International Journal of Sustainable Energy and Environmental Research
2022 Vol. 11, No. 1, pp. 23-36.
ISSN(e): 2306-6253
ISSN(p): 2312-5764
DOI: 10.18488/13.v11i1.2965

INVESTIGATING THREATS TO POWER PLANTS USING A CARVER MATRIX AND PROVIDING SOLUTIONS: A CASE STUDY OF IRAN

Rahim Zahedi[1+]
Sina Golivari[2]

[1]*Department of Renewable Energy and Environmental Engineering, University of Tehran, Tehran, Iran.*
Email: rahimzahedi@ut.ac.ir Tel: +989126801778
[2]*Department of Biology, Faculty of Beheshti, Farhangian University, Tehran, Iran.*
Email: sinag79g@gmail.com Tel: +989355806698

(+ Corresponding author)

Article History
Received: 10 February 2022
Revised: 21 March 2022
Accepted: 4 April 2022
Published: 14 April 2022

Keywords
CARVER matrix
Power plants
Threats
Risk assessment
Energy security
Reliability.

ABSTRACT

This paper examines Iran's power plants as potential targets of enemy groups. It identifies the most plausible targets and suggests preventive strategies to counter the threats. There are different models to assess the threat to potential targets. A commonly used model in various fields is the Carver matrix model, which, due to its comprehensiveness, has been used to assess power plants as targets of enemy action. The Carver model has six main factors, each of which is assigned a certain coefficient. To evaluate Iran's power plants as targets, information on their capacity, location, number, age, and fuel type is collected, as well as information on the various threatening groups based around Iran. Using the information on the power plants and the specified coefficients of the Carver matrix, the Iranian power plants have been evaluated as targets. The results of this study indicate that Iran's largest and most sensitive power plants are highly attractive targets for enemies.

Contribution/Originality: In this paper, a modified Carver matrix is used to assess power plants as potential targets. This method can be extended to evaluate energy security in any country.

1. INTRODUCTION

As, in the past, there have always been wars and threats between countries, today there are threats to the values and capabilities of a country. This has led countries to take precautionary measures to protect their assets. To deal with threats, the attractiveness of each asset must be examined from the enemy's point of view. The vulnerability of assets to attacks was examined by Lilliestam (2014). These assets can include any equipment or facilities. A current concern is the prevention of utility outages, such as electricity, gas, water, etc. Electricity is one of the most important sources of energy (Zahedi, Ahmadi, Eskandarpanah, & Akbari, 2022). Today, electricity is not only a service commodity and an economic commodity but represents the vital artery of society, and in the absence of electricity, society will struggle to function. Hospitals, supermarkets, traffic lights, as well as many household appliances depend on electricity. If the electricity is cut off, the natural processes of society will be severely damaged (Van der Vleuten & Lagendijk, 2010). One of the assets that should be examined from a threat point of view is a country's sources of electricity generation – the power plants. Power plants use different types of fuel. For example, Aryanfar et al. (2020) studied the use of solar power in Iran. Statistics from various countries show that infrastructure and energy facilities, including electrical equipment and gas lines, are at increased risk of attack, any of which would disrupt the electricity network. In the electricity industry, threats target four main factors: 1- blackouts and damage; 2- energy supply management; 3- energy exports; 4- network and asset management for various purposes and programs. The first factor naturally occurs even when the region is not under threat; in this case, an enemy would seek to reduce the tolerance threshold of the community by creating blackouts and damaging assets to destroy the community through the consequences of power outages, or by triggering the society to rise against the government, in which case an erosive war will take place to force the society to surrender to their enemy's goals. The other three factors follow when an area is occupied by a hostile group. In the case of the energy supply management factor, one group seeks to supply electricity to its affiliated areas and to shut down areas that are not under its control. In fact, under these circumstances, the group seeks to control society so that it can align people with their views and ideologies. The third factor is the export of electricity, which may be used as a source of income after the occupation of a region by the group if there is an export infrastructure. Given all these issues, hostile groups seek to manage the networks and assets of the electricity industry; clearly, they do not seek to reduce losses and increase network reliability, but rather to identify and examine the network to identify its weaknesses and threats. In this way, they can determine their future actions, so that if an area is removed from their control, they can cause problems in that area with a single blow to the power grid, thus creating potential damage points in the existing grid. If the electricity in the unoccupied areas is connected to the threat-controlled network, they can try to create overvoltages or voltage shocks to put pressure on the area in question and force them to surrender.

Another important aspect of energy systems is their resilience (Perrings, 2006). Resilience is the ability of a power system to recover quickly from destructive events, such as high impact events with a low probability of occurrence, as well as to analyze these events to take steps to prevent the destructive effects of similar events in the future. Resilience can be applied in organizational, social, economic, and engineering arenas. As a result, a system with low resilience must have high security. Preventive measures must be taken to avoid the destruction of energy systems, especially energy systems with low resilience. To do this, it is necessary to be familiar with the types of threats posed by the enemy. One way to identify a possible enemy attack is to become familiar with the attack models. There are various models for planning and preparing an attack or threat, and it is crucial to identify them (Adger, 2000; Brown, Carlyle, Salmerón, & Wood, 2006; Kahnamouei, Bolandi, & Haghifam, 2017).

One of these models is the Carver matrix, which evaluates objectives. The Carver matrix was created by US Special Operations Forces during the Vietnam War as a simple, uniform, and somewhat quantifiable tool for selecting targets for possible missions. The Carver matrix can be used for either offensive or defensive purposes. Carver is an acronym for the six criteria used to prioritize goals: Criticality of the target, Accessibility of the target, Recuperability of the target, Vulnerability of the target, and Recognizability of the target. The Carver method is an economical and effective method of analysis for use as a risk prevention tool.

