بسمه تعالی

جمهوری اسلامی ایران

فرماندهی کل قوا

ستاد کل نیروهای مسلح

دانشگاه و پژوهشگاه عالی دفاع ملی و تحقیقات راهبردی

دفترچه زبان انگلیسی

ویژه مصاحبه دوره دکتری (Ph.D)

رشته مدیریت راهبردی پدافند غیرعامل

سال تحصیلی ۱۴۰۲-۱۴۰۱

1. Today, Passive Defense as a necessity and broad area in all aspects of economic, cultural, political, technological and social approach of prevention and deterrence, plays a vital role in preserving Islamic values, preserve the honor of Iran, to reduce vulnerability in key parts of the country as well as promoting resource efficiency and power management in different areas. In addition to defending the land, passive defense is to defend beliefs and values against the dangers that threaten the country, with increased resistance, maintaining morale and cohesion of the people against the threats, through attention to cultural and religious infrastructure. This research utilizes library studies, content analysis and interviews with experts in the field of Islamic culture, passive defense and entrepreneurship to study and analyze the promotion of passive defense culture from the perspective of Islamic values and the role of the custodian organizations of the cultural and educational sphere in the country in the context of entrepreneurial and innovative actions.

2. The level of potential losses that a society or community considers acceptable given existing social, economic, political, cultural, technical and environmental conditions. In engineering terms, acceptable risk is also used to assess and define the structural and non-structural measures that are needed in order to reduce possible harm to people, property, services and systems to a chosen tolerated level, according to codes or “accepted practice” which are based on known probabilities of hazards and other factors.

3. Geological process or phenomenon that may cause loss of life, injury or other health impacts, property damage, loss of

livelihoods and services, social and economic disruption, or environmental damage. Geological hazards include internal earth processes, such as earthquakes, volcanic activity and emissions, and related geophysical processes such as mass movements, landslides, rockslides, surface collapses, and debris or mud flows. Hydro meteorological factors are important contributors to some of these processes. Tsunamis are difficult to categorize; although they are triggered by undersea earthquakes and other geological events, they are essentially an oceanic process that is manifested as a coastal water-related hazard.

4. Relationship building is the process of establishing and nurturing cooperative efforts with like-minded people or organizations. This is an ongoing process involving existing aligned organizations or individuals as well as non-aligned organizations or individuals that are being courted or controlled in some way. The relationship-building process is never-ending and will always present challenges as social and economic conditions change or evolve.

5. Deception is the process of using invalid or false information or pretense to convince opponents that a specific position or proposition is true when there is no factual basis for the position. Deception is also the process of trying to influence an opponent or a potential supporter to support a specific position or action based on the belief that such support will lead to desired results for the potential sup- porter. The deceiver attempts to influence the target with a promise of results that the deceiver cannot or does not intend to provide.

6. Confusion tactics are processes designed to disorient and deceive opponents regarding what is real and not real. In many ways, this is a classic propaganda method that is meant to instill fear, uncertainty, and doubt. It can involve misinformation about what has happened or what is about to happen, and is designed to disorient opposing organizations or individuals and stimulate actions on their part that are counterproductive or even self-destructive.

7.Trolling is the process of having troops respond to social media posts by commenting on existing posts in an attempt by individuals or in the name of organizations to influence, deceive, or recruit and indoctrinate. The effectiveness of this is yet to be proved, but given the propensity for trolling in social media, it is obvious that there are many who think it is effective. If nothing else, the act of trolling and opposing those with different beliefs may have a motivating effect on these “troops .

8. Social Media Warfare Rangers and Activists

Rangers are generally rather secretive people with special talents and abilities that distinguish them and set them apart. They often work and live on the fringes of society and remain secluded but in touch with the world around them. Rangers ultimately work for a cause although their methods are not always in line with social norms and conventions.

9. Vulnerability: Vulnerability is a measure of system weakness regarding the occurrence of cascading events. The concept of vulnerability involves a system's security level (i.e., static and dynamic security) and its tendency to change its conditions to a critical state that is called the "Verge of Collapse State".

10. Resiliency: Resiliency includes the ability to harden the power system against—and quickly recover from—HIGH-IMPACT, LOW-FREQUENCY events. Such events can threaten lives, disable communities, and devastate generation, transmission, and distribution systems, as well as interdependent systems such as natural gas pipelines and fuel transport and telecommunications.

