A three-phase defense and protection strategy for Critical infrastructures

Masoud Hayeri Khyavi **Neda Ghavami**

m.hayery@itrc.ac.ir **n.ghavam@itrc.ac.ir**

Abstract

Protecting critical infrastructure in a country/nation is a very critical issue and how to do this and governance it is very challenging. The internal political, social and economic conditions of a country, relations with other countries, the emergence of new communication and information technologies, climate changes and other cases are key and changing factors that must be taken into account in the field of protecting critical infrastructure. take This requires that a flexible and updateable strategy should be used in this field.

Considering the existing challenges, in this article it has been tried to create a policy in the field of creating a suitable and resilience platform or defense structure by considering most of the aspects and factors using a three-phase approach.

Keywords: Defense, Protection, Critical Infrastructure Protection, Risk, Strategy.

Introduction

The first step in defending a country in all areas is to be familiar with its critical infrastructures and their interconnections. Every infrastructure has its own risks and vulnerabilities.

Contemporary modern societies have become significantly more vulnerable, and the spectrum of possible causes of disruptions and crises has become broader and more diffus, As a result, it can be said The term “Critical Infrastructure Protection” (CIP) refers to a broader concept and it is no longer restricted to concrete defense against immediate dangers or criminal prosecution after a crime has been committed, but increasingly refers to preventive security measures as well[1].

Among the factors that should be considered in the defense policy of any infrastructure are the following: An accurate understanding of the infrastructure, its weak points, the effects of infrastructure damage on other infrastructures, identifying threats and how to deal with them, returning infrastructure activity to its previous operational state, and similar cases. Command and control in defense should be done purposefully, on a regular basis, and with the most recent information.

This activity needs to be guided by a comprehensive strategy to ensure that it is effective, to avoid unnecessary duplication of effort, and to maintain continuity[2] . In this paper, a solution (three-phase

solution) is presented to meet and solve the challenges in this field.

Challenges

Developing the information sharing and coordination capabilities needed to effectively deal with computer threats and actual incidents is complex and challenging but essential. Moreover, once an imminent threat is identified, appropriate warnings and response actions must be effectively coordinated among government agencies, the private sector, and, when appropriate, other nations. It is important that this function be carried out as effectively, efficiently, and quickly as possible in order to ensure continuity of operations as well as minimize disruptions [3].

The infrastructure's high risks assets present serious challenges and are crucial to safety, efficiency, and reliability. Any nation must recognize and determine how to cope with any type of threats to their critical infrastructure as well as the strategies to remain resilient [4]. It becomes obvious that like other security issues, the vulnerability of modern societies – caused by dependency on a spectrum of highly interdependent information systems – has global origins and implications [1].

Related works

In [5] some recommendations are mentioned for the protection of critical infrastructure, which are:

1. Establishment of the platform for public-private partnership
2. Establishment of mechanisms for exchange of sensitive information/data among participnats in the critical infrastructure protection system
3. Establishment of preconditions for development of the national center for critical infrastructure
4. Creating normative and strategic frameworks in strengthening resilience and protection of critical infrastructure

Resilience can be defined as the capacity of critical infrastructure to absorb a disturbance, recover from disruptions and adapt to changing conditions, while still retaining essentially the same function as prior to the disruptive shock. In order to better integrate the complexity, interdependencies and interconnectedness of critical infrastructure, adopting a systemic approach to critical infrastructure resilience provides complementary perspective[6].

Three-phase solution Solution

The proposed three-phase solution is as follows:

Phase 1. Comprehensive familiarization with the infrastructure

- **Identification of critical infrastructures**

According to this policy, all critical infrastructures relating to material assets and IT (information technology), networks, electricity, gas, water, telecommunications, etc., whose disruption would have grave consequences for national interests, have been identified.