The Carver matrix has been used in various applications. For example, Mathieu and Rao (2011) used a Carver matrix to identify vulnerabilities in water and drinking water treatment systems. It was also used by Kulawiak and Lubniewski (2014) to support decision-making in urban development and infrastructure protection. A Carver matrix was also used to study and analyze physical and sensitive urban applications from the perspective of passive defense in the city of Zabol (Roozbazar, 2017). However, one of the most important assets for any country to protect is its power plants (Fovino, Guidi, Masera, & Stefanini, 2011). If preventive measures are not taken to counter threats to power plants, devastating consequences may result. One of the most likely and important consequences is the creation of deliberate blackouts in the power grid (Bo et al., 2015; Farmer & Allen, 2006; Rose, Oladosu, & Liao, 2007). In this paper, a Carver matrix is used to assess power plants' vulnerability to threats. Specifically, power plants in Iran are evaluated, although this method can naturally be used to evaluate power plants in other countries. As mentioned, a Carver matrix can be used for either offensive or defensive purposes. This matrix is such that the six main factors mentioned above are determined by a specific weighting of coefficients for each potential military target. The coefficients for each target form a matrix. The target with the highest value for the six factor coefficients is the most likely to be attacked. The coefficients are determined by the person chosen as the decision maker. Here, the weighting coefficients for each power plant are determined by the relevant elites.

2. SYSTEM DESCRIPTION

First, we should consider an overview of the importance of the plants and the types of threats they face. As mentioned above, the rationale behind investigating Iranian nuclear power plants from the perspective of threats is that Iran has large, sensitive plants. Depending on which of Iran's borders is attacked, the impact on the border production networks will be different. In fact, concerning threats to power generation networks, there are two scenarios for the capture of plants: production disruption and production and consumption. In the production disruption scenario, only production will be eliminated. However, in both scenarios, it is important that the national power grid not be disturbed. Therefore, measures should be taken to deal with these scenarios. In the threatening scenario called attack and flight, it is assumed that in each of the border cities the enemy has invaded, the enemy has destroyed the electrical installations in the area and then left, leaving both the region's electricity and its export power cut off. In the capture scenario, we assume that the enemy has invaded and captured the city, in which case the grid does not need to supply the region's electricity. Although the region's production is not necessary, the region's consumption will be almost zero, which is only a problem in the borders near the country's capital and other regions. Several scenarios impose threats on the Iranian electricity grid, and these are of great importance depending on when and where they take place (Zahedi, Ghorbani, Daneshgar, Gitifar, & Qezelbigloo, 2022). The location of the plant is particularly important in terms of whether it is in a border or non-border region because border regions are more prone to attacks in Iran. Therefore, by precisely identifying the border points and the threat points, predictions can be made concerning damage to plants or transmission lines, as well as the required measures to reduce the losses to the power grid.

There are many paramilitary groups around the cities of Iran - known groups such as IS, Pezhak, Jaish-ul-Adl, Taliban, and intra-regional powers. These groups are scattered around the Iranian border. The existence of such groups is a great threat to the country of Iran, and all aspects of necessary security measures should be considered.

3. DATA AND METHODOLOGY

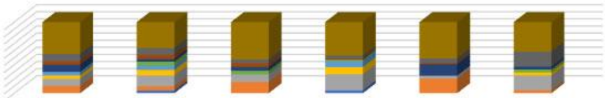
3.1. Data Description

There are important points to consider when evaluating the attractiveness of a power plant to an attack. For this article, which examines Iranian power plants from the point of view of threats, it is necessary to collect information on the number, location, capacity, fuel, and lifespan of Iranian power plants, as well as on the various hostile groups based around Iran. Each of these aspects is important in its own way. The most important factor to assess the attractiveness of a target is the power plant's capacity; the higher the production capacity of a power plant, the more attractive it is. Another important issue is the enemy's access to the power plant; the more easily accessible the power plant is, the more attractive it is. Another factor is the volume of enemy threats near the power plant. For this reason, the threats or hostile groups that are present in proximity to each power plant must be identified. The next item is the location of the power plant. A power plant in the center of the country is more secure than one near the border. Another factor is the type of fuel consumed by the power plant (Daneshgar & Zahedi, 2022). A power plant that is heavily dependent on a single type of fuel is more vulnerable to threats. Another issue to consider is the age of power plants; older power plants have a higher level of vulnerability.

This paper investigates the attractiveness of the targets, power plants, using a Carver matrix. Power plants with a higher weight factor have a higher level of attractiveness for enemy attacks. The commander determines the values of the weighted coefficients of the Carver matrix to meet the objectives of this paper. These weighting coefficients are thus determined according to the opinions of the elite. The remainder of this section presents the required information about Iranian power plants that will be used in the Carver matrix, which has been collected through extensive research.

3.1.1. Number and Location of Power Plants in Iran

The number and location of Iranian power plants can be seen in Figure 1 (Shorabeh, Firozjaei, Nematollahi, Firozjaei, & Jelokhani-Niaraki, 2019). These data have been obtained from extensive research throughout Iran. The table shows that the most power plants are in the center of the country and the fewest in the islands. Also, a significant number of power plants have been built in border areas.

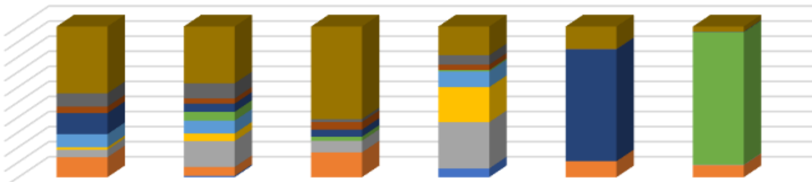


	Heater	Gas	Combined	Diesel	Hyedropower	Other
Center	9	19	10	23	25	10
Northwest border	2	5	1	2	3	5
Western border	1	3	1	1	1	0
Southwest border	2	2	1	0	8	1
Persian Gulf border	0	3	1	1	0	1
South border	1	3	0	4	0	0
Southeast border	1	4	0	5	0	1
Northeast border	2	8	2	11	2	5
Caspian border	2	3	3	0	10	1
Island	0	2	0	2	0	0

Figure 1. Number and location of Iranian power plants.

