

## **Analysis of the importance of the spatial data infrastructure in establishing societal security**

Malek Mohammad Maleki\*<sup>1</sup>, Abas Askarzadeh<sup>2</sup>

1. Employee of Ahvaz Power Distribution Company.

2. Employee of Ahvaz Power Distribution Company

---

### **ARTICLE INFO**

---

#### **Article History**

Received 14 April 2017

Accepted 10 June 2017

#### **Keywords**

Spatial infrastructure

Information and

Communications

Technology

Societal security

Critical infrastructure

### **ABSTRACT**

---

Information is one of the fundamental needs in managing various issues. In fact without possessing exact, reliable, and on-time information implementing optimal management is impossible. A development which is based on shrewdness and acumen is dependent on having proper information and make decisions and planning based on several types of information. The majority of the information in organizations in various affairs from decision-making, decision-taking, management, planning, execution and even daily operation have a spatial essence. Therefore, to achieve continuous development based on shrewdness, it is inevitable to, produce, access, and employ proper, reliable, and high-quality spatial data in the procedure of decision-making and planning for the regular course of affairs in an optimal manner. The infra-structure for the spatial data goes beyond a spatial database. In fact SDI is the host for the spatial data, documentaries about data and metadata, instruments to find, display, and assessing data and displaying the inventory, making maps, creating a website, and methods and methods for an easy access to the mentioned data. The spatial data infrastructure is one of the influential elements in the continuous development. The spatial data infrastructure looks for establishing effective relationships between people and the spatial data. The infra-structure for the spatial data includes two fundamental sections of spatial data and share ability and in terms of societal security is considered as part of the vital resources of the state. Due to this, in discussions about society considering the security considerations in the spatial infra-structure is necessary but the systemic approach requires that consider it as a vast generality. In this paper the author by noting the specificity of the spatial data talks about the importance and the necessity of considering the resulting security discussions and social issues in designing and implementing the spatial data infrastructure.

---

### **Introduction**

Today the continuous development is one of the key concerns of various societies. Knowledge is defined as the basis for continuous development. Knowledge is acquired by means of information. Information is the product of processing data. Due to this it can be said that high-quality data is considered as one of the vital factors in decision-making toward continuous development and on the other hand studies which are being carried out indicate that %80 of the existing spatial data are essentially spatial (Abdolfattah, 2002). Due to this, having high-quality and applicable spatial data plays an important part in the continuous development of a society. The existing problems in making use of the spatial data can be classified under the four areas of existence of spatial data, accessibility of spatial data, applicability of spatial data, and the amount of using spatial data:

-The first problem for the user of spatial data is about the existence of data in a way that in the existing system there is a lack of data in some cases and there is encountering one subject by several state organizations in a corruptive manner in some others.

-Accessibility of the required information is another problem for the user of spatial data which is due to an improper information distribution by organizations about the existing spatial data in the pertinent organization and also lack of appropriate policy making about presentation of data.

-Another problem which exists in alignment with this issue is the ability to use data and in other words is the level of compatibility of the data with the need of the user.

-The other problem is the amount of using spatial data. Contrary to what is expected, in most cases even in case of the existence of the data and its accessibility and its appropriateness in terms of quality and applicability, the amount of using spatial data is negligible.

Assessing the performance of the spatial data substructure is too complicated and difficult. The cause of it is that the very infrastructure of the spatial data is complicated and its building blocks have several aspects ( Mansourian (2005).Due to the justification of the consumption of resources and the efficiency of the spatial data infrastructure and some other reasons interest in studying on this has grown in the recent years and multiple studies have been done on this issue at various levels toward this issue (Crompvoets,2004).

To resolve such a problem there is a need to a mechanism which makes the efficient accession to the high-quality spatial data at multiple layers of the society possible. This substructure is defined under the title of spatial data infrastructure. The spatial data infrastructure makes accessibility, retrieval, and the distribution of spatial data possible under a safe and of course simple framework for a vast array of users. (Poorebrahimi, 2010). In other words, this substructure looks for developing effective relationships between people and the spatial data through policy making, standardization activities, and creating networks (Zargani, 2011).