- **Classification of critical infrastructures**

After identifying the critical infrastructures, a specialized steering committee of experts defines parameters to determine the criticality of the infrastructures, and the infrastructures are classified based on these parameters. This classification varies based on emergency conditions and is crucial because it increases the capacity to defend against a variety of threats and incidents while decreasing additional costs.

- **Determining the connection between critical infrastructures**

After classifying the infrastructures, the connection between them must be identified in order to determine the impact of any damage to one infrastructure on the others. What is the connection and symmetry between infrastructure vulnerabilities and threats, and how significant and urgent are they?

- **Adopting a policy or reviewing existing defense policies in the field of infrastructure**

After identifying, classifying, and determining the connection between infrastructures, the policies for each infrastructure should be developed or, if already in place, reviewed and improved. The policy should be reviewed and revised at predetermined intervals.

After preparing a policy for each infrastructure, a general and comprehensive policy must also be developed. This policy may include security, defense, or other deemed-necessary standards; consequently, the use of standards should be evaluated in light of the country's circumstances (indigenization).

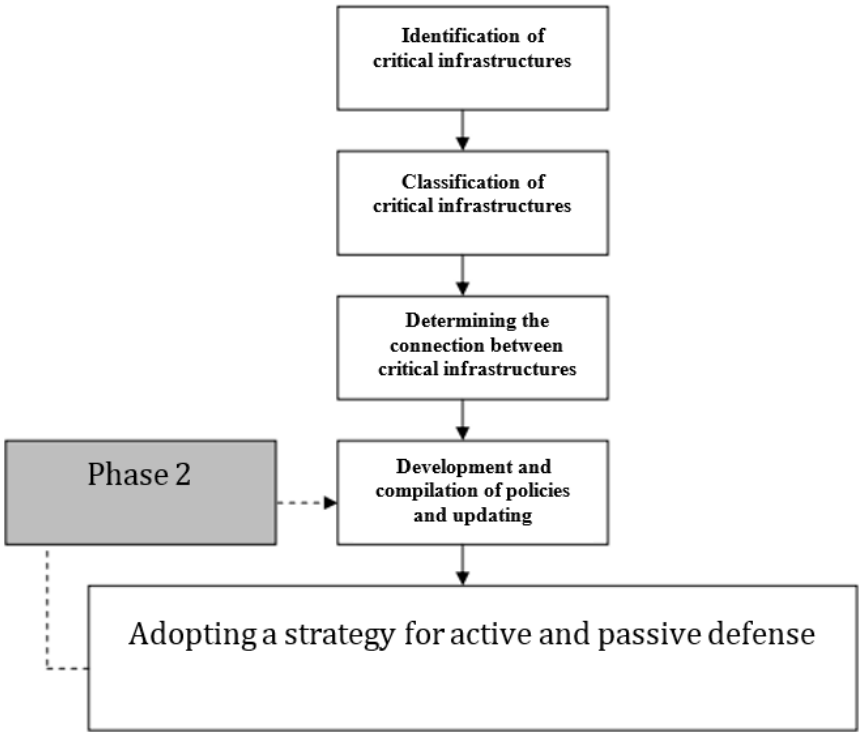

Figure 1 Comprehensive familiarization with the infrastructure

Phase 2. Research and revision

In phase 2, following the preparation and drafting of the policy, it is time to adopt an active and passive defense strategy. However, the most important issue raised is risk management.

In this phase, which can be somewhat similar to phase 1 (Figure 2), it is proposed to identify, monitor, and research new infrastructure threats and risks. In network infrastructure and information technology, for instance, the discussion of viruses, worms, and network attacks grows and evolves daily. Consequently, updating information (about these risks) and, if necessary, updating defense solutions is an obvious requirement for improving and updating policies.

In the electricity and power industry, for instance, the emergence of new weapons, such as carbon bombs and phosphorous bombs, necessitates adopting new solutions. In addition, risk management plays a significant role in this regard.

Unfamiliarity with these threats or the slightest delay in adopting appropriate defense measures will result in irreparable damages.