3.1.2. Capacity and Location of Power Plants in Iran

The capacity of Iranian power plants in each location can be seen in Figure 2 (Mazandarani, Mahlia, Chong, & Moghavvemi, 2011). The data in this table have been obtained from extensive research throughout Iran. They show that the greatest amount of power is produced in the center of the country and the least amount of power in the islands. Significant amounts of power are also generated in the border regions.



	Heater	Gas	Combined cycle	Diesel	Hydropower	Other
Center	6543	6461	9286	64	1597	39
Northwest border	1300	1719	288	21	41	4
Western border	640	589	769	12	9	0
Southwest border	2065	929	704	0	7995	1
Persian Gulf border	0	1001	415	3	0	1020
South border	1280	1454	0	35	0	0
Southeast border	246	864	0	78	0	0.66
Northeast border	733	2951	1155	103	0	4
Caspian border	1955	1014	2488	0	1144	92
Island	0	146.918	0	19.525	0	0

Figure 2. Capacity of Iranian power plants per location (MW).

3.1.3. Fuel Type of Iranian Power Plants

Information on the amount of fuel consumed in Iranian power plants is presented here. A graph illustrating the fuel share of power plants in border regions is shown in Figure 3 (Murshed, 2020). As can be seen, the border power plants are most dependent on gas, and the three important borders regions of southwest, northeast, and northwest, which have the highest production levels, are naturally more dependent on gas. Figure 4 shows the fuel share diagram for central power plants. As can be seen, the center of the country is most dependent on gas and hydropower for its production capacity. In fact, this region shows a dependence on gas of above 10,000 MW, which indicates the importance of gas in Iran.

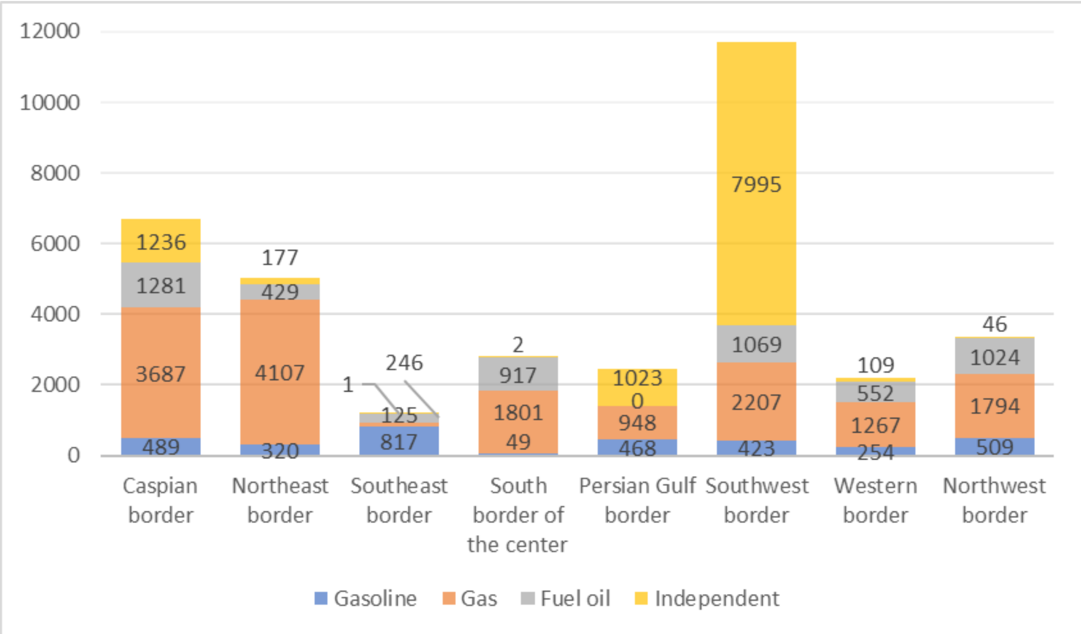


Figure 3. Fuel share chart for border region power plants (MW).

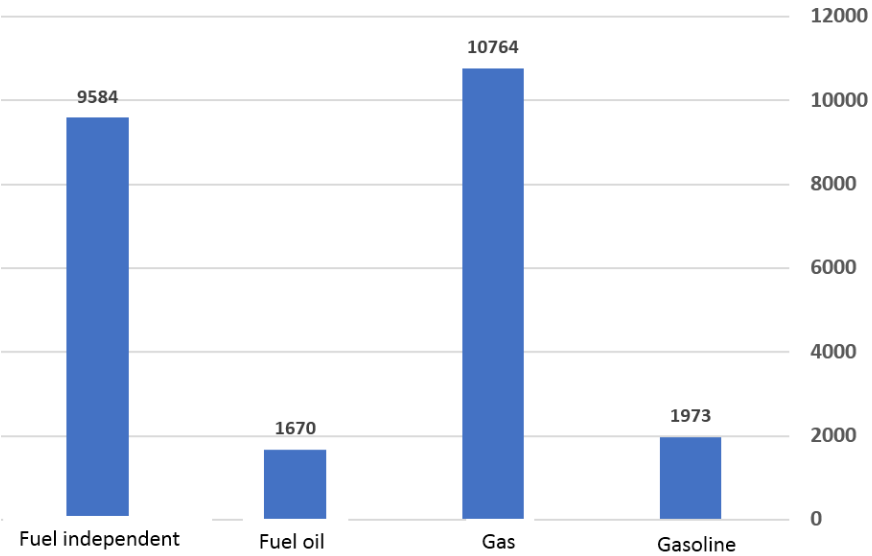


Figure 4. Fuel share of central power plants (MW).