Create substructure of the spatial data during the current decade is considered as one of the key constituents of the spatial data management (Lemmens ,2011).Today monitoring and assessing the substructure of spatial data is one of the key challenges in this area to which more attention should be paid both theoretically and practically because no comprehensive method is introduced yet to assess SDI. Due to this, during the recent years researchers in this field are trying to introduce a method to assess SDI that of course each of them has dealt with this issue from a different viewpoint( Williamson,2005). An appropriate summation of these two methods is given in (Crompvoets,2004).By noting the issue of security while exchanging spatial data it is recommended to give an evaluation of SDI from this viewpoint.

### Systemic View

Systemic approach is a scientific method to identify and analyze human phenomena in current world. The key attitude in this method is to present a holistic view compared to the entire constituents of a system whether individuals, various cases of hardware, software, reciprocal diplomacies, and so on to make progress in the current dynamic and changing environment. The world around us is made up of totalities called system. Each totality is made up of constituents that interact with each other and with other systems in the world to actualize a specific goal. What differentiates the elements of this system from elements of other systems is the difference of goal which this element has due to the membership in this system with another element in another system. In other words the goal for activity in a system is the same as the goal for activity in each part of it.

Systems have characteristics which don't necessarily come from the sum of its constituent's features. Thus to recognize any system it can't be broken down into its constituents. In fact a system is something more than the sum of its constituents and it's for the manner of arrangement of constituents and the cooperation among them.

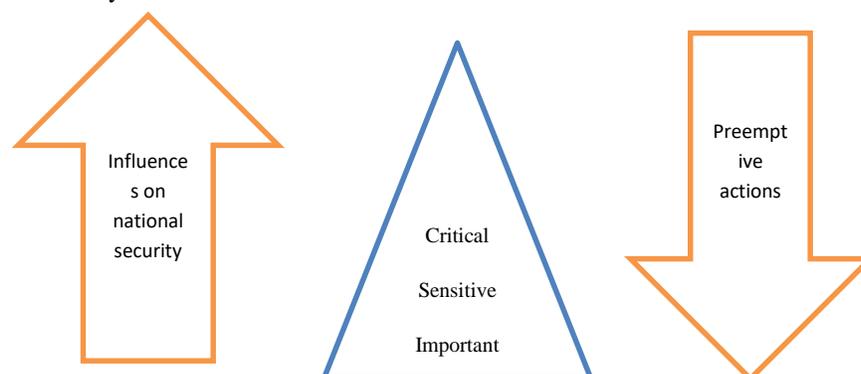
The systemic view besides having a holistic and indecomposable attitude is founded on another concept called "dynamic view". Dynamic view commits decision makers to pay attention to the behaviors and changes in a system in the course of time in order to make decisions about it.

By noting the undeniable complexity of the current world and the speed of events in it the systemic view is the only way to have a correct understanding of and present proper solutions to resolve issues and perform multiple activities(Giff,2008).

### Security Levels

From security point of view, the entire centers and domains should be classified. From this viewpoint three groups are defined as "critical", "sensitive", and "important" which is observed in figure No.1.

Figure 1. Classification of security levels



The critical centers and domains are the ones which the annihilation or the creation of a partial disturbance in all or part of it leads to the occurrence of crisis and considerable damages in the political system, guidance, control and management, economic and manufacturing, backup, communicative and driving system, social and defensive with a level of trans-sectoral or impressionability at the countrywide level.

“Sensitive” centers and domains consist in the ones which devastation or the making disorder in whole or in part of them lead to the rise of crisis, harm, and serious and perilous damages in the political system, guidance, control and management, economic and manufacturing, backup, communicative and driving system, social and defensive with a regional or sectional level of impressionability.

“Prominent” centers and domains consist in the ones which devastation or making disorder in whole or in part of them limited harms and damages may be inflicted upon the political, social, and defensive system with regional and localized levels of impressionability (Crompvoets,2008).