- **Monitoring**

Monitoring and searching for sources of information on new threats and risks for each infrastructure and predicting potential threats;

A comprehensive analysis of global conflicts, including how parties attack and defend, identify weapons,

etc. For instance, the use of carbon bombs in the Balkan conflict and phosphorous bombs in the Gaza conflict.

- **Identification**

Identification of emerging risks and threats:

For instance, identifying and researching the performance of carbon and phosphorus bombs

- **Research**

Research on the effects of new threats and risks to infrastructure, the effects of damage to the intended infrastructure, and the prediction of potential threats:

For example, detailed research on the direct effects of carbon and phosphorus bombs on infrastructure and living organisms, side effects, and future effects, as well as predicting the possibility of the emergence of a new generation of these weapons.

- **Reaction and response**

Investigating how to deal with damages caused by hazards; adopting and compiling Business Continuity Plan (BCP) (which is infrastructure activity here) and Disaster Recovery Plan (DRP): For instance, how to respond to and defend (actively and passively) against carbon and phosphorus bomb attacks, as well as the necessary countermeasures to mitigate the side effects in the event of a successful attack.

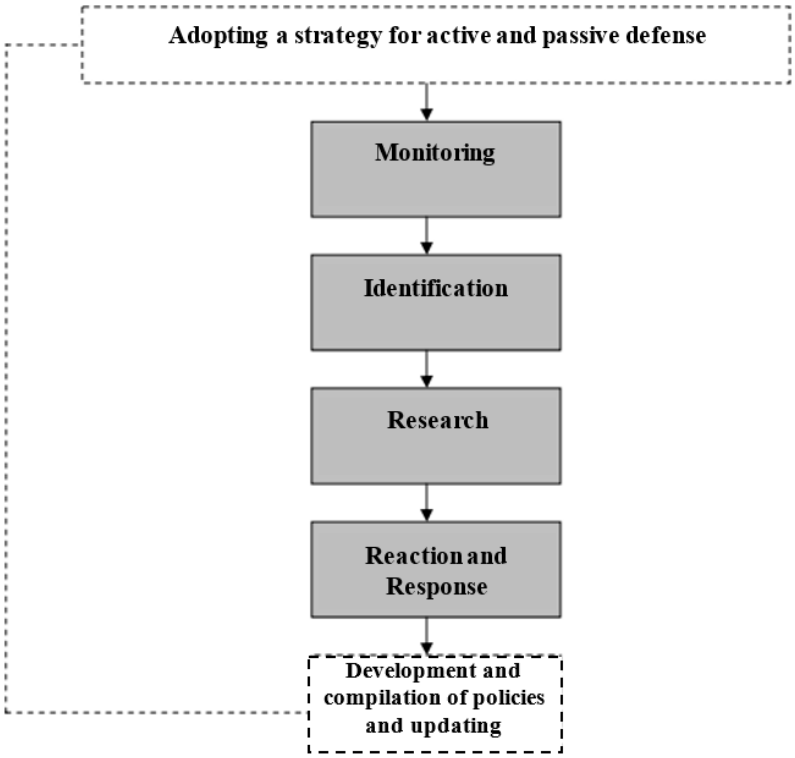

Figure 2 Research and revision

Phase 3. Command and control

After phases 1 and 2, it is time for command and control, which is also a phase of implementation (Figure 3). Control and command, or the adoption and planning of active and passive defense strategies, reaches the action phase based on the steps and items mentioned in phase 1 and the identification and updating in phase 2. Command and control are the foundation for implementing adopted defense policies.