3.1.4. Age and Capacity of Large and Sensitive Power Plants in Iran

Table 1 examines the largest power plants in terms of their production capacity as well as their age (Moazzami, Hemmati, Fesharaki, & Rad, 2013). Undoubtedly, these 11 power plants are the most vital in Iran and attract a great deal of attention for enemy attacks. Among these power plants, 5 are on borders that are more accessible to the enemy.

Table 1. Age of large and sensitive power plants in Iran.

Life Span	Power	Number of the power plant	Type of power plant	Location of the power plant
Year	MW	**n**	**Thermal**	**Border**
22	1810	Power plant 1	Thermal	Southwest border
3	1020	Power plant 2	Thermal	Persian Gulf border
30	1280	Power plant 3	Thermal	Southern border of central region
22	1715	Power plant 4	Thermal	Caspian border
29	1186	Power plant 5	Thermal	Caspian border
17	1592	Power plant 6	Thermal	Center
14	1270	Power plant 7	Thermal	
9	2271	Power plant 8	Thermal	
23	1000	Power plant 9	Thermal	
10	1451	Power plant 10	Thermal	
14	1111	Power plant 11	Thermal	

3.1.5. Types of Groups Based Around Iran

Figure 5 shows a map of Iran. The areas under threat have been identified by the presence of hostile groups, hostile countries in the region (HCR), and trans-regional hostile countries (TRHC), which these days threaten the southwestern border of the country and the cities of Khuzestan and Bushehr.

It is clear that various groups on all sides of Iran pose a threat and intend to attack. This is a warning to Iran to take the necessary security measures to prevent the enemies from reaching their goals and to increase its capacity to deal with any threat and manage crises accordingly.

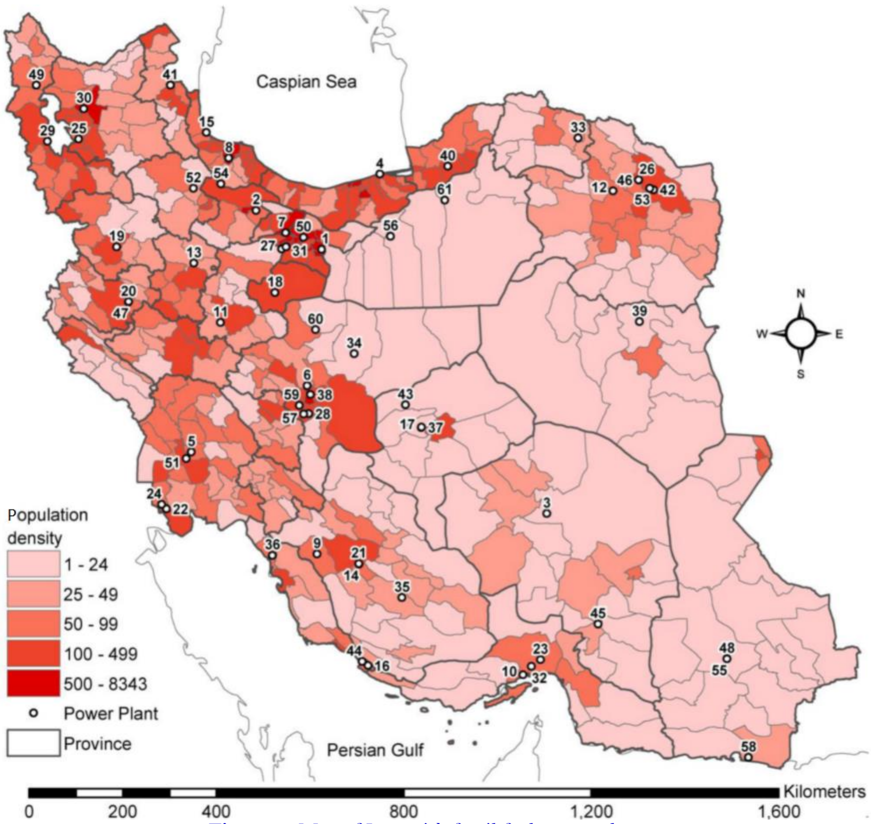


Figure 5. Map of Iran with fossil fuel power plants.

3.2. Model Specification

There are different models within attack theory. In this paper, the Carver matrix model is applied to power plants. This model is very complex due to the number of factors related to the hostile group's goals, their access to the target, and the impact of an attack on the population, the economy, and government operations. Targets at risk of an attack include both facilities and people. In this model, the goals are evaluated by experts and, in accordance with the information, priorities are assigned to threatening goals (Cook, Janicke, Smith, & Maglaras, 2017).

3.2.1. Target Threat Assessment Model

The Carver matrix is used by the US military as a basis for target evaluation. It is defined by six criteria, which are outlined in Table 2 (Gao, Li, & Zhong, 2020).

Table 2. CARVER target assessment matrix components and their descriptions.

Component	Description
Criticality	Criticality is a measure of the relative importance of the target and its importance to the functioning, well-being, and confidence of the population. Factors include: • Time – How rapidly taking out the target will affect operations or ability to respond or continue. • Quantity – What percentage of the capability will be affected.
Accessibility	Measure of how easily the target can be reached or infiltrated
Recuperability	Measure of the ability to recover if the target is destroyed
Vulnerability	Measure of the expertise and means to destroy a target
Effect on the Population	Influence on the population if the target is destroyed
Recognizability	Degree to which the target can be recognized with respect to nearby objects or clutter

There are two ways to determine these coefficients. The first is to calculate the coefficients of the 6 factors in proportion to a maximum score defined for each factor, so that, for example, for component C, the maximum score is 5, and for component A, the maximum score is 10, and so on. The coefficient is considered. The second method considers the sum of the coefficients of the 6 factors to be 1 or 100%. For example, for factor C, the maximum is 0.2, for factor A, the maximum is 0.3, and so on, taking into account that the sum of the 6 factors should not exceed 1 (Greaver, Raabe, Fox, & Burks, 2018).

