Journal of Practical Management Information Systems

J. Practical MIS, 2(1): 25-30, 2021

Research Paper

Information Pollution and Its Destructive Role as a Tool of the Domination System in the Information War with Other Countries

Majid Jangizehi*[a] , Abdolreza Rasouli Kenari [b] , Javad Hosseinkhani [c]

[a] Department of Computer Engineering, Sistan and Baluchestan Science and Research Branch, Islamic Azad University, Zahedan, Iran

[b] Faculty of Electrical and Computer Engineering, Qom University of Technology, Qom, Iran

[c] Department of Computer Engineering, Zahedan Branch, Islamic Azad University, Zahedan

Received: 18 December 2020 Revised: 24 January 2021 Accepted: 15 February 2021

Abstract

The world today is an infinite collection of data. People try to discover and make meaningful data and turn it into information according to their needs. Meanwhile, governments are increasingly competing in the production and use of this information. However, along with the progress that has been made in this realm, problems such as information pollution are increasingly emerging. Information pollution is one of the powerful tools of governments to penetrate the body of other countries and influence them through information warfare; For this reason, every country tries to have the power of attack and at the same time strong defense against hostile governments, based on information warfare. In this article, after reviewing information pollution and its two-way role in attacking and defensing, the methods of information pollution and how this pollution affects the information war in today's world are discussed. This study shows that information pollution is one of the most important factors that threatens the information bases of any country by building a platform for information warfare. Therefore, the experts should look for solutions to safely pass through information pollution and, if it occurs, minimize its effects and increase the security of data and information of the system and the organization.

Keywords: Information, information pollution, information warfare, domination system.

How to cite the article:

M. Jangizehi, A. Rasouli Kenari, J. Hosseinkhani, Information Pollution and Its Destructive Role as a Tool of the Domination System in the Information War with Other Countries, J. Practical MIS, 2021; 2(1): 25-30,

1. Introduction

Nowadays, different societies use different methods and channels to send and receive information. This has been facilitated by the development of information and communication technologies, computer networks and the Internet. Apart from that, such an approach has created negative consequences such as a flood of scattered, repetitive and inaccurate information. (Rezayi, 2016) Information in the present age is rapidly created and published in less than a fraction of a second around the world using electronic communication tools. The speed of the information production and transmission cycle has increased so much that it has caused an explosion of information. One of the consequences of information explosion is information pollution. Information gathered from different sources may be contradictory; Additionally, there are many sources of information in which incorrect information has been published intentionally or unintentionally. With increasing volume, it is very difficult to control the dissemination of information; Thus, in an environment where there is no control over the dissemination of information, some people contaminate information by disseminating false or misleading information. (Jistan and Jistan, 2014)

Contamination of information with political, social, etc. impacts causes an imbalance in the power of organizational information of society in relation to reliable and confirmed facts. In the long run, such an imbalance weakens a country's intelligence power relative to other countries, especially hostile powers. This happens without any ordinary

physical attack, which is interpreted as an information war. (Pourasad et al.,2015) For this reason, the concepts of information, information pollution and information warfare with their relationship with each other are explained and then the role of information pollution in the occurrence of information warfare as a tool of the domination system is investigated. In the end, summary, discussion, conclusion and suggestions are presented.

1.1. Literature Review

Human beings as a real entity and at the macro level of organizations and governments as legal entities have long been associated with the concept of data and information. The term 'information' in this article means the content or meaning of a message. In most wars and confrontations between countries, the main goal has been to influence the enemy's intelligence systems. In a broader sense, information systems include means or methods by which specific knowledge or beliefs can be gained. (Bahramsari et al., 2015) In other words, information systems are a complete set of knowledge, beliefs and decision-making processes of the enemy, so the desired result will be achieved when the enemy receives messages in a way that convinces the cessation of war. (Sherbati et al., 2014) Toffler in his book Shift in Power: Knowledge, Wealth and Violence at the turn of the twenty- first century, for the first time comprehensively addressed the possibility of information pollution. (Norouzi, 2000) The following issues have been examined by different researchers: The Level of Information Pollution in Different Scales of Work Environments (Iqbal et al, 2020), Information Pollution and Its Moral Reflections in the Behaviors of Members of Postmodern Society (Wang, 2020), Information Pollution Management As a Conceptual Study Among the Learning Organization Workforce (Yang et al, 2018). Bahramsari et al. also examined the information in social networks (Bahramsari et al., 2015) and Benvinist investigated the possibility or impossibility of free access to information that can be cited in the contaminated space. (Benvenisti, 2017) Increasing advances in information science have led various systems to examine the possibility of domination and attack on other countries through indirect wars called information warfare. Similarly these concepts have been addressed by different people: A Way to Use Electronic Warfare and Information Signaling in Network-based Warfare (Ahangar et al, 2020), The Idea of Intelligence Warfare and Infiltration Operations As a Tactic in US Cyber Attacks (Straub and Traylor, 2018), The Defense of Information in the Context of Electronic Warfare (Rezayi, 2016), Methods of Countering Cyber Attacks Based on Information Contamination by Enemies in Water Treatment Plants (PoursoltanMohammadi et al., 2017), National Security Threats in Iran to Prioritize Countermeasures against Routine Physical Attacks and Cyber-Intelligence Intrusions. (Salehniya and Bakhtiari, 2018)

