of these practices on marginalized populations and enhance the role of technology in supporting inclusive governance.

References:

Manipulating uncertainty: Cybersecurity politics in Egypt | Journal of Cybersecurity |

Oxford academic. (n.d.-c).

https://academic.oup.com/cybersecurity/article/7/1/tyaa026/6137887