When creating policies in cybersecurity, human factors play a role in the creation of the policies themselves. Human factors can lead to a direct violation of standard operation procedures. Human factors have evolved over the years and as a result they have essentially crippled those who a susceptible to attacks such as social engineering attacks, improper update practices and weak password creation. I believe that we can argue that in the 2023 National Defense Strategy for Cybersecurity it is very easy to see how human factors could potentially cause trouble with our government’s designated organization dedicated to carrying out the intentions of the document. I will examine the important pillars of the National Cybersecurity Strategy and show how human factors can play a role in the creation of the strategy. The National Cybersecurity Strategy has been proposed to increase America’s defense capabilities outside our own cyberspace. The document that was released has different points of interest starting that all possess the same level of importance. From the information in the document, it seems that we have moved on from some of our past problems that were present within our country, and we have seemed to shift our focus to external threats. This is more than likely a result of increasing looming threats that have advanced their own cyber capabilities such as China, North Korea, Iran and Russia most importantly as Russia preforms numerous amounts of cyber-attacks across the globe. Because of these dangers America has realized that in order to achieve a prosperous and connected future it will have to depend on information technology laid out through a comprehensive system that will protect the integrity of our country. They address concepts that will allow us to bring all forces of national power and international power of our allies to work in a joint effort to overcome emerging trends. This concept is heavily prevalent throughout the document, and it emphasized heavily in order to inform our nation on whom our enemy is and why they intend to attack from a cyber method. The document discusses how we intend to counter these threats by mentioning the steps that we are taking in place in order to prevent the opposing sides from having success against our nation. The document describes to average American citizen how these external threats also play a bigger a role in their lives than they may think. In the document they discuss aside from the more direct “offensive" method of cyber-attack such as DDoS, malware, and ransomware, attacks the opposing aggressors are attacking from concealed methods such collecting data from foreign owned apps such as TikTok or WeChat (both owned by China). The importance of allowing citizens to understand where they stand within cyberspace in the document is of high importance due to frequency at which the incursions of data being breached happens. To achieve the previously mentioned points of interest, the United States of America has decided to implement a two fundamental shift in which they state will change how “the United States allocates roles, responsibilities, and resources in cyberspace”. (US DoD pg.4) The US government allows plans to implement the new additional five pillars strategy that will build on previous strategies implemented by former administrations that are meant to shape the strategic environment and digital ecosystem. The five-pillar strategy is spearheaded by the first pillar which is the **Defend Critical Structure Infrastructure** pillar. This pillar is essential and imperative to operation capability. Without this pillar our country would not be able to perform the basic functions that allow us to keep our cyberspace safe. The second pillar is the **Disrupt and Dismantle Threat Actors** pillar, this pillar will allow us to engage in global protection posturing activities. This could include intelligence gathering, intercepting enemy communications, or countering cybercrime at root source. The third pillar is the **Shape Market Forces to Drive Security and Resilience. This** pillar develops the plan on how we intend to build on security measures regarding data. The fourth Pillar is the I**nvest in a Resilient Future,** provides insight on how we intend to manage our finical foundation and longevity for our nation. The fifth pillar is the **Forge International Partnerships to Pursue Shared Goals.** This pillar allows us to build allies so that we can rely on and lend help when we or they need it most. Overall, the document is meant to further our cyber capabilities as a country not just domestically but globally as well. The document lays out what is meant to be taken as a brief guideline to what we intend to pursue in terms of cybersecurity measures to protect ourselves. With plans like this our country can make decisions and set goals that will propel us ahead of our adversaries and will ensure that the United States has decisive and swift victory against those who intend to harm it. Simultaneously the document informs the average American citizen where they fit into the scheme and how will affect or already affects them respectively depending on which concept is being discussed in the