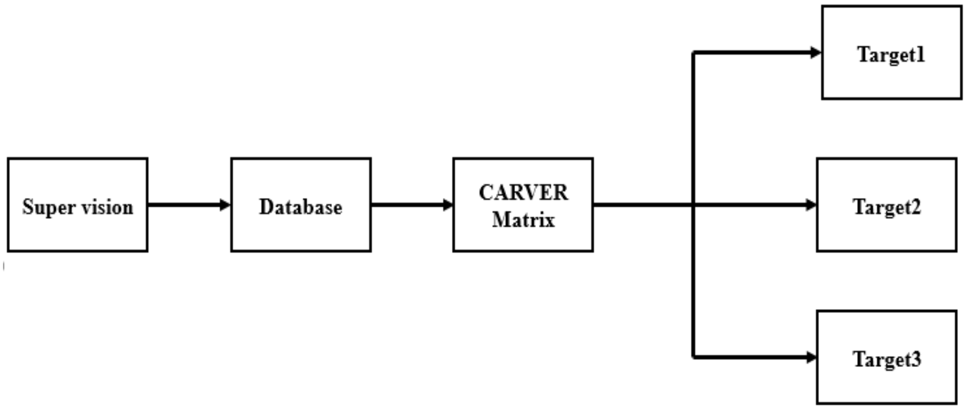
The Carver method thus involves evaluating a goal and assigning a numerical value to 6 factors that indicate the strengths and weaknesses of that goal. Using this method as an offensive tactic can increase efficiency and reduce casualties. However, another useful application of the Carver method is as a defensive action, simply by performing the same analysis and using it as a method of assessing target security.

3.2.2. CARVER Modulation

After collecting information for the purpose and applying this to the Carver matrix, the obtained coefficients are stored in a database. The observer, who may be a military commander or anyone else, plans the attack according to the obtained coefficients, which have prioritized a certain target. The coefficients thus allow targets to be more easily identified, and the enemy commander uses a Carver matrix to identify the most promising targets. Of course, this process may also be carried out by the asset owner himself. This allows the owner of the asset to counter a possible attack by identifying the enemy's priority targets and then implementing the necessary measures to prevent the attack.

After evaluating each Carver factor for each potential target, the values are placed in a matrix. Each column of the matrix is one of the Carver factors. Each row of the Carver matrix represents the total value of the 6 Carver factors for a target. This gives defense personnel the advantage of being able to predict where or how an attack might occur. The analysis also provides a priority list for security personnel. Although one cannot depend entirely on a risk pattern, a Carver analysis can indicate where the enemy intends to attack.

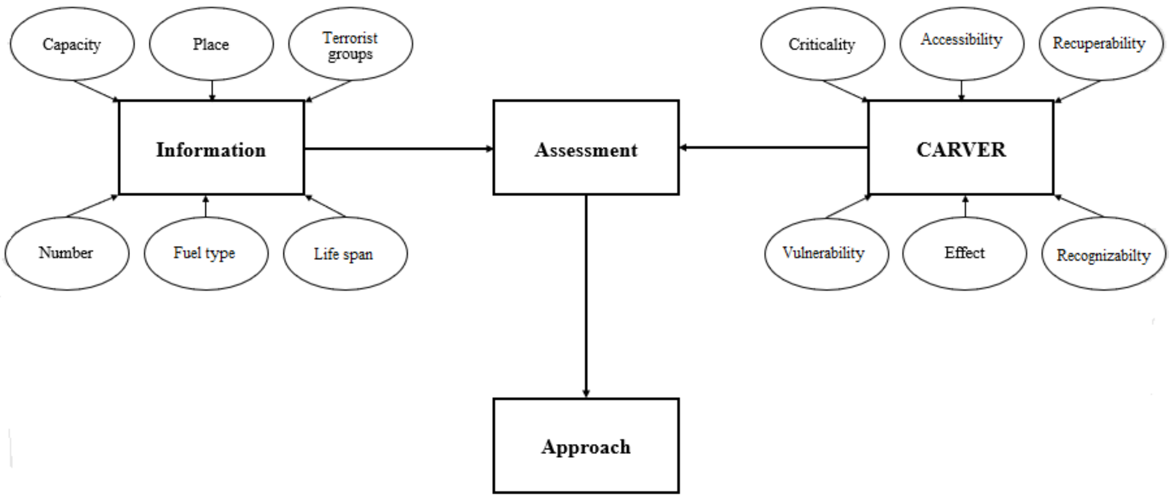
Figure 6 shows a general model of the operation of a Carver matrix. In this model, by way of example, three potential targets have been examined, and a 6 * 3 matrix is therefore defined. The Carver matrix information is stored in a database and the monitoring department can use the information as needed.



	C	A	R	V	E	R	Total
Target1	✓	✓	✓	✓	✓	✓	✓
Target2	✓	✓	✓	✓	✓	✓	✓
Target3	✓	✓	✓	✓	✓	✓	✓

Figure 6. Carver model flowchart and sample 6 * 3 Carver matrix.

The schematic framework of the present study is shown in Figure 7.



C	A	R	V	E	R	CARVER
0.2	0.3	0.03	0.03	0.4	0.04	1

Figure 7. General framework of the present study.