2. Information Pollution

There exist various threats for information. The most important of these damages are pollution, explosion, proliferation and duplication of information. Information pollution is a type of information damage. Information pollution refers to the combination of right and wrong information. (Bahramsari et al., 2015) Changes in the quality and accuracy of various information due to the entry of other elements, the existence of irrelevant information and lack of information load, as well as the overlap of information with disturbance and noise are common types of information pollution. (Norouzi, 2000) Information in the present age is rapidly created and published worldwide in a fraction of a second using electronic communication tools; Today, increasing the speed of the information production and transmission cycle has caused an information explosion. One of the consequences of information explosion is information pollution. Information collected from different sources may be contradictory. There are many sources of information in which misinformation is intentionally or unintentionally published. As the volume of information increases, it becomes very difficult to control the dissemination of this huge amount of information. Thus, in an environment where there is no control over the dissemination of information, some governments contaminate information by disseminating false or misleading information. (Aguaded, 2014) Today we are faced with huge amounts of worthless, inaccurate, incomplete and distorted information, and the current world is full of useless and inaccurate information, or in other words, contaminated information. (Norouzi, 2013)

2.1. Consequences of Information Pollution

Information pollution has different consequences. The most important of them are the following:

- Creating problems in the correct decision process (Iqbal et al, 2020)
- Reduction of search speed and accuracy (Helbing et al, 2018)
- Memory wasted due to storage of infected files
- Increasing costs due to the storage of infected and useless information (Sepiddam, 2014)
- Confusion of users due to the formation of different versions of information (Norouzi, 2013)

2.2. Ways of Contaminating Information

Information can be contaminated in a variety of ways; The most important of these methods are the following:

1. Conscious deletion of information: conscious selection and deletion of a range of information for personal or organizational reasons (PoursoltanMohammadi et al., 2017)
2. Replacement of information: Replacement of incorrect information with correct facts without the audience being aware of the information facts or being fully acquainted with it. (Salehniya and Bakhtiari, 2018)
3. Inreadability of information: Disruption of the information system due to illegible and distorted information (Abasiraei et al., 2015)
4. Information impurity: reduction, loss of purity and mixing of information in one system with information in another system. (Jung et al, 2001)
5. Lack of up-to-date information: obsolescence due to lack of information consumption (Norouzi, 2000)
6. Irrelevant information: the existence of information in the system that has nothing to do with the nature of the system and its purpose.
7. Duplication of information: Existence of duplicated information due to occupying the information source space, without any results and benefits (Talachi and Zarei, 2010)
8. Delay in sending information: With such delay, the information that was useful in its time will lose its value. (Helbing et al, 2018)
9. Non-uniformity of information: In this method, the existing information does not have harmony, uniformity, coherence and logical relationship with each other. This method of contamination is often overlooked, but can cause problems for information users and their decision-making. (Iqbal et al, 2020)

2.3. Relationship Between Information Pollution and Other Information Damages

Information pollution is directly or indirectly related to other types of information damage, the most important of which are the following:

1. Information explosion and information pollution: The existence of a huge amount of information has caused the current era to be called the information explosion era. Explosion of information is one of the types of information damage. This factor has increased the level of information pollution. The rapid formation and development of computer networks and the Internet has facilitated information pollution and increased the likelihood of its occurrence. There is a direct relationship between information explosion and information pollution; This means that the more information is produced, the more information pollution will increase. (Yang et al, 2018)
2. The proliferation of information and information pollution: Currently, the speed of increasing the volume of information is faster than the speed of its consumption, this factor causes a large phenomenon of information. Too much information is one of the information harms that has a direct impact on information pollution. In terms of time and effort, there are limitations that prevent information users from consuming information. Since there is no balance and coordination between the production of information and its consumption, the phenomenon of information proliferation occurs. (Bahramsari et al., 2015)
3. Information duplication and information pollution: Another information damage is information duplication. Some information producers and senders publish certain types of information in different information sources. This is an example of duplicated information. It should be noted that even if this information is useful, it does not need to be republished. (Benvenisti, 2017)
4. Information pollution and information warfare: The relationship between information pollution and warfare, unlike the previous cases, is reverse. In other words, information pollution at the macro level causes information warfare (Salehniya and Bakhtiari, 2018)

In the next section, information warfare is discussed as one of the most significant effects of information pollution.

