**Homeland security activities and programs in cybersecurity and privacy protection**

Britain Cox

The University of Arizona Global Campus

HSM 497: Homeland Security & Emergency Management Capstone

Kenneth Jenkins

August 3, 2021

**Introduction**

Over the last few years, there has been a significant increase in technologies and internet use. It has helped revolutionize so many sectors, including the national government. That is why ensuring that cyberspace is secure and reliable is very important, especially for the government. The more technology increases, the higher the cybercrime cases, which means that the different sectors have to work harder to ensure that they are maintaining secure cyberspace. The different technology and internet systems have become a driving factor in running economic systems, government offices and services, forms of communication, and other mannerisms in which national security is maintained. Unfortunately, even with all the efforts being put in place, cybercrime rates continue growing every day. The minute that one vulnerability and security issue is solved. They develop another method to attack. The department of homeland security works at its best bit. Still, the cybercrimes rate is not going down (Radvanovsky, R., & McDougall, 2018). These cyber-attacks have increased security intrusions, specific content, and information from government exposure, among others. With these, the economy gets affected by the increased attacks, and the general well-being of the people who trust their information in the systems is also at the risk of being compromised.

**Research Question**

When it comes to the security provision in cyberspace, is homeland security reliable and effective in the different programs and activities that they run?

Notably, various sectors within the government cannot function without technology. Also, with increased cybercrime, their effectiveness is put at risk, and it also affected the general flow of things like information and communication. That is why homeland security must find manners in which they can prevent cybercrimes or at the very least have them better controlled. As a search, they have come up with different programs geared towards that, but the question remains of how effective they are. The rates of cyber-crime keep on increasing, and this question will help in unnerving the reasons why they are effective or not.

**Hypothesis**

The department of homeland security programs is effective in the reduction of cyber-crimes.

Homeland security deals with making sure that the systems within the government are secure and one way to do that is by ensuring that cyberspaces are secure. The different activities that they take help to enhance security and reduce rates of cybercrimes, especially when it comes to national-related information and plans (Comiskey, 2018). One of the programs includes education on the matter of cybercrimes and how they can be identified. When people learn more about a problem, then they are in a better position to handle it. That is the case with homeland security education programs. While cybercrimes are still high, differences have been seen after the education on cybercrimes and how to combat them. With the increase in white hackers, it has become an issue that can be easily solved.

Additionally, education means that they gather more information which helps them determine the vulnerabilities in the systems. It also creates a platform for research and development concerning the internet and other systems that are vulnerable to attacks. It is a way for them to innovate and develop better reliable strategies that can be used in the different government sectors.

**H1**

The programs that homeland security has come up with have helped the matter of national threat coverage adequately.

While there are different activities that they have put in place, the rates of cybercrimes keep on increasing. A good example was the pandemic hit in 2020. Many people had to work from home, and the rates of cyber-crimes skyrocketed. Homeland security does put much effort into managing cybercrimes, but they only work to a certain extent (Eller, W. S., & Wandt, 2020). The creation of solutions only lasts for the already existing problems, and each problem has to be dealt with as an individual. What this shows is that the solutions only exist for issues that have already been suffered. Therefore they have provided the capacity to manage the threats and intrusions but not completely prevent any intrusions or threats.

It would be better for better coverage and cybersecurity if they had activities and programs that predicted an attack and solved it before it happened (Lewis, 2019). That is the eradication of each innovation coming with new possible cyber vulnerabilities especially given that technology keeps increasing. In the future, most departments will be fully dependent on technology.

**H2**

The availability of innovative technologies is what has helped homeland security in dealing with cybercrimes.

This goes to point out that innovation is what helps in homeland security cybercrime control and solving. Therefore, many resources are geared towards coming up with new technologies to overcome the vulnerabilities and the different ways that they are being attacked. The new technology makes sure that it overrides the previously existing vulnerabilities (Payne, B. K., & Hadzhidimova, 2018). This leaves them to deal with any incoming new issue that they may have overlooked with the latest technology.

It also shows that every effort to help solve the issues depends on the new technologies being launched. Even then, the latest technologies are made to serve the purposes that may be lacking in the previous innovation, making them more reliable and solving cybercrimes' issues. The problem with the innovated technology is that it gets to solves the existing issues but never provided a bulletproof system from any attacks. Therefore, it solves a problem but leaves the system open to new threats and vulnerabilities.

**References**

Comiskey, J. (2018). Theory for homeland security. Journal of Homeland Security Education, 7, 29-45.

Eller, W. S., & Wandt, A. S. (2020). Contemporary policy challenges in protecting the homeland. Policy Studies Journal, 48, S33-S46.

Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.

Payne, B. K., & Hadzhidimova, L. (2018). Cyber security and criminal justice programs in the United States: Exploring the intersections. International Journal of Criminal Justice Sciences, 13(2).

Radvanovsky, R., & McDougall, A. (2018). Critical infrastructure: homeland security and emergency preparedness. crc press.