### **Information warfare and offense**

The issue which should constantly be taken into consideration in security investigations is the difference between offense and warfare. These two categories should be considered as distinct since the approaches to deal with them are different. “Offense is committing or quit doing something which is punishable in law”(Mansourian,2011). Offense has mostly ethical and social aspects and is condemned in all nations and schools of thought. The purpose of offenses is usually financial and social issues but “warfare” is the hostile behaviors of states against each other which is carried out with an aim of destruction, bring under domination, and exploitation (Crompvoets,2008). In fact, wars have a political aspect and the colonizing countries will spare no effort although against the ethical principles to reach their vicious goals. The entirety of an enemy’s attempts to have hostile behaviors is to aim the social security of a society. Therefore, the key point in wars is to put the social security in jeopardy. Murder is a crime but murdering a nuclear scientist by agents of a foreign state which were done to decelerate the nuclear developments of a country are the sub-branches of warfare.

Approaches in the war by noting its considerable costs, success with a high risk, overshadowing the entire resources of the state, and increase in the military power of the entire states have oriented toward a war without physical weapons.

Manufacturing and storing military weapons have immense costs. For instance, manufacturing a high-tech missile may cost some hundred thousand dollars. At the same time if that missile is going to be used in a worthless site its manufacturing cost is wasted. Another point is that in some situations that missile injures/hits the friendly forces like the event which occurred in the vicinity of the city Karaj and besides inflicting huge financial losses killed some military forces such as a commander. Thus it can be deduced that the physical war has lots of costs and risks or another example is the presence of the spies from one country in another country is so dangerous for the country which dispatches spies. Because after long-term training, the spy may be killed by accident or intentionally. Worse than that is the condition in which the spy is arrested and his/her information are used against the belligerent country.

But when the overbearing countries can totally reach their vicious goals by means of electronic devices which are based on information and communications technology, whether in terms of intelligence (i.e. before an attack) or during a military attack, there is no reason to tolerate the heavy losses and the high risk of physical war. In the recent years the belligerent countries have been successful in toppling several governments which worked against their wills without spending any money directly in a physical war directly. In fact by a negligible cost and a low risk the entire goals of a military war are being actualized through information warfare.

Today in alignment with the development and rise of modern technologies such as information and communications technology the value of information in increasing the deterrence power and establish superiority in war plays a determining role. The two main reasons for an increase in the importance of information in war can be mentioned as follows:

- 1- The huge increase in the amount of the information produced in the current world.
- 2- Establishing the capabilities to process and analyze data delicately.

Therefore, According to the avowal of all experts, information is introduced as the key necessary source for the entire activities at several levels whether personal, organizational, and national.

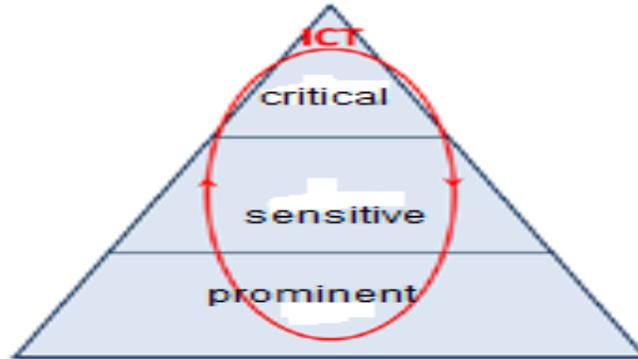
Therefore, preserving the superiority at the political level in each country either in conditions of peace or in war has a direct relationship with their information superiority. By noting the high value of information, some conflicts may arise among competitors at all levels to preserve the information superiority. Such conflicts which don’t arise in a traditional manner are called information warfare. The strategy for the information warfare is in the manner that after gaining the required information in various areas whether political, economic, military, social, and so forth, the enemy studies the weak and vulnerable points and in a purposeful and planned manner makes use of arms in a concentrated way to attack the weak points and inflicts the most possible harms.