3. Information Warfare

Information warfare is an offensive and defensive operation used by organizational or individual organizations with specific policies and strategic goals to exploit or destroy information contained in computers or the Internet and other networked information systems. (Sharbati et al., 2014) Information warfare is a feature of military conflict in which intelligence systems are directly or indirectly attacked or defended so that the enemy's data, knowledge, beliefs or combat potential is diminished or completely destroyed and at the same time preserve the data, knowledge, beliefs and militancy of one's own forces. (Ahangar et al, 2020) Information warfare includes, security of operations, military deception, psychological operations, electronic warfare and physical destruction to affect, degrade, or destroy the enemy while at the same time preserving the command and control capabilities of the one's own against the similar operations of the enemy in the

military dimension and diplomatic and political war in the civilian dimension. (Rezayi, 2016) Information warfare is most often due to the occurrence of battle. Battle is a set of all lethal and non-lethal activities performed to overcome the intention of an opponent or enemy. (Straub and Traylor, 2018) In this sense, battle is not synonymous with war and is not associated with a situation called a state of war. (Kiyani Falavarjani, 2016) Battle can be fought by or against government groups, government-sponsored groups or non -governmental groups. The goal of battle is not necessarily to kill enemies, but to bring them under control basically. (Poursultan Mohammadi et al., 2017)

3.1. Objectives of Information Warfare

The goals of information warfare can be distinguished at three levels, with a specific outcome at each level:

1. Information system layer: This layer contains material elements, production, transmission and storage, and attacks against information systems cause technical consequences. (Yang et al, 2018)
2. Management layer: This layer contains processes for managing and processing information that has been attacked and has created functional consequences.
3. Decision layer: This level is related to decision making and the use of information in formulating and regulating policies and decisions. Attacks at this level can have operational consequences. (Sharbati et al., 2014)

3.2. Features of Information Warfare

Information warfare is different from warfare in the general sense due to its inherent nature and characteristics. The most important features listed in various sources for information warfare are:

1. The low cost of entering the information war
2. Ultra-sophisticated technology (Ahangar et al, 2020)
3. Flexibility
4. Defects in traditional demarcations
5. Increasing the importance and role of manipulation (Rezayi, 2016)
6. Difficult problems of tactical warning and attack assessment
7. New spy challenge
8. Difficulty of forming and maintaining a coalition (Salehniya and Bakhtiari, 2018)

3.3. Types of Information Warfare

There are different types of information wars depending on the time and place, the most important of which are:

1. Command and control war: In this type of information war, the goal is to cut the connection between the structure and the enemy command from the body under his command. (Wang, 2020)
2. Targeting the commander's head: The basis of this type of information warfare is the attack on a command center, which, if carried out in a timely manner, can disrupt operations even without harming the high-ranking enemy commander.
3. Targeting the commander's neck: This operation is carried out against the command and communication lines of the command and different parts of the operation scene. Disconnecting this electronic communication leads to weakness and defeat. (Rezayi, 2016)
4. Information-centric warfare: This type of warfare occurs when the main operation is directly related to the type of information. (Sepiddam, 2014)
5. Information warfare-offensive axis: This type of warfare depends on the information technology used. It can be said that the environment of future wars will have various sensors that fully show the battlefield so that the commander can execute battle plans and programs. (Straub and Traylor, 2018)
6. Information warfare-defensive or defensive axis: In this type of war, the main importance is based on creating a defensive method in order to increase the gap between image and reality on the battlefield. In other words, the main operation is to create a situation in which the sensors of the enemy intelligence gathering devices either do not reach the information or if they do, it does not correspond to reality (Salehniya and Bakhtiari, 2018)
7. Electronic warfare: This type of warfare is done to reduce communication at the physical level such as jamming and at the combined level such as interception. (Sharbati et al., 2014)

Electronic warfare includes the following forms:

