Social Implications of U.S. National Cybersecurity Strategy (2023)

Cayden Bass-Hensley

CYSE 425W

Cybersecurity Strategy and Policy

Professors: Bora Aslan

The U.S. National Cybersecurity Strategy (2023) lays out a bold vision for enhanced national resilience in the face of an ever-evolving threat landscape. Nonetheless, the social implications of the strategy reflect complex relations among government policies, citizen responsibilities and social consequences. This analysis looks at the social implications of the strategy, such as social forces which have driven the development of the strategy and cultural forces which will affect the implementation of the strategy.

Social Factors that Lead to Policy Development

Increased reliance on digital technologies and the risks that accompany them underpin the U.S. National Cybersecurity Strategy. Dunn Cavelty et al. (2023) claim that cybersecurity policies are not only technical fixes, they also depend on how people interact and how society is organized. The strategy stands to illustrate responsibility separate from that of the collective. It tries to take some of the burdens off of technology companies and government officials' shoulders.

This transformation is an assumption that everyone would actually follow a strong cybersecurity practice. As Renaud et al. (2023) explain, previous approaches have weighed responsibility too much on the individual and have focused on capabilities that may not exist, considering the gaps in technical competency between demographic groups. As contrasted to past approaches that have been decidedly individualistic, the 2023 Strategy has a strikingly different attitude toward the digital environment in the interest of systemic resilience and equity

Social Consequences of the Policy

The U.S. National Cybersecurity Strategy 2023 has societal implications in all areas and affects sections of the population disproportionately. By safeguarding critical infrastructure, it

prescribes security measures on providers of technology that would certainly assure overall safety but is also likely to result in unintended consequences for citizens at a cost: With more constraints, some communities are paying higher prices for services and continuing to be further marginalized.

Research indicates that cybersecurity policies often fail to recognize the lived experience of at-risk populations holistically. Dunn Cavelty et al., 2023 note, that while systemic approaches are needed, they could inadvertently consolidate wider societal demands without paying adequate heed to local communities, and to the myriad of inequalities that marginalized groups face. The key problem is the creation of corresponding policy frameworks that do not widen existing gaps for digital security outcomes.

Cultural and Subcultural Influences

Reception and effectiveness of the U.S. National Cybersecurity Strategy is framed within the lens of cultural values and sub-cultural practices. It represents the American cultural norms towards freedom, individualism, and market solutions. Ganapati et al. (2023) observe that this may determine how other actors — private companies and people — will react to the strategy's mandates.

Such cultural dynamics also manifest themselves on the basis of generational differences. Younger generations are much more digitally literate and accustomed to online security so are much more likely to comply with the demands of the strategy compared to the older generations, which may find the new security measures difficult to cope with. Additionally, the provisions of the Strategy can give rise to professional subcultures in fields as diverse as health and finance

that, through bespoke approaches, may be either supportive of, or counter to, the provisions of the Strategy, thereby creating possible institutional practice versus national standards conflicts.

Policy Implications and Recommendations

The 2023 U.S. National Cybersecurity Strategy helps create an opportunity in dealing with both the technical and social faces of cybersecurity, including the focus on resilient systems, equal access to digital means, and accountability within the government—still, one step toward more inclusive moves warranted by detailed social views in achieving its full goals.

To make it work better, some suggestions include:

1. Cultivate different levels of technical knowledge through public education programs that lay the foundation for cybersecurity training.
2. Recognize the bounds of individual responsibility such that institutional safeguards should become the first line of defense, particularly for critical infrastructure.
3. Take into consideration the cultural diversity in security practices by providing outreach and support programs between specific communities.
4. Develop targeted aid for vulnerable populations, such as subsidies or incentives to enable low-income families to receive safe technologies.

As Dunn Cavelty et al. (2023) underline, cybersecurity should be addressed as a "social problem+technology" rather than a "technical problem+humans." Policies built on this basis are more likely to result in fair and sustainable solutions and create advantages for the whole of society.

References

Dunn Cavelty, M., Eriksen, C., & Scharte, B. (2023). Making cyber security more resilient: Adding social considerations to technological fixes. *Journal of Risk Research*, *26*(7), 801-814.

Ganapati, S., Ahn, M., & Reddick, C. (2023, July). Evolution of cybersecurity concerns: a systematic literature review. In Proceedings of the 24th Annual International Conference on Digital Government Research (pp. 90-97).

Renaud, K., Van Der Schyff, K., & MacDonald, S. (2023). Would US citizens accept cybersecurity deresponsibilization? Perhaps not. *Computers & Security*, *131*, 103301