Information warfare consists of a definite operation to preserve the consolidation of the information system of the home country against the destruction, detachment, or the exploitation of the enemy while simultaneously exploits, annihilates, or destroys a hostile information system and carries out the procedure of achieving information superiority to make use of forces (Giff.,2008). In this study the utmost effort of the authors go toward explaining the hostile approach of the enemy to achieve and make use of information specifically local information to achieve their vicious intentions.

### **Information and Communications Technology Domain as an infrastructure for infrastructures**

In all wars the concentration of the enemy is directed toward annihilation and disrupting the critical substructures since as it was stated in section three, the critical domains' level of influence is trans sectorial and at the countryside level. In other words, the enemy is intended to inflict the greatest harm against a country at the lowest cost. Domains such as agriculture, water, food, general health, emergency services, government, defiance industries, energy, transportation, banking affairs, stock exchange, chemical and hazardous materials, Postal service and transportation all of which are considered as substructures of a country but information and communications technology (ICT) is the Infrastructure for infrastructures. Since today, in alignment with developments in technology specifically information and communications technology, the entire domains are intertwined with this domain and any disruption in this domain leads to disruption in the entire domains. (Figure 3) Contemporaneously with the arrival of ICT in the domain of societal security, the entire management and communicative procedures among several sectors were entrusted to it. Thus, by considering the enemy's approach in reducing the cost of war and inflicting the utmost harm, ICT domain is the main domain which creating disturbance in it influences the entire substructures or in other words influences the whole company (Giff., 2008).

Figure No.2. Tran- sectorial influence of ICT to catch hold of management procedures



### **Spatial information as a specific subseries of Information and Telecommunications Technology**

As it was stated in the previous sections, information and telecommunications technology (ICT) is considered as the infrastructure for infrastructures and a critical element in societal security. From among several types of information, spatial information has a specific feature which increases its role in the societal security compared to other types. Communication channel can be classified into two general types of serial and parallel. While communication in parallel manner instruments to transfer information are words which are read or heard. To become audible, words should enter the ear or eye in a serial and parallel manner and reach the brain through channels in the nervous system. At that time in case of being meaningful the brain analyzes it and it will be understood. The main feature of the serial information transfer is that studying or listening to a subject might be very time-consuming. For instance, studying a one-thousand page document or speaking for ten hours consumes too much of somebody's time. Another point is that to read or listen to a specific part of interest, one should look of it and this can be time-consuming as well. For instance, finding a specific point in a one-thousand page document isn't an easy job although in case of finding it, it might be necessary to study the pages prior to it to get the prerequisites to understand it. Another feature of serial communications is that they aren't sensitive to wrong data. That is, the false and true information can be put together easily because the relationship between words in comparison with the parallel method is lesser. Another weak point in this method is that lots of issues can't be transferred via words. The layman's level example for it is human feelings and sensations and its technical example is maps. Basically, if we want to present a map in the shape of a text, it loses all of its privileges and then anything called the spatial information system will be meaningless.

But in the parallel communications channel, the instruments of transfer instead of words are pictures. Maps are falling under this category due to their pictorial nature. In this type sequence and order are meaningless and the individual gets his/her intended information by keeping their eyes focused on various parts of a map. The map's information is in a manner which can't be put under a framework. Because there is so much information in a map which put them in writing is impossible. For example, consider a thematic map which demonstrates the entire mines of the country by proper symbolization throughout the state. After taking a thorough look at it by an expert in special sciences, the coordinates, distance relations between mines,