1. Anti-radar: interferes with the performance of radar by creating noise.
2. Anti-telecommunications: or targeting communications
3. Encryption: Communication of messages in the form of codes between local forces (Kiyani Falavarjani, 2016)
4. Psychological warfare: the use of information against people's minds and thoughts

The types of psychological warfare are as follows:

1. Operations against the national will (Kiyani Falavarjani, 2016)
2. Operations against enemy command
3. Operations against military forces (Jistan and Jistan, 2014)

4. Cultural war (Rezayi, 2016)
5. Infiltrator war
6. Economic information war (Pourasad et al., 2015)
7. Cyber or Internet war (Salehniya and Bakhtiari, 2018)

The methods of attack in cyber war are as follows:

1. Internet sabotage: attacks to change the content and the problem of web pages or disruption of services (Jistan and Jistan, 2014)
2. Data collection: access to classified information for espionage
3. Widespread attacks disrupting services
4. Disruption of equipment: interception or change of commands and communications by attackers in military activities in which computers and satellites are used for coordination (Pourasad et al., 2015)
5. Attack on critical infrastructure such as power plants, water supply, refueling facilities, communications, transportation, etc.
6. Perceptual warfare: operations that exploit the mass media available to them in order to influence people's beliefs and behavior. Perceptual warfare has a similar purpose to psychological operations, however its scope is broader than the practical scope of psychological operations. (Rezayi, 2016)

3.4. Information Warfare Tools

Individuals, organizations, and governments utilize basic tools to win the information war. Here are the most important of these tools:

1. Viruses: Viruses are programs that are able to replicate themselves in larger programs. Virus programs are activated when the host program starts running, which in turn multiplies the virus and infects other programs.
2. Worms: A worm is a standalone program that is increasingly replicating itself and moving from one computer to another, often over networks. The destructive consequences of this type of computer weapon can be examined from two perspectives. First, the destruction of existing information resources in the network and second, the transformation and dissemination in the network. (Aguaded, 2014)
3. Trojan horse: are programs that are hidden inside other programs and execute their function. Trojans can disguise themselves and even be included in network security programs.
4. Rational bomb: A logic bomb is a type of Trojan horse that is used to release viruses or other aggressive systems and can act as a standalone program embedded in the system by a programmer and designer. (Jung et al, 2001)
5. Back or trap doors: includes the mechanisms that the designer installs during the construction of the software to allow the possibility of secret entry into the system and the destruction of circuits during the normal operation of the system. (Sharbati et al., 2014)
6. Germs: Unlike viruses, they can affect hardware and cause severe system damage.
7. Electronic disorders: Used to block communications and, in the advanced stage, to give incorrect and excessive information. (Salehniya and Bakhtiari, 2018)
8. Electromagnetic pulses: The source of these pulses can be nuclear or non-nuclear explosions and are exploded by special forces that have penetrated into the enemy area near electronic centers and cause the destruction of electronic parts of all computers and telecommunication systems in an area. (Rezayi, 2016)

The tools discussed in this section for information warfare are each selected for attacking according to the circumstances of time and power, and each can easily and in a short time threaten and attack the national security of countries. (Salehniya and Bakhtiari, 2018) However, regardless of the type of tool selected, the study of the current increasing attacks shows the movement of countries and their defense organizations from classical wars to cyber wars based on information pollution (Pourasad et al., 2015); For this reason, in the current environment, the aristocracy of various organizations, especially organizations involved in information technology, the concepts of pollution and information warfare, along with methods to prevent, detect and deal with them, has become doubly important. (Sharbati et al., 2014)

4. Discussion and Conclusion

This article examines the concept of information pollution and its impact on the occurrence of information warfare as one of the tools of hostile governments against other countries and vice versa. In the previous sections of this article, the research background, information concepts, information pollution and information warfare, as well as the methods and relationship of these concepts with each other and their role in the security of the country were stated. The world today is based on information and related technologies; This has led various countries to try to empower their operational processes based on knowledge recognition and how to use it to improve their position. Information pollution is one of the tools of governments for information warfare to infiltrate and attack other countries; In other words, each country tries to strengthen its tools for intelligence attacks on other countries and defense against attacks by enemies. Current developments have led to a sharp increase in the volume of information in societies, and as a result,

problems such as information pollution are inevitable. However, it is necessary to prevent the occurrence of information pollution by planning and setting goals, and in case of its occurrence, by increasing its effects, the security of data and information of the system and the country will increase. It is also suggested to other researchers in future studies to use methods based on data mining, decision-making based on existing criteria and organizational management to model the problem of information pollution and information warfare.