11. Cyber-attacks: Cyber-attacks could incorporate, but not be limited to, combinations of the following:

Distributed denial-of-service attack in which attackers flood network resources to render physical systems unavailable or less responsive.

Rogue devices to access and manipulate the system or provide incorrect data to system operators.

Reconnaissance attacks that probe a system to provide attackers with information on system capabilities, vulnerabilities, and operation.

Eavesdropping that violates confidentiality of network communication.

Collateral damage as unplanned side effects of cyber-attacks.

Unauthorized access attacks in which the attacker obtains some control over the system, and accesses and manipulates assets without authorization.

Unauthorized use of assets, resources, or information that would feed incorrect information to system operators.

Malicious code or malware through viruses, worms, and Trojan horses.

12. Resiliency Engineering: Resiliency engineering points to the use of reactive, proactive, and predictive approaches. In this framework, system recovery is reactive to a high-impact event, but learning from past system recoveries and incorporating lessons learned can lead to proactive approaches. Damage prevention (hardening) and survivability are both clearly proactive. All of these approaches can also be predictive if the potential impacts of events are predicted, approaches for minimizing the impacts are anticipated, and ongoing steps are taken to make the power system more able to tolerate such events through hardening and systems operating practices.

13. Recovery and Response**:** Effective response after a physical attack is vital and should include the following:

Consider the safety of staff responding to the attack. Considerations need to be different than when responding to a standard equipment failure, given the potential for a follow-up threat (e.g., gunfire or blast).

Environmental impacts may differ from those of a normal equipment failure, due to both the failure mode and magnitude of the event.

The spares and replacement plan may need to be adjusted, because they are usually based on the historical failure rate of equipment. In a physical attack, the potential is greater for damage to multiple assets, requiring sufficient spares and an approach to address this aspect specifically.

Address operational recovery and response. To enhance survivability, utilities could run a series of physical breach scenarios and develop an operational framework for operating a degraded grid, for example, by diverting power around disabled equipment to load centers and increasing the output of local generation.

14. Detection: Detection includes the sensing of an adversary action by equipment (sensors) or people followed by timely assessment of whether the alarm is valid. Assessment is completed by personnel deployed to the site or by closed-circuit television (CCTV). Entry control, a means to allow entry of authorized personnel and to detect the attempted entry of unauthorized personnel and contraband, is considered part of the detection function.

15. Resilience matrix: A resilience matrix collectively provides a unifying framework to assess system resilience which may be applied productively to societies and groups, when seen as systems. Formal Resilience Matrix (RM) classifies four general resilience domains of complex systems that include a mixture of physical infrastructure and more abstract capabilities, and takes into account the performance of these domains throughout the event's occurrence and disruption.

١٦. Crisis management is the process by which an organization deals with a disruptive and unexpected event that threatens to harm the organization, its stakeholders or the general public. Bernstein emphasizes that crisis management is not a single activity. There are several levels of activity, like crisis prevention, planning, training, response and recovery.

17. Overall vulnerability is a multidimensional property of a system that describes the degree to which it is susceptible to realizing a specified degree of loss following the occurrence of an initiating threat event. Overall vulnerability consists of both protection vulnerabilities and response vulnerabilities. Protection vulnerability describes the probability of realizing damage following an initiating threat event, and considers the fragility of critical elements, target accessibility, and security system weaknesses. Response vulnerability describes the probability of realizing loss given damage considering the intrinsic susceptibilities of the target system to loss and the availability of response and recovery measures. Aggregate vulnerability is the sum of the overall vulnerability for a variety of alternative initiating threat events weighted according to their relative probability of occurrence which, in the case of malicious initiating threat events, can be influenced by visibility and attractiveness.

18. National Preparedness Goal

The National Preparedness Goal describes the five mission areas as follows:

•Prevention: Prevent, avoid, or stop an imminent, threatened, or actual act of terrorism.

•Protection: Protect our citizens, residents, visitors, and assets against the greatest threats and hazards in a manner that allows our interests, aspirations, and way of life to thrive.

•Mitigation: Reduce the loss of life and property by lessening the impact of future disasters.

•Response: Respond quickly to save lives; protect property and the environment; and meet basic human needs in the aftermath of an incident.

• Recovery: Recover through a focus on the timely restoration, strengthening, and revitalization of infrastructure, housing, and a sustainable economy, as well as the health, social, cultural, historic, and environmental fabric of communities affected by an incident.