4. RESULTS AND DISCUSSION

4.1. CARVER Matrix Analysis of 11 Sensitive Power Plants

A value is selected for each of the Carver matrix factors. Criticality is defined as the volume of enemy threats (maximum 0.2). Accessibility is the availability of the power plant to the enemy (maximum 0.3). The fuel consumption of the power plant is considered Recuperability (maximum 0.03). The age of the power plant is considered Vulnerability (maximum 0.03). The production capacity of the power plant is taken as the Effect (maximum 0.4). Finally, the location of the power plant is considered Recognizability (maximum 0.04). It should be noted that the factor values have been determined through extensive research and conform to the opinion of the elite.

Eleven major power plants were selected based on their sensitivity and size; these power plants have been examined in terms of their attractiveness to enemies, resulting in the Carver matrix shown in Table 3.

Table 3. The CARVER coefficients for 11 large and sensitive power plants in Iran.

Power Plants	C	A	R	V	E	R	CARVER
Power Plant 1	0.18	0.26	0.02	0.03	0.38	0.03	0.9
Power Plant 2	0.19	0.28	0.01	0.01	0.3	0.04	0.83
Power Plant 3	0.19	0.28	0.02	0.03	0.32	0.04	0.88
Power Plant 4	0.1	0.2	0.01	0.03	0.37	0.01	0.72
Power Plant 5	0.1	0.2	0.02	0.03	0.31	0.01	0.67
Power Plant 6	0.11	0.22	0.03	0.02	0.35	0.02	0.75
Power Plant 7	0.12	0.24	0.02	0.02	0.32	0.02	0.74
Power Plant 8	0.11	0.22	0.03	0.01	0.4	0.02	0.75
Power Plant 9	0.13	0.26	0.02	0.03	0.3	0.03	0.77
Power Plant 10	0.11	0.22	0.01	0.02	0.34	0.02	0.72
Power Plant 11	0.12	0.24	0.01	0.02	0.31	0.02	0.72

The results obtained from the matrix indicate that Power Plant 1 is the most attractive to enemies, and Power Plants 3 and 2 are the next enemy priorities, respectively. According to the results, Power Plant 5 is the least likely to be attacked. The coefficients obtained for these 11 large and sensitive power plants indicate that they are very attractive targets for attack. Therefore, solutions must be found to counter threats and increase the plants' passive defenses. Below, several strategies are suggested to deal with threats.

4.2. Passive Defense Solutions against any Threat Category for the 11 Power Plants

In this section, passive defense solutions are presented for each of the hypothesized threats against the 11 primary thermal power stations of Iran that would result in extensive loss of life.

4.2.1. Destruction and Sabotage of Assets

The most important solution to the threat of destruction and sabotage is to reduce the grid's dependence on a specific asset, or in other words, to disperse the provision of electricity across the territorial, national, and provincial space. To achieve this, the best way to generate electricity is through distributed generation. This solution makes it possible to island the network in the event of an incident. In this way, despite the loss of transmission lines and certain power plants, the network will not completely shut down, and it will be possible to continue to provide the minimum loads needed to provide services. Thus, passive defense solutions against the first category of threats are:

- Modifying the production management policy to develop distributed production.
- Enabling network islanding in the event of an incident.
- Minimizing and creating scatter.

4.2.2. Use of Bombs and New Threats

New threats include electromagnetic, graphite, and laser bombs that destroy network assets by creating overvoltages, short circuits, and concentrated heat, respectively. The best solution to these threats is to strengthen the network with adaptations such as shielding, coating, etc., as well as reduce the sensitivity of the network to the loss of a single asset. Thus, passive defense strategies against the second category of threats are:

- Shielding control and electronic equipment.
- Coating and insulating conductors.
- Earthing the equipment body and boards etc.

4.2.3. Cyberattacks

Since the implementation of automation and network intelligence projects, all networks in the electricity industry are controlled digitally and computerized. Cyberattacks allow network information to be retrieved and changed, and commands can be changed to suit the adversary group. In this way, the stability of the network is disrupted. Thus, passive defense strategies against the third category of threats include:

- Optimal design of network information flow, while maintaining security and accessibility for executive and decision-making units.
- Creating an independent telecommunication network to improve the security and stability of telecommunication systems.
- Cyber retrofitting.
- Equipping the network with automation and intelligence systems to increase the response speed in the event of an incident.
- Development of network monitoring of cyber defense.

4.2.4. Stimulating Iranians to Consume at the Same Time

This threat is people-centered and starts by inciting people to a sudden increase in consumption, which results in network weaknesses. Overload network designs are usually considered to be somewhat specific. Thus, passive defense strategies against the fourth category of threats are:

- Controlling the load and managing the demand of Iranian consumers, especially through economic parameters and floating prices.
- Increasing the number and capacity of capacitors in the distribution network to provide reactive power in the distribution sector and minimize the reactive power required by the power plants and transmission network.
- Balanced development of production centers.
- Balanced development of power plants with balanced loads across different geographical areas.
- Use new sub-loading methods when an error or defect occurs.

4.2.5. Identify and Exploit Network Vulnerabilities

Network vulnerabilities are identified either through the collection and analysis of information or by collecting informed elements in the system.

These include points with inadequate protection or inadequate stability control, network design weaknesses, such as overload weakness, or inadequate emergency control systems. Thus, passive defense strategies against the fifth category of threats include modifying the network structure as well as the design and planning of transmission network development with the following considerations:

- The network remains stable when one of the lines is lost.
- Load uncertainty and sudden increases are taken into account so that lines and backs are not overloaded.
- Electricity export considerations.
- Optimal management of the use of protective devices for repair and adjustment.
- Continuously re-read the power grid and readjust the protection relays.
- Secure coordination between network protection and production.
- Automatic and digital control of generator excitation system.
- Regular maintenance, evaluation, and testing of power plants and substation equipment.

