International Journal of Cyber-Security and Digital Forensics (IJCSDF) 5(1): 21-29
The Society of Digital Information and Wireless Communications, 2016 (ISSN: 2305-0012)

Cyber Operation Planning and Operational Design

Muhammer Karaman, Hayrettin Catalkaya, Ahmet Zeki Gerehan and Kerim Goztepe
Operations and Intelligence Turkish Army War College
War Colleges Command, 4. Levent/Istanbul, 34330, Turkey
mkaraman@harpak.edu.tr; hcatalkaya@harpak.edu.tr; azgerehan@harpak.edu.tr;
d065006003@sakarya.edu.tr

ABSTRACT

Improving ICT infrastructure, dramatic increase in internet usage and increasing dependence on networks have carried with cyber risks and threats. Complex, shape shifting and emerging risks and threats have systematically paved the way for cyberspace to emerge as a new domain after land, air, maritime and space. It is obvious enough that cyber threats probably continue to take part in global cyber theatre for years. However, it is sometimes hard to pinpoint at first a specific axis of cyber threats; they are generally varied merely from a simple computer code to systematic cyber strikes like targeted cyber attacks, cyber terrorism and industrial espionage activities. Due to the exponential use of cyberspace and the complex nature of cyber attacks, along with the multivariable cost they cause, it becomes a requirement for operation planners to handle cyber operations and the problems in this sphere in an operational design process. In this study, we tried to handle cyber operations in operational design process in order to comprehend, visualize and enlighten complex cyber incidents holistically and present preventive and systematic approaches by proposing a cyber operational design model. By presenting such model, we aim to help operation planners understand the complexity of cyber operations, show the advantage of using factor and center of gravity analysis (COG) that is generally handled in military decision making process (MDMP) and finally help the technical personnel to have an understanding of operational planning. With the cyber operational design presented as a sample in this study, we plan to provide the commanders with a comprehensive approach in cyber operations.

KEYWORDS

Cyberspace operations, operational design, cyber threats, cyber operational design, military decision making process (MDMP).

1 INTRODUCTION

Throughout history, there has always been a struggle of force among communities. Struggles, conflicts or fights have managed to reach up to modern times with different forms of tools, tactics and techniques [1]. Strategies are developed to direct and command armies and also envision the enemy and its tactics. These strategies mainly vary depending on the commanders' intents that form the desired end state on the enemy. When we compare two outstanding military strategists, Sun Tzu and Clausewitz, and their work in order, "The Art of War" and "On War", we can see some differences in them. For example, the concepts of Sun Tzu generally imply that the force should be the last resort to apply. If the enemy is defeated without fighting that is better or to take a state untouched is recommended by him [2] On the other hand, Clausewitz emphasizes theoretically the importance of "total war" or "absolute war". As it is understood, he defines a war that is waged against the enemy with all resources and momentum until the enemy is wiped out [2]. In today's complex and multi-dimensional security environment, commanders need to analyze the strategies and also take the new variables like cyberspace, which is emerging as a new domain after air, land, maritime and space [3], into account. The operational environment, comprising of friend, enemy and neutral systems, has been experiencing a new factor, cyberspace, that supports and interacts with operational variables like political, military, economic, social, information, infrastructure etc [4] [5]. The operational environment (OE) is not separate from information system infrastructure due to the large amount of information running on networks [3]. Evolving technology and the increasing use of social networks has necessitated the governments

and institutions to have at first the situational awareness and then more than that.

Particularly, increasing use of information communication technologies (ICT), smart devices (phones and tablets) and over three billion people having internet access have popularized the use of blogs and social networks[6][7]. And along with these facts, cyberspace has become a suitable area for criminals and terrorist organizations [8]. For example, ISIS has been using the social media to spread its ideology and message after it seized Mosul, Iraq's second-largest city, [9]. In particular, ISIS was able to succeed in creating an atmosphere of fear in Iraq by releasing the execution videos and photos on social networks like Twitter and YouTube [10]. The power of social networks, during elections, street incidents in repressive regimes or during natural disasters, has proved its ability to change traditional one-way media, from news agency to people. With this change in media, big news agencies also have taken advantages of user generated footage [11] As a consequence of those facts, some government actions are seen on interferences and restrictions on access to information sources especially from social networks that provide instant feeds.

In this new operational environment where it is easy to conceal itself for a long period of time, cyber wars have been waged similarly with physical ones [12]. Being as real as physical ones, cyber wars start in cyberspace and have effects and influences in real life [13]. Increasing number and diversities of cyber attacks require people, institutions and countries to take strong measures against them. These precautions range from personal actions like being aware of cyber risks, having situational awareness to strategic actions like having a national cybersecurity document, forming a computer incident response team (CIRT). More comprehensive approaches are also put into action by founding governmental and military cyber organizations to protect the assets, defense and cooperate. In these organizations, according to its level, vulnerability assessment, cyber incident handling, configuration management and cyber training activities are handled. As an institution, military organizations must ensure that its cyber assets are being protected and must be prepared by adapting its procedures, plans and doctrines to operate in this evolving and ambiguous area, cyberspace, where it is replete with criminal organizations and individuals [3]. The targets of cyber attacks can vary according to the causes and desired end states which the planners or perpetrators struggle to attain. Qiao and Wang, The Two Chinese Strategies, define the battlefield: "The battlefield is next to you and the enemy is on the network. Only there is no smell of gunpowder or the odor of blood" [14].

