The Open Access Journal of Science and Technology
Vol. 10 (2022), Article ID 08, 2 pages
doi:10.11131/OAJOST.2022.10.008.

AgiAl Publishing House
http://www.agialpress.com/

Perspective

Critical Infrastructure: Cyber Security, Cyber Doctrine and Cyber Warfare

N. Borg*

Department of Civil Engineering, RMIT University, Melbourne, Australia

Corresponding Author
N. Borg
borgnader@rmit.edu.au

Dates
Received: 30-Jul-2020, Manuscript No. OAJOST-22-70766; Editor assigned: 01-Aug-2020, PreQC No. OAJOST-22-70766 (PQ); Reviewed: 15-Aug-2022, QC No. OAJOST-22-70766; Revised: 04-Oct-2022, Manuscript No. OAJOST-22-70766 (R); Published: 12-Oct-2022, DOI:10.11131/OAJOST.2022.10.008.

1. Introduction

The extensive network of roadways, linking bridges and tunnels, railways, utilities and buildings required to maintain everyday life as usual is considered critical infrastructure. These essential systems are necessary for energy, clean water, transportation and business.

Potential infrastructure vulnerabilities have been identified by the Science and Technology directorate (S and T) programme managers of the Department of Homeland Security (DHS), in collaboration with infrastructure owners, operators and the cybersecurity and infrastructure security agency. In order to provide better ways to safeguard infrastructure or in the event of a disaster, to provide the tools for the most rapid recovery, S and T collaborates with national labs, universities and partners from both public and private business. In particular, S and T are working to create and test fresh ideas that will offer superior defence against natural and man made calamities including solar storms, explosions and flooding. This work will contribute to infrastructure improvement, lessen the risk of disruption to the daily contact and trade that these systems enable and strengthen our nation's overall security.

2. Description

Cyber doctrine: The president issues Homeland Security/Presidential Directives (HSPDs) on topics relating to homeland security. They are designed to offer direction, establish standards and improve collaboration amongst all federal agencies. The HSPDs that affect cyberspace are listed below.

- **HSPD 1:** The homeland security council's structure and operations. Coordinates all operations related to homeland security among executive departments and agencies and supports the efficient creation and application of all policies related to homeland security.
- **HSPD 5:** Controlling domestic incidents creates a unified, comprehensive national incident management system, which improves the United States ability to handle domestic situations.
- **HSPD 7:** Identification, prioritization and protection of critical infrastructure establishes a national policy for federal departments and agencies to identify and priorities essential resources and infrastructure in the United States that must be safeguarded from terrorist attacks.
- **HSPD 8:** Nationwide readiness outlines actions for better collaboration in handling incidents. In accordance with this direction, federal departments and agencies must get ready for such a response, including by engaging in preventative measures in the early

phases of a terrorist incident. Along with HSPD-5, this regulation also exists.

- **HSPD 12:** Common identification policy for federal contractors and employees creates an obligatory, federal wide standard for trustworthy, secure forms of identity that the federal government issues to its contractors and employees (including contractor employees).
- **HSPD 23:** Initiative for national cybersecurity. Details those were classified but generally centred on the work that was done.
- **HSPD 24:** Identification and screening using biometrics to improve national security establishes a framework to make sure that the federal executive departments respect the privacy of the persons' biometric information and other legal rights by using mutually compatible methods and processes.

Cyber warfare: Critical to the country's health are the following areas, which rely heavily on the internet. Agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, defense industrial base, department of defense, dams, emergency services, energy, government facilities, healthcare and public health, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, transportation system and water as specified. The Critical Infrastructure and Key Resources (CIKR) protection plan maintained by the US Department of Homeland Security (DHS) tracks these international capabilities or initiatives. They facilitate vulnerability assessments, protective programme implementation, security protocol improvements, real-time information sharing and recovery and contingency planning.

3. Conclusion

The Emergency Services Sector (ESS) is one of our country's Critical Infrastructure and Key Resources (CIKR), according to homeland security presidential directive to save lives, save property and aid in recovery following a disaster, the ESS acts as the first line of defence for our country. Additionally, it aims to defend and guarantee the resilience of other CIKR sectors (e.g. food, water, energy, transportation and others). The ESS disciplines include public works, emergency management, emergency medical services, fire and emergency services and law enforcement. The US Department of Homeland Security (DHS) serves as the Sector Specific Agency (SSA) to lead the security of the ESS through a Sector Specific Plan (SSP) that coordinates goals and attempts to optimize performance under the National Infrastructure Protection Plan (NIPP).