19. A crime prevention strategy based on evidence that the design and form of the built environment can influence human behavior. CPTED usually involves the use of three principles: natural surveillance (by placing physical features, activities, and people to maximize visibility); natural access control (through the judicial placement of entrances, exits, fencing, landscaping, and lighting); and territorial reinforcement (using buildings, fences, pavement, signs, and landscaping to express ownership).

20. Primary infrastructure systems (e.g., utilities, telecommunications, transportation) whose incapacity would have a debilitating impact on the organization's ability to function.

systems and assets, whether physical or virtual, so vital that the incapacity or destruction of such may have a debilitating impact on the security, economy, public health or safety, environment, or any combination of those matters, across any federal, state, regional, territorial, or local jurisdiction .

21. An emergency operations center is the protected site location where management decisions are made and coordinated responses are orchestrated related to an emergency incident. It is designed and equipped to provide staff support to commanding officers in coordinating and guiding response to emergency incidents. EOCs may be established at the regional or local installation level. EOC may range in size from dual use conference rooms to a complete standalone facility.

22. Physical or logical facility, encompassing all necessary infrastructure required to facilitate nationwide information-sharing between one or more federal, state, and/or local law enforcement entities, dedicated to the integration of multiple diverse data sources within a defined functional domain. A collaborative effort of two or more agencies or program offices who provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorism related activity by applying the concepts of fusion, and to provide a means of intelligence dissemination.

23. Passive defense (with high emphasis on pre-crisis management) is any unarmed act which results in reducing damage to and maintaining the safety of human resources, buildings, installations and equipment against natural and manmade crises. Passive defense is a set of unarmed actions that increase inhibition, reduce vulnerability, keep up vital activities, promote national sustainability and facilitate crisis management, and ultimately, provide national security.

24. Weapon of mass destruction (WMD).

Any device, material, or substance used in a manner, in a quantity or type, or under circumstances showing an intent to cause death or serious injury to persons, or significant damage to property. An explosive, incendiary, or poison gas, bomb, grenade, rocket having a propellant charge of more than 4 ounces, or a missile having an explosive incendiary charge of more than 0.25 ounce, or mine or device similar to the above; poison gas; weapon involving a disease organism; or weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

25. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. The criticality of national infrastructure and associated key assets became an important issue when President Clinton issued Executive Order 13010 (EO-13010) in 1996. This executive order established a Presidential Commission on Critical Infrastructure Protection (PCCIP). The commission was chaired by Robert Marsh and subsequently became known as the Marsh Report. It defined critical infrastructure in terms of "energy, banking and finance, transportation, vital human services, and telecommunications." The Marsh Report was the first publication to use the term critical infrastructure and has become one of the foundational documents of CIP.

26. Certain National Infrastructures

Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures include telecommunications, electrical power systems,

gas and oil storage and transportation, banking and finance, transportation, water supply systems, emergency services (including medical, police, fire, and rescue), and continuity of government. Threats to these critical infrastructures fall into two categories: physical threats to tangible property ("physical threats"), and threats of electronic, radio frequency, or computer-based attacks on the information or communications components that control critical infrastructures ("cyber threats"). Because many of these critical infrastructures are owned and operated by the private sector, it is essential that the government and private sector work together to develop a strategy for protecting them and assuring their continued operation.

27. Risk analysis

Risk analysis is a sophisticated technology developed over the past 250 years to estimate the potential for financial loss in games of chance. In modern times the technology has been applied to a wide variety of disciplines in engineering, social and political science, and, of course, the stock market. At the heart of risk analysis is a simple idea-risk is expected gain or loss under uncertainty. In its simplest form, risk is expected loss: R = PR(C) C, where PR(C) is the probability of an event occurring with a gain or loss equal to C. In the study of CIP, C is most often defined as consequence from a disastrous event. Consequence can be measured in casualties, dollars, or time. Quantitative risk analysis is a form of rational actor behavior that assumes rational people try to maximize their gain or minimize their loss.

28. Return on Investment (ROI)

Making investments in infrastructure is called resource allocation and has a diminishing return-the point at which return on investment (ROI) no longer increases as more money is spent to prevent or respond to a CIKR collapse. Diminishing returns must be incorporated into CIP resource allocation, because without it, resources are wasted. ROI is typically measured in terms of reduced risk per invested dollar. The point at which further investment is no longer advantageous is a policy decision.

