The article "Building social cybersecurity: An integrated approach" published in the March-April 2019 issue of Military Review. Discussed an interesting perspective on cybersecurity that focuses on the social and cultural aspects in addition to the more technical defenses. As someone who works to help build cyber resilience for organizations, I found the ideas presented in the article quite thought-provoking. It argued that just strengthening passwords and firewalls is not enough - we must also address the human factors that contribute to threats like phishing attempts succeeding all too often. People are ultimately behind both the creation of vulnerabilities as well as their exploitation by bad actors. I appreciated how the authors proposed an integrated approach involving education, awareness training, and empowering digital citizens to make better online choices. Simply commanding users to be more secure rarely works - they need to understand risks and feel a sense of responsibility too. The concepts of a "security culture" and cultivating trust align with what my colleagues and I have observed in building employee buy-in for our clients' security programs. In the future, I plan to incorporate some of these social aspects more deliberately into how my team and I advise clients. We can do more to foster everyday security habits and shape norms within their organizational communities. Evaluating success also needs holistic metrics beyond just compliance. If this approach reduces even one breach by inspiring people to spot that dubious email, it will be worth it. Overall, I found the article's perspective insightful. Cybersecurity is as much about people as it is technology. A truly integrated strategy considering both seems most likely to strengthen security in a sustainable way. I appreciate the Military Review for publishing thought-provoking pieces like this that can help improve practices in my field