References

[1] Abasiraei, A., Khanzade, Ch., and Pakniyat, M. (2015). Information pollution and the need to deal with it in military organizations. International Conference on New Research in Industrial Management and Engineering.

[2] Aguaded, J. I. (2014). From Infoxication to the Right to Communicate/Desde la infoxicación al derecho a la comunicación. Comunicar (English edition), 21(42), 7-8.

[3] Ahangar, M. H., Rahmati, A., and Heydari, H. (2020). The Use of Electronic Warfare and Information Signaling in Network-based warfare. Majlesi Journal of Telecommunication Devices, 10(2).

[4] Bahramsari. SH., Ahmadizade.S., and Niyazmand. M. (2015). Information pollution in social-scientific networks and providing appropriate self-archiving solutions (Case study: social-scientific networks of the Academy and Mendel). Mehr Book, 17(1).

[5] Benvenisti, E. (2017). Ensuring Access to Information: International Law's Contribution to Global Justice.

[6] GlobalTrust Working Paper Series 2017-09. University of Cambridge Faculty of Law Research.

[7] Helbing, D., Frey, B. S., Gigerenzer, G., Hafen, E., Hagner, M., Hofstetter, Y., ... and Zwitter, A. (2019). Will democracy survive big data and artificial intelligence?. In Towards digital enlightenment (pp. 73-98). Springer, Cham.

[8] Iqbal, Q., Ahmad, N. H., and Nawaz, R. (2020). Perceived information pollution: conceptualization, measurement, and nomological validity. Online Information Review.

[9] Jistan, Z., and Jistan, H. (2014). The concept of cyber warfare and the study of different dimensions. The first national conference on computer science and engineering.

[10] Jung, S. W., Sung, K. H., Park, T. W., and Kwon, H. C. (2001). Intelligent integration of information on the Internet for travellers on demand. In ISIE 2001. 2001 IEEE International Symposium on Industrial Electronics Proceedings (Cat. No. 01TH8570) (Vol. 1, pp. 338-342). IEEE.

[11] Kiyani. F. (2016). Develop an electronic warfare technology strategy and algorithm Develop a technology roadmap for emerging products in the field of future electronic warfare. Fourth National Conference on Defense Science and Engineering in the IRGC. Imam Hossein University of Officers and Guards Training.

[12] Norouzi, A. (2013). Information pollution. Information Quarterly. 15(1).

[13] Norouzi, A. (2000). Information pollution and its consequences Journal of Information Processing and Management. 10(1).

[14] Pourasad, Y. Jistan, Z., and Jistan, H. (2015) . Understanding cyberspace and the doctrine of some countries. The Second International Conference on Research in Engineering, Science and Technology.

[15] Poursoltan.M. A. H., Chehelamirani, M., and Faqihi, F. (2017) . Passive defense in the face of cyber attacks to combat intentional environmental pollution and biological attacks of water and wastewater treatment plants (Case study: Quds city treatment plant). Quarterly Journal of Environmental Science and Technology, Tehran, Islamic Azad University, Science and Research Branch.

[16] Rezayi, H. (2016). Information defense in the context of electronic warfare. Journal of Ferdowsi University.

[17] Salehniya, A., and Bakhtiyari, H. (2018).Prioritization of National Security Threats of the Islamic Republic of Iran by Hierarchical Analysis Method. Quarterly Journal of Strategic Studies in Public Policy. 8(27).

[18] Sepiddam, M. (2014). Information pollution in virtual social networks. First National Conference on Computer and Information Technology. Islamic Azad university-Sepidan branch.

[19] Sharbati, S., Meysami, H., and Soleymaniyan, H. (2014). Review of the C4I system in information warfare. 8th National Conference on Command and Control of Iran. Shahid Sattari Airforce University.

[20] Straub, J., and Traylor, T. (2018). Introduction of a Maritime Model for Cyber and Information Warfare. In 2018 International Conference on Computational Science and Computational Intelligence (CSCI) (pp. 25-29). IEEE.

[21] Wang, X. (2020). The Dilemma of Information Ecology in Postmodern Society and the Reflections of Its Practical Ethics. In Multidisciplinary Digital Publishing Institute Proceedings (Vol. 47, No. 1, p. 62).

[22] Yang, S., Iqbal, Q., Nawaz, R., and Lin, Y. (2018). Infollution (information pollution) management, filtering strategy, scalable workforce, and organizational learning: a conceptual study. Information Management and Business Review, 10(4), 1-7.