document. All previous pillars are important and essential to the progression of our country, however there is one pillar that is the most pivotal in the scheme. The first pillar is imperative in nature as it provides a means for our country to operate all the other pillars in the scheme. This pillar defends the systems and assets that our country operates on every level. The first pillar withing the scheme has been divided into objectives that mean to increase preparedness and readiness within our country’s defense boundaries. Defending our critical infrastructure will take numerous amounts of key components and according to the document can only be achieved though establishing cybersecurity regulations to secure critical infrastructure. The document discusses how this will be achieved by stating “Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance” (US DoD pg.8). These regulation checks are to be done by separate agencies and will allow the creation of the more secure infrastructure protection method. Stemming from the creation of safer infrastructure, it will allow a better opportunity for public to private collaboration. These two concepts go hand in hand with each other, because they cannot function without one or the other. The CISA (Cybersecurity and Infrastructure Security Agency) and the SRMA (Sector Risk Management Agencies) work together to maintain the needs of critical infrastructure owners and operators in their sectors. This is also an important part of the pillar because without these two agencies our infrastructure would become obsolete compared to our adversaries. Branching out from SRMA’s we have the integration of federal cybersecurity centers meant to coordinate with authorities and capabilities of the departments of the agencies respectively. This branch is solely responsible for integrating cyber defense planning within the government and with partners that work in conjunction with the CISA. This agency plays a pivotal role in government affairs as they provide the means for being able to extend our cyber capabilities globally as well. Along with global communication and interaction comes global conflict within our government. This is where the pillar exemplifies the importance of updating federal incident response plans and processes so that we can study our adversaries' attack methods and patterns. Without some form of damage control, it is impossible to learn from previous incursions that have occurred in the past. The NCIRP (National Cyber incident Response Plan) is responsible for that role. They are responsible for the CIRCIA (Cyber Incident Reporting for Critical Infrastructure Act) which enhances our awareness and likelihood of being to correctly respond to critical infrastructure damage. Following any incident that occurs, the CSRB Cyber Safety Review Board will work with the CIRCIA and provide extensive countermeasures to protect maintain the mission of the first pillar. The final point the first pillar discusses is the modernization of federal defenses. Perhaps the most relative concept to the main goal of the entire document, the objective of the key pillar point is to explain the importance of staying one step ahead of those who mean to harm our nation. This can extend to protecting NSS (National Security Systems) which contain our country’s most sensitive data or even federal agencies’ security measures as well. This part of the pillar requires data protection methods such as clearance level, multi-step factor authorization, and data encryption. The first pillar of the National Cybersecurity Strategy of 2023 is easily the most pivotal part of the document due to its role in our government and without its presence there will be no capability nor defense measures present within the United States. The first pillar will help our government mold the future of our digital ecosystem until next year’s strategy is released in which the actions mentioned in this year’s strategy are hopefully fulfilled. After examination of the document, I believe it easy to create parallels as to why human factors can play a role in the organization of our government. If we change our systems and upgrade our systems, we will reduce human-induced vulnerabilities. The cyber defense strategy is simply to technologically focused which leads to a lack of internal solutions (humans' factors).

References

Kramer, F. D., & Butler, R. J. (2019). A ROADMAP TO BETTER CYBERSECURITY. In *CYBERSECURITY: CHANGING THE MODEL* (pp. 5–20). Atlantic Council. <http://www.jstor.org/stable/resrep20932.5>

Lord, R., & Roseen, D. (2019). Personal Introduction by Robert Lord. In *Do No Harm 2.0* (pp. 10–14). New America. <http://www.jstor.org/stable/resrep19972.5>

HONG, J. (2016). A PATH FORWARD TO A SECURE INTERNET OF THINGS. In *TOWARD A SAFE AND SECURE INTERNET OF THINGS* (pp. 8–11). New America. <http://www.jstor.org/stable/resrep10509.6>

Matthews, E. D., Arata, H. J., & Hale, B. L. (2016). Cyber Situational Awareness. *The Cyber Defense Review*, *1*(1), 35–46. <http://www.jstor.org/stable/26267298>

Www.whitehouse.gov. (n.d.). Retrieved March 19, 2023, from <https://www.whitehouse.gov/wp->content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf