Critical infrastructure and homeland security essay example

War, Intelligence

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Overview

In efforts to uphold and improve public safety, the United States government has instituted several defensive and offensive plans in collaboration with several of its independent security agencies. Such security organizations as the National Security Agency (NSA), the Central Intelligence Agency (CIA), and the Department of Homeland Security (DHS) have over the years intensified their efforts to keep away potential threats to national security. This has especially been catalyzed by heinous acts of terror on the homeland such as that witnessed in September 11, 2001. Among the efforts put in place under the directorship of the DHS are elaborate programs to secure those public and private assets deemed crucial to the US economy. As such, the National Infrastructure Protection Plan (NIPP) was established through stakeholder participation in 2006; it was later revised and updated in 2009 (Department of Homeland Security (DHS), n. d.).

Critical Infrastructure and Key Resources (CIKR)

The main focus of the NIPP was to identify America's Critical Infrastructure and Key Resources (CIKR), both in the private and public sectors (DHS, n. d.), in order to protect them from any external or internal threats. The CIKR comprises infrastructural elements of 18 of America's crucial sectors, such as health, communication, energy, and commerce. A keen examination of the NIPP and CIKR reveals that the government has indeed made valiant efforts at ensuring the country's most critical sectors and infrastructural installations are protected from possible terrorist threats. This has, however, come at the some cost to the American public. For instance, the issue of intelligence gathering that undoubtedly accompanies these preventive efforts has meant some unavoidable level of compromise on privacy.

Areas for Improvement

Though the country's critical sectors and key infrastructure are relatively well protected, the feeling of invasion of privacy might lead the public to undermine the government's efforts by attempting to circumvent the instituted security measures. For instance, there have been widespread concerns that the NSA's intelligence gathering operations involve, in essence, unwarranted spying on the American public through electronic monitoring and surveillance. This has led some people to seek counter measures that sometimes compromise national security by creating security loopholes, which may be used by opportunists. According to King (2003), some people have filed legal tort claims of invasion of privacy at their places of work, thereby paralyzing intelligence gathering operations by concerned

security agencies, albeit temporarily.

As much as the CIKR aims at identifying and protecting critical sector facilities in the US, they are still liable to attack from such high-level quarters as high-altitude nuclear detonations and the subsequent EMP. Such an attack would disable all electronic equipment and basically paralyze most of the country's socio-economic operations by compromising such key sectors as communication, transport and, by extension, health. Perhaps the government needs to establish ways of getting the private sector to invest in defensive mechanisms against the risk of an devastating EMP attack; these attacks have now become more than just conjecture since the end of the cold war, with China slated to have the technical and financial capability of developing EMP weapons (Schneider, 2009).

References

Department of Homeland Security. (n. d.). National Infrastructure Protection Plan. Retrieved from the Department of Homeland Security website at: http://www. dhs. gov/national-infrastructure-protection-plan#0

Foster, J. S., Gjelde, E., Graham, W. R., Hermann, R. J., Kluepfel, H. M., Lawson, R. L., Soper, G. K., Wood, L. L., Woodard, J. B. (2004). Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (Volume 1: Executive Report). Retrieved from the EMP Commission website at: http://www. empcommission. org/docs/empc_exec_rpt. pdf

King, NJ. (2003). Electronic monitoring to promote national security impacts workplace privacy. Employee Responsibilities and Rights Journal, 15(3), 127-

147.

Schneider, M. (2009). The nuclear doctrine and forces of the People's Republic of China. Comparative Strategy, 28(3), 244-270.