Development of a New 'Human Cyber-Resilience Scale'

Solen Grossman

Date: 11/13/2025

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

Introduction/BLUF

This article intends to address the gaps in research on cyber resilience of individual users in a domestic setting by developing and validating a self-report measure of "human cyber resilience," which measures how much a person can resist and bounce back from a cyber-attack (Johnson et al., 2023). It assesses four key areas: self-efficacy, helplessness, social support, and learning and growth using 16 items to address these four key areas (Johnson et al., 2023). The final study using this scale showed that it was valid due to correlations with established measures of convergent validity, predictive validity, and demographics (Johnson et al., 2023).

Relation to Social Science Principles

In terms of Cybersecurity Principles, this study touches on the principles of determinism, objectivity, and empiricism. D**eterminism,** or the principle that past actions will determine the future behaviors or experiences of an individual, is seen with how this study shows that a person's cyber resilience is determined by their prior experiences and psychological constructs. It also focuses on **objectivity** in being open to what conclusions the studies present without preconceived views influencing the study. It is also **empirical** in obtaining its knowledge through observations and experiences compiled across multiple surveys and studies.

This study is a survey, a foundational tool in social sciences research, used to study the individual's ability to cope with cyber threats - a core topic in cyberpsychology. The 4 subscales used in this study directly assess key aspects of an individual's cyberpsychology profile. For example, within the six schools of cyberpsychology (Structuralism, functionalism, psychodynamic, behaviorism, cognitive, social-cultural), and of these schools, the **cognitive school** which is defined by studying mental processes such as perception and judgement can explain one's **self-efficacy** (Their perceived competence in digital space), **helplessness** (Their perceived inability to know what to do), and **learning and growth** (Interpreting a cybersecurity threat as an opportunity to improve). Meanwhile, the cyberpsychology

social-cultural school deals with matters of how social situations influence thinking and behavior which explains **social support** (Seeking social connections to protect against stress).

Research Question / Hypothesis / Variables

The study was conducted on the premise that there was a dearth of comprehensive research in the cyber resilience of users in a domestic context (Johnson et al., 2023). Therefore, the question it poses is **"How can we measure an individual's cyber resilience"** (Johnson et al., 2023). The study hypothesizes that through parsing through the various independent variables and condensing them into core subscales and 16 items **one can develop a valid and reliable self-report scale for human cyber resilience**. The independent variables pertinent to this study would be **the underlying psychological constructs (Self-efficacy, social support, helplessness, and learning and growth).** Through this study, the dependent variable derived is the **score on the Human Cyber-Resilience Scale** and **its subscales.**

Types of Research Methods Used

This study employs quantitative methodology focused on scale development. It utilizes **five studies** with **n = 1503 individuals** and **51 candidate** items adapted from a variety of existing resilience scales which were recontextualized to be about cybersecurity (Johnson et al., 2023). For the first to fourth study, they were from the UK and Ireland, while the fifth study was based around the USA, Canada, and UK (Johnson et al., 2023). Using these profiles, the article refined and validated the items across the five studies to develop a final measurement tool.

Types of Data Analysis used

Studies 1 through 3 used an **exploratory factor analysis** for scale refinement, with the goal being to reduce the initial pool of items by identifying a coherent factor structure and to test new items for emerging subscales; the first subscales settled on being self-efficacy, social support, learning and growth, and helplessness (Johnson et al., 2023). The fourth study is a **confirmatory factor analysis** using the four subscales and 161 participants, and it showed strong statistical support for the model when applied to the

finalized 16-item scale (Johnson et al., 2023). The goal of the final study was to **compare** scores on cyber resilience amongst three English speaking countries (The US, Canada, UK) and examine convergent and discriminant validity. It did this with a final sample of 579 through correlating the 4 subscales with existing measures of general resilience, computer self-efficacy, and cybersecurity behavior through the **Security Behavior Intentions Scale (SeBIS)** (Johnson et al., 2023). The study expected a positive correlation between self-efficacy and SeBIS and a negative correlation with helplessness and SeBIS (Johnson et al., 2023). Through the study, the prediction of a **positive correlation with self-efficacy** and **negative with helplessness** was confirmed (Johnson et al., 2023).

Connections to Other Course Concepts

As aforementioned, there is a strong connection between this study and the topic of cyberpsychology, especially the cognitive and social-cultural schools of cyberpsychology. Some social science topics it touches on are **security fatigue**, a real phenomenon from overwhelming demands which may negatively affect cyber resilience due to increasing the helplessness subscale, and **hyperbolic discounting** where one looks at short-term gains over long-term gains which has a negative correlation with self-efficacy. This study is also a strong example of the practice of Human-Centered Cybersecurity by providing a tool to measure the human factors that NIST emphasizes.

Connections to the Concerns of Marginalized Groups

The study examined the relationship between the level of cyber resilience and demographic characteristics of the participants (Johnson et al., 2023). In doing so they found that **males reported greater resilience in terms of self-efficacy and learning and growth** while **females reported greater resilience through social support and lowered resilience through increased helplessness** (Johnson et al., 2023). The study reports that the gender differences for efficacy and helplessness replicate previous findings in reported efficacy in cybersecurity settings (Johnson et al., 2023). This suggests women are at greater risk of cyber-threats, which highlights a concern from this demographic. These concerns over the greater risk of women over cyber-threats may be addressed with increased fostering of the principles of

self-efficacy and a mindset conducive to learning and growth. One other concern of this study is it was exclusively Anglocentric in looking at the US, UK, Canada, and Ireland; other countries and cultures may yield different results and correlations for studies.

Overall Societal Contributions/Conclusion

This study has comprehensively laid out a valid framework for a cyber resilience assessment which helps translate purely technical solutions to human-centric matters. By parsing through various subscales and items it has been able to reduce it down to 4 core subscales of self-efficacy, learning and growth, social support, and helplessness, and 16 strong items that help the person taking the test discern where they stand for those 4 subscales. This test can help reduce the public's vulnerability, mitigate "security fatigue" that negatively affects vigilance, and empowers individuals to better protect themselves from cybersecurity threats. This scale is conducive to a more cyber-resilient society by focusing on the human element, which is the ultimate source of most security incidents.

Reference

Adam N Joinson, Matt Dixon, Lynne Coventry, Pam Briggs, Development of a new 'human cyber-resilience scale', *Journal of Cybersecurity*, Volume 9, Issue 1, 2023, tyad007, https://doi.org/10.1093/cybsec/tyad007