4.2.6. Creating Multiple Blackouts and Faults Simultaneously

Normally, a country's electricity network should remain stable even when an asset (line, post, power plant) is lost. But the nature of attacks on the power grid has changed, and they currently focus on disabling at least two assets simultaneously. This danger can be mitigated by complicating the structure and increasing the number of reserve lines, as well as increasing the rotating reserves. However, there is a need for more investment, which requires the support of the government and the private sector. Thus, the practical passive defense strategy against the sixth category of threats is:

- Modify the production management policy to increase distributed production.

4.2.7. Create Defects in Areas where there is No Balance between Production and Consumption

As mentioned, where there is a lack of balance between production and consumption in a specific geographical area, that area becomes more susceptible to influence by foreign and neighboring governments. On the other hand, places in which production is much lower than consumption are at much lower risk. In order to create blackouts, high production areas are highly attractive. Thus, passive defense strategies against the seventh category of threats are:

- Modify the production management policy to increase distributed production.
- Balanced development of power plants with balanced loads across different geographical areas.

4.2.8. Identify and Exploit Areas where there is No Emergency Control System

As mentioned above, attacks on the power grid intensify when there is no emergency control system or its operation is disrupted. Thus, passive defense strategies against the eighth category of threats are:

- Modify the production management policy to increase distributed production.
- Equip the network with automation and intelligence systems to increase the response speed in the event of an incident.
- Increase the number, capacity, and capabilities of fast-start emergency units.
- Development of network monitoring of cyber defense.

4.2.9. Influence on Human Resources

This category of threats, which are mainly caused by the enemy's influence on the decision-making centers, has wide and diverse manifestations, and different defensive strategies must be adopted for each.

Strategies to combat infiltration in the executive body of the electricity industry are:

- Management and command of the grid, as well as coordinated planning and operation between regional electricity suppliers.
- Strengthen operators to improve their ability to deal with disruptions, and strengthen their monitoring.

Strategies to deal with infiltration in the management body of the electricity industry are:

- Modify regulations to encourage investment in the distribution sector.
- Modify electricity prices to improve investment mechanisms in the production sector and network.
- Regulation of the private sectors of the electricity industry to ensure quality performance, such as safe production, proper repairs, etc.
- Development of self-sufficiency in the production of goods, services, and consulting.
- Improve private sector oversight.

Strategies to combat infiltration in the Ministry of Energy are:

- Not transferring the transmission network to the private sector.
- Using people to help monitor service companies and amend laws (drafting laws such as protecting consumer rights).

4.2.10. Sanctions

Sanctions reduce the ability of governments to control and manage affairs economically, limit the purchase of goods and services from other countries, and thus reduce the level of services available to the demands of society. There are four basic ways to deal with this threat.

1) Demand level control

- Load control and management of consumer demand, especially through economic parameters and floating prices.

2) Self-sufficiency and resistance economy

- Development of self-sufficiency in the production of goods, services, and consulting.
- Implementing a resistance economy in the power industry.

3) Reform regulations

- Modify regulations to encourage investment in the distribution sector.
- Implementation of economic evaluation.
- Monitoring the economic performance of companies affiliated with the Ministry of Energy.

4) Resource diversification

- Creating diversity in the types of power plants: hydropower, combined cycle, wind, solar, geothermal, nuclear, seismic, etc.
- Creating diversity in foreign sources of equipment and non-unique sources of production and sale of goods, equipment, and tools required.

5. CONCLUSION

This article examines Iran's power plants from the point of view of their vulnerability to external threats. A Carver matrix was used to evaluate the primary power plants. The factors selected to help determine the Carver coefficients were the power plants' capacity, location, number, age, and fuel type, as well as the proximity to different threatening groups stationed around Iran. The evaluation has shown that Iran's largest power plants are very attractive targets for enemy action. The data also show that the power plants in border areas are most dependent on gas. In the center of the country, plants are most dependent on gas and hydropower. Most of the production capacity depends on gas fuel and the price of electricity generation behind the dam. In fact, gas supplies more than 10,000 MW of power, which shows the importance of gas fuel in Iran. It is suggested that the type of fuel consumed by power plants, especially those in border areas, be reconsidered.

There are several ways to deal with the various threats to the energy sector, the most important of which is downsizing power plants as a strong deterrent to attack; the dispersion and downsizing of power plants is completely possible. Threats would struggle to simultaneously target all the power plants due to their large number and the existence of national security, and due to the reduced capacity of the power plants, an attack on a small number of power plants would not cause serious problems for the network or the country's electricity supply. Another issue that is of great importance is the diversification of power plants to reduce their dependence on a particular fuel type; then, the electricity network will not face serious problems due to an attack on a particular fuel network. It is natural to develop balanced production, and power plants can prevent the concentration of the production network at a single point. Furthermore, it is necessary to reduce the dependence of the entire electricity network on the country's border power plants as much as possible. Another solution that should be considered is an increase in power plants' fuel reserves so that in case of damage to the fuel supply network, power plants can continue to operate until the crisis is resolved. Upgrading security and backup and transmission networks can also greatly mitigate the risks to the electricity industry.

Funding: This study received no specific financial support.
Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study.

REFERENCES

Adger, W. N. (2000). Social and ecological resilience: Are they related? *Progress in Human Geography, 24*(3), 347-364.

Aryanfar, A., Gholami, A., Pourgholi, M., Shahroozi, S., Zandi, M., & Khosravi, A. (2020). Multi-criteria photovoltaic potential assessment using fuzzy logic in decision-making: A case study of Iran. *Sustainable Energy Technologies and Assessments, 42*, 100877.Available at: https://doi.org/10.1016/j.seta.2020.100877.

Bo, Z., Shaojie, O., Jianhua, Z., Hui, S., Geng, W., & Ming, Z. (2015). An analysis of previous blackouts in the world: Lessons for China′ s power industry. *Renewable and Sustainable Energy Reviews, 42*, 1151-1163.Available at: https://doi.org/10.1016/j.rser.2014.10.069.