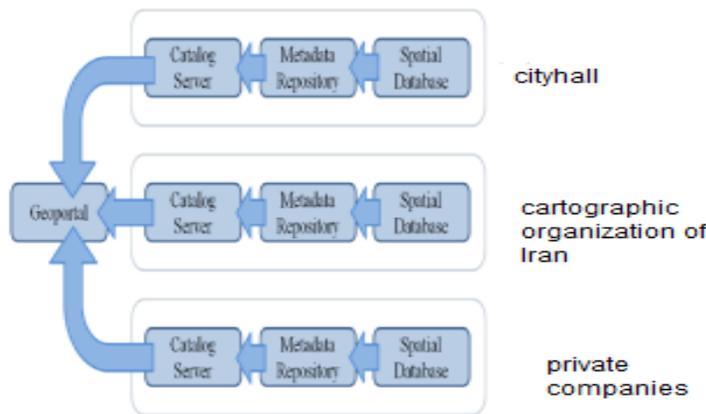
between mines and other significant geographical features such as frontier, rivers, etc. Density of mines is understood by the expert through considering the types and the distribution of mines and many other things. Therefore, sometimes a map can bear more information than thousand pages of documents or hours of lectures. Another positive point is the transfer of information in a parallel fashion is that the relations between the entire geographical features are obvious and by producing error in any geographical feature its direct influence on other geographical features becomes visible. Thus, it can be stated that the parallel relation in comparison with the serial one is more error-sensitive. Another feature of the maps is that to analyze and comprehend then an expert in spatial sciences is needed and laypersons usually can't completely realize the entire things which an expert understands from a map(Giff.,2008).

Noting the above-said points, all the words which were stated in the previous sections about the importance of information and communications technology in the societal security is more intense for the spatial data.

**The infrastructure of spatial data from societal security view**

In previous sections the importance of information specifically the spatial data in the societal security was elaborately discussed. Domain of information and communications technology, as its name signifies, is made up of two parts of information and communication. These two sections don't have any workability separately. Having information without any capability to share it is totally useless. Also, the ability to communicate without having any information is meaningless(Giff.,2008). Thus, the relation between information and communication and their subsections constitutes a complete system. Within the domain of spatial data, the most complete domain in terms of the mixture of information and communication is SDI. In fact SDI is the illustration of ICT in the spatial sciences since like ICT, SDI is made up of the two parts of the spatial data and sharing it which is indicated in figure No.4.

Figure No.4-A schematic view of the capability of SDI in improving the accessibility to the spatial data of the country



Noting the entrance of SDI in the two domains of information and communication, its vulnerability from the viewpoint of societal security is in two domains; that is information is vulnerable to being robbed. Thus, SDI contains the most significant information for the enemy and at the same time is vulnerable to the robbery of data more than any other domain in the spatial data systems. Because of SDI's higher level of vulnerability in the two domains of information and communication and the concentration of the enemy to achieve this information at any rate, the necessity to take security measures for it is vital. Necessity to provide security is important to the extent that the lack of existence of an SDI in comparison to the existence of it at the highest level and without security measures has priority from the point of view of societal security. Since the societal security has priority over the entire state affairs, so discussing the security of SDI holds specific significance and in case the emergence of the societal security necessitates, the possibility of seizing the activities which are relevant to SDI is possible in our country just as this big problem still exists in the way to make an effectual SDI and prevents its constitution.

Noting the points which were stated in part two on the importance of considering the security considerations and the systemic approach, SDI is a system which has various parts one of whom id security. Thus, security in SDI consists in two parts: the subsystem of security and providing security for the remaining subsystems. In this respect security can be viewed as a specific and of course a very important subsystem of SDI. A secure SDI is the product of unity among its constituents which security is one part of it.

Beside the above points, security is dynamic. It means that always individuals who intend to impair the societal security following the blockade of unauthorized ways to access and steal information, look for making new and creative ways. Thus, defensive actions should always be dynamic toward these attacks. Thus thinking that it's a static SDI, which means that it's designed one time and after that continues its job without undergoing any change is secure is an inane imagination. Thus, in

the preliminary design of SDI, its dynamicity is considered and the authorities by realizing the importance of spatial data from the viewpoint of societal security are constantly looking for seal the vents against the infiltration of factors that inflict harm on the system.

Thus, by noting the entire points being mentioned, the security of SDI contrary to the beliefs of the experts in the spatial sciences isn't a secondary subject but is a part of SDI, meaning that it is an issue which should be noted at the onset of designing. Separating SDI from security is a mistake which has brought several obstacles whether technical or non-technical in the way of producing an effectual SDI; since societal security is one of the main issues in estimating the profit or cost of an SDI and can readily tip the scales in favor of both sides.

### Conclusion

Noting the huge cost and the high risk of success, overshadowing the entire resources of the country and boosting the military power in all countries, the inclination of wars had changed toward wars without physical warfare or information warfare. Information warfare is a series of actions which are done to keep the information dominance. Spatial data is the most significant type of data which can tip the scales in favor of the side which has dominance in terms of spatial data in comparison with the other side. SDI includes the two domains of information and sharing it. Thus in both parts stealing information may occur for SDI. Noting the high vulnerability and also the considerable significance of the spatial data for an enemy, providing security for SDI is of great significance in a way that the societal security can take a halt to the establishment of a SDI, no matter how much is it to the advantage of the country. Thus considering security as a constituent of SDI is a reality that one should accept. Therefore, considering the security measures isn't a story apart from SDI and should be considered in all respects from designing to usage.

### References

- 1-Abdolfattah, A. (2002). "What are crime and Criminalization". Legal and Judicial Journal of the Judiciary, No.135, pp.41-160.
- 2-Hasani Pazoki, S., Hakimpoor, F. (2011) "Displaying GML through extension to XSLT (MA thesis proposal), Tehran University, Technical Faculty, Department of Cartography Engineering.
- 3-Poorebrahimi, A., Bonabi, S., (2010). "Familiarization with Principles of Environmental Security in Information Technology.", 1<sup>st</sup> publication, 2010, Islamic Azad University, (Electronic Branch).
- 4-Zargani, S.H., A'azami, H. (2011). "Analysis of the Military-Security Considerations in planning and locating the centers and the military settlements emphasizing Razavi Khorasan Province, Journal of Management Studies in Iran-The Humanities Teacher, vol.15, pp.141-161.
- 5-Lemmens, M.J.P.M. (2001) An European perspective on Geo-Information Infrastructure (GII) issues. [Online]. <http://www.GIS Development.net>.
- 6- Mansourian, A. (2005) Development of an SDI Conceptual Model and Web-based GIS to Facilitate Disaster Management (PhD Thesis). K.N.Toosi University of Technology, Faculty of Geodesy & Geomatics Eng.
- 7- Masser, I. )2007( Building European Spatial Data Infrastructures .ESRI Press, Redlands, CA.
- 4)Vandenbroucke, D., Crompvoets, J., Vancauwenberghe, G., Dessers, E., Orshoven, J.V. (2009). A Network Perspective on Spatial Data Infrastructures: Application to the Sub-national SDI of Flanders (Belgium), Transactions in GIS, Vol. 13, PP. 105-122.
- 8- Williamson, I., Grant, D., Rajabifard, A. (2005) Land administration and Spatial Data Infrastructures. FIG Working Week 2005 and GSDI-8.
- 9- Crompvoets, J., Bregt, A., Rajabifard, A., Williamson, I. (2004) Assessing the worldwide developments of national spatial data clearinghouses. International Journal of Geographical Information Science, Vol. 18, No. 7, PP. 665-689.
- 10- Budhathoki, N.R., Nedovic-Budic, Z. (2007) Expanding the SDI knowledge base. In H. Onsrud (Ed.), Research and theory in advancing spatial data infrastructure, Redlands: ESRI Press, PP. 7-32.
- 11- Giff, G.A., Crompvoets, J. (2008) Performance indicators. A Tool to Support Spatial Data Infrastructure Assessment. Computer Environment and Urban Systems.
- 12- Crompvoets, J., et al. eds, (2008) A multi-view framework to assess SDIs Space for Geo-Information (RGI). Wagen-ingen University and Centre for SDIs and Land Admini-stration, Department of Geomatics, University of Mel-bourne, Melbourne, Australia.
- 13- Mansourian, A., Omid, E., Toomanian, A., Harrie, L. (2011) Expert system to enhance the functionality of clearinghouse services.Computers, Environment and Urban Systems Vol. 35, No. 2, PP. 159-172