29. Threat

Threat is typically associated with human attacks-terrorism-while natural disasters are typically associated with a hazard such as an earthquake or hurricane. When convenient, threat and hazard will be used interchangeably, here. In both cases, an asset must be associated with threat or hazard to make sense. Thus, threat-asset pairs such as malware hacker-Internet Web site, hurricane-house, thief-bank, and so on must be paired together before PR(C), T, V, or C has any meaning.

30. Vulnerability

Vulnerability is Physical feature or operational attribute that renders an asset likely to fail due to a given hazard. The probability of failure if attacked or subjected to the threat. Also Risk is also not vulnerability or threat. These two terms are often mistaken for risk, because they are closely related to risk. Generally, vulnerability is a weakness in an asset that may be exploited to cause damage. It can be quantified as a probability, but it is not risk, because it is not expected gain or loss. Similarly,

threat is a potential to do harm that can also be quantified as a probability, but it is not a form of risk for the same reasons as vulnerability. Generally, threat can be quantified as the probability of an attack or catastrophic event and assigned a number between zero and one.

31. Competitive Ecosystems Progress (CEP)

The Competitive Ecosystems Progress (CEP) says that competitive ecosystems tend to eliminate all but one competitor, because sooner or later, one competitor gains a small advantage over all others and grows faster and becomes fitter than all others. This leads to a monopoly, in general, which reduces redundancy and diversity. CEP diminishes resilience, largely because monopolies are optimized organizations that tend to build optimized (profitable) systems. In general, critical infrastructure systems abhor competition and tend to become monopolies, which is a form of "putting all your eggs in one basket.

32. Public criminology

Public criminology is an approach to criminology that disseminates criminological research beyond academia to broader audiences, such as criminal justice practitioners and the general public. Public criminology is closely tied with “public sociology”, and draws on a long line of intellectuals engaging in public interventions related to crime and justice. Some forms of public criminology are conducted through methods such as classroom education, academic conferences, public lectures, “news-making criminology”, government hearings, newspapers, radio and television broadcasting and press releases. Advocates of public criminology argue that the energies of criminologists should be directed towards "conducting and

disseminating research on crime, law, and deviance in dialogue with affected communities." Public criminologists focus on reshaping the image of the criminal and work with communities to find answers to pressing questions. Proponents of public criminology see it as potentially narrowing "the yawning gap between public perceptions and the best available scientific evidence on issues of public concern", a problem they see as especially pertinent to matters of crime and punishment.

33. Categories of Critical Infrastructure Dependencies (Frederic Petit et al, 2015):

As Rinaldi, Peerenboom, and Kelly state, “it is clearly impossible to adequately analyze or understand the behavior of a given infrastructure [organization] in isolation from the environment or other infrastructures” (Rinaldi, Peerenboom, and Kelly, 2001). Critical infrastructure is thus in constant interaction with its environment, using and transforming inputs from the environment to provide outputs to the same environment (Figure 3). The interactions between critical infrastructure and its environment can be characterized into three categories:

- Upstream dependencies. The products or services provided to one infrastructure by another external infrastructure that are necessary to support its operations and functions.
- Internal dependencies. The interactions among internal operations, functions, and missions of the infrastructure. Internal dependencies are the internal links among the assets constituting a critical infrastructure (e.g., an electric generating plant that depends on cooling water from its own onsite water well).

- Downstream dependencies. The consequences to a critical infrastructure's consumers or recipients from the degradation of the resources provided by a critical infrastructure.

34. The Biological and Toxin Weapons Convention (BTWC) (The USA Countering Weapons of Mass Destruction2014).

The BTWC established the first multilateral treaty banning the development, production, or stockpiling of an entire category of weapons. The BTWC prohibits parties from developing, producing, and stockpiling biological agents and toxins in types and quantities that have no justification for prophylactic, protective, or other peaceful purposes. The BTWC does not prohibit the biological agents or toxins themselves, but rather certain purposes for which they may be employed. Parties agree to the voluntary exchange of confidence-building measures "in order to prevent or reduce the occurrence of ambiguities, doubts, and suspicions and in order to improve international cooperation in the field of peaceful biological activities." The confidence-building measures consist of six measures, including exchange of data on research centers and laboratories; national biological defense research and development programs and outbreak of infectious diseases and similar occurrences caused by toxins; encouragement of publication of results and promotion of use of knowledge; declaration of legislation, regulations, and other measures; declaration of past activities in offensive and/or defensive biological research; and development programs and declaration of vaccine production facilities.