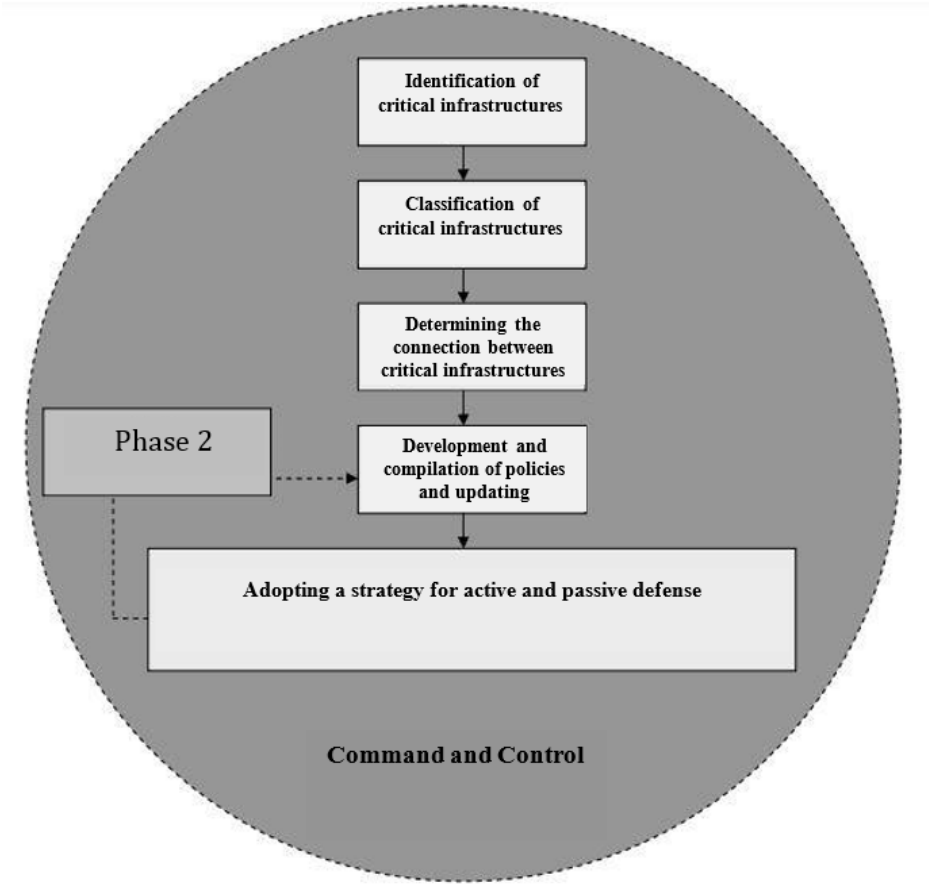

Figure 3 Command and control

Conclusion

Adopting a defense policy necessitates a targeted, consistent, and precise program. Using programs, tools, and other defense issues, even if they are current, will cost money and waste time if there is no appropriate platform.

This solution aims to emphasize the importance of having a flexible, firm, and applicable defense policy and to describe the debates surrounding a nation's defense policies. And it suggests a simple way of working that can be expanded.

References

[1] Andreas Wenger, Victor Mauer and Myriam Dunn Cavelty, “International CIIP HANDBOOK 2008/2009”, Center for Security Studies, ETH Zurich

[2] "Governance challenges for critical infrastructure resilience," OECD High Level risk Forum, 2023.

[3] J. Jack L. Brock, "Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination," United States General Accounting Office, 2000

[4] M. Roshanaei, "Resilience at the Core: Critical Infrastructure Protection Challenges, Priorities and Cybersecurity Assessment Strategies," *Journal of Computer and Communications,* vol. 9, no. 8, 2021.

[5] R. p. team, "RESILIENCE OF CRITICAL INFRASTRUCTURE PROTECTION: Guidline," European Commission - Directorate-General for Humanitarian Aid and Civil Protection- , 2015.

[6] D. Rehak, P. Senovsky, M. Hromada, T. Lovecek, "Complex approach to assessing resilience of critical infrastructure elements", International Journal of Critical Infrastructure Protection, Volume 25, Pages 125-138, 2019,