Brown, G., Carlyle, M., Salmerón, J., & Wood, K. (2006). Defending critical infrastructure. *Interfaces, 36*(6), 530-544.

Cook, A., Janicke, H., Smith, R., & Maglaras, L. (2017). The industrial control system cyber defence triage process. *Computers & Security, 70*, 467-481.Available at: https://doi.org/10.1016/j.cose.2017.07.009.

Daneshgar, S., & Zahedi, R. (2022). Investigating the hydropower plants production and profitability using system dynamics approach. *Journal of Energy Storage, 46*, 103919.Available at: https://doi.org/10.1016/j.est.2021.103919.

Farmer, R. G., & Allen, E. H. (2006). *Power system dynamic performance advancement from history of North American blackouts*. Paper presented at the 2006 IEEE PES Power Systems Conference and Exposition. IEEE.

Fovino, I. N., Guidi, L., Masera, M., & Stefanini, A. (2011). Cyber security assessment of a power plant. *Electric Power Systems Research, 81*(2), 518-526.Available at: https://doi.org/10.1016/j.epsr.2010.10.012.

Gao, Y., Li, D.-s., & Zhong, H. (2020). A novel target threat assessment method based on three-way decisions under intuitionistic fuzzy multi-attribute decision making environment. *Engineering Applications of Artificial Intelligence, 87*, 103276.Available at: https://doi.org/10.1016/j.engappai.2019.103276.

Greaver, B., Raabe, L., Fox, W. P., & Burks, R. E. (2018). CARVER 2.0: Integrating the analytical hierarchy process's multi-attribute decision-making weighting scheme for a center of gravity vulnerability analysis for US special operations forces. *The Journal of Defense Modeling and Simulation, 15*(1), 111-120.Available at: https://doi.org/10.1177/1548512917717054.

Kahnamouei, A., Bolandi, T., & Haghifam, M. (2017). *The conceptual framework of resilience and its measurement approaches in electrical power systems*. Paper presented at the IET Conference Proceedings the Institution of Engineering & Technology.

Kulawiak, M., & Lubniewski, Z. (2014). Safe city—a GIS-based tool profiled for supporting decision making in urban development and infrastructure protection. *Technological Forecasting and Social Change, 89*, 174-187.Available at: https://doi.org/10.1016/j.techfore.2013.08.031.

Lilliestam, J. (2014). Vulnerability to terrorist attacks in European electricity decarbonisation scenarios: Comparing renewable electricity imports to gas imports. *Energy Policy, 66*, 234-248.Available at: https://doi.org/10.1016/j.enpol.2013.10.078.

Mathieu, T. N., & Rao, A. S. (2011). Identifying drinking water and water treatment systems vulnerabilities using the CARVER matrix method. *International Journal of Critical Infrastructures, 7*(1), 37-49.Available at: https://doi.org/10.1504/ijcis.2011.038955.

Mazandarani, A., Mahlia, T., Chong, W., & Moghavvemi, M. (2011). Fuel consumption and emission prediction by Iranian power plants until 2025. *Renewable and Sustainable Energy Reviews, 15*(3), 1575-1592.Available at: https://doi.org/10.1016/j.rser.2010.11.043.

Moazzami, M., Hemmati, R., Fesharaki, F. H., & Rad, S. R. (2013). Reliability evaluation for different power plant busbar layouts by using sequential Monte Carlo simulation. *International Journal of Electrical Power & Energy Systems, 53*, 987-993.Available at: https://doi.org/10.1016/j.ijepes.2013.06.019.

Murshed, M. (2020). An empirical analysis of the non-linear impacts of ICT-trade openness on renewable energy transition, energy efficiency, clean cooking fuel access and environmental sustainability in South Asia. *Environmental Science and Pollution Research*, *27*(29), 36254-36281.Available at: https://doi.org/10.1007/s11356-020-09497-3.

Perrings, C. (2006). Resilience and sustainable development. *Environment and Development Economics*, *11*(4), 417-427.

Roozbazar, A. (2017). *Investigation and analysis of Physical-physical critical and sensitive urban use from the perspective of passive defense of Zabol city*. Doctoral Dissertation, University of Zabol.

Rose, A., Oladosu, G., & Liao, S. Y. (2007). Business interruption impacts of a terrorist attack on the electric power system of Los Angeles: Customer resilience to a total blackout. *Risk Analysis: An International Journal*, *27*(3), 513-531.Available at: https://doi.org/10.1111/j.1539-6924.2007.00912.x.

Shorabeh, S. N., Firozjaei, M. K., Nematollahi, O., Firozjaei, H. K., & Jelokhani-Niaraki, M. (2019). A risk-based multi-criteria spatial decision analysis for solar power plant site selection in different climates: A case study in Iran. *Renewable Energy*, *143*, 958-973.Available at: https://doi.org/10.1016/j.renene.2019.05.063.

Van der Vleuten, E., & Lagendijk, V. (2010). Transnational infrastructure vulnerability: The historical shaping of the 2006 European "Blackout". *Energy Policy*, *38*(4), 2042-2052.Available at: https://doi.org/10.1016/j.enpol.2009.11.047.

Zahedi, R., Ahmadi, A., Eskandarpanah, R., & Akbari, M. (2022). Evaluation of resources and potential measurement of wind energy to determine the spatial priorities for the construction of wind-driven power plants in Damghan City. *International Journal of Sustainable Energy and Environmental Research*, *11*(1), 1-22.Available at: https://doi.org/10.18488/13.v11i1.2928.

Zahedi, R., Ghorbani, M., Daneshgar, S., Gitifar, S., & Qezelbigloo, S. (2022). Potential measurement of Iran's western regional wind energy using GIS. *Journal of Cleaner Production*, *330*, 129883.Available at: https://doi.org/10.1016/j.jclepro.2021.129883.