In this study, we tried to adapt cyber operations to fit in an operational design and named it cyber operational design in order to help cyber and operation planners to understand each other better and share this new OE in common. Operational design is generally done before planning to visualize the enemy and operation environment and deal with the ill structured problems in a more comprehensive way [15]. In section two we emphasized the need of cyber operational design with mentioning about the well known cyber attacks having strategic objectives. In this section we also defined our study that it is not based on a real cyberspace operation. We haven't discussed about the legality of cyberspace operations in this section. In section 3, we mentioned about operation planning, military decision making process (MDMP), operational art, operational design and its elements. We also prepared a sample cyber factor analysis that sheds light on cyber operational design explained in the following section. In section 4, we defined the relations between cyberspace operations and cyber operational design and the need of understanding of these two. In this section we prepared a cognitive map of cyber operational design by the help of factor analysis and cyber center of gravity. In conclusion, we have drawn attention to the need of cyber operational design and by this we have shown the importance of bringing cyber specialists and operation planners together for better planning of military operations.

2 METHODOLOGY

Understanding a complex operational environment such as cyber warfare requires a combination of art and science and ability to blend knowledge,

experience, intuition, and critical thinking that are essential to operational design with analytical methods and tools that support detailed planning. [15]. In this study we assume that cyber operations (defence, active defense or offense) have become an integral planning factor in operational and strategic operations of countries or a supplementary tool in reaching strategic objectives. We reach this data from some cyber and intelligence related incidents that quite many professionals call them "cyber warfare" One of the leading cyber incidents is Stuxnet that intended to disrupt a country's nuclear facilities and it is widely believed that it is driven by a nation or nations having a strategic objectives. Other cyber warfare and intelligence activities can be Flame, Duqu, Red October, Regin and so on. Some of these are believed to be initiated by intelligence organizations and some are also nation sponsored. Due to the complexity of cyberspace and lack of enough legal evidence on attribution to a specific source, they are not yet rightly ascribed to a source or structure.

In our study, we will not discuss the legality of waging cyber warfare to an organization, country or enemy and we will not probe the philosophy of just or unjust war. We are interested in the process of planning cyberspace operations (CO) alone or as a part of another operation. We also emphasize that a clear definition of jobs related to cyber operations in military organizations should be prepared in detail and legal issues both in government and institutional level must entitle the commanders and operation planners to act freely within the boundaries of a legal framework.

In this paper, we haven't planned a real cyber operation and analyzed a previously planned cyber operation either. We struggle to adapt cyber operations to take advantage of operational design, operational planning and military decision making process (MDMP) and used the elements of operational design to fit cyberspace operations (CO) like cyber line of operations (CLOO), cyber center of gravity (CCOG), cyber decisive points (CDC) and cyber desired end state. While there are also some other elements of operational design, we haven't analyzed all of them here. Our study can be better executed in operational and strategic level unaided or in tactical level as a part of a higher command. In our study, we have assumed that the complex security environment that we are currently living in, the interoperability, joint operations and cutting-edge technology are going to play a significant role. What we have deducted from our assumption are to understand operation planners and cyber professionals each other better in order to have a thorough, well prepared cyber operation planning and to draw also a cyber situational awareness to both technical and staff personnel.

3 OPERATION PLANNING, MILITARY DECISION-MAKING PROCESS (MDMP)

3.1 Operation Planning

Planning is an activity that helps bring the commander's visualization into practice and forms course of actions to reach a military target [16]. Due to the ambiguous nature of military operations, many variables of the operational environment and unforeseen events necessitate the planning to be a continuous activity. According to the Field Manual 5-0, The Operations Process, planning is associated with art and firstly comprehending then visualizing a fact and putting forward the ways to reach the target. [17]. Regardless of its level, planning is an indispensable part of an every organization. To manage the available time effectively and spare maximum time to subordinates [18], parallel planning is applied during a military decision making process which is an analytical process or a checklist to carry out every element in sequence to reach a detailed document without escaping even a small point one's notice.

Operational design and operational planning are two close, concurrent elements that can be prepared by a different or same team. It may not be easy to have two different (designers and planners) teams doing these two jobs. Besides, having two separate teams may result with lack of coordination, synchronization and may harm the nature of coupling of these two. Operation planning, is a set of procedures that are needed to be started after getting a higher command's order, commander's initial guidance or directly from the situation. Operational planning can be classified in

two sections, conceptual and detailed planning [19]. In this context; while the operational design forms the conceptual planning (with a cognitive map) the military decision-making process forms the detailed planning. [19]. And FM 5-0 also describes that a powerful and useful planning is composed these two (conceptual and detailed) kinds of planning [20].

3.2 Military Decision Making Process (MDMP)

The military decision-making process (MDMP) is a continuous and recurrent process helping commander and staff to comprehend the situation, to analyze the mission, to get the commander's initial guidance, to develop course of actions [22] [23]. With the inputs of each staff officers relating with their professions, functional areas (Command and control, engineering, air defense etc.), started mission and other iterative planning methodology that integrates the activities of the commander, subordinate headquarters, staff and other partners to understand the situation.

Table 1: A Sample of Cyber Factor Analysis (Three Column Format)

Mission / Critical Activity / Functional Area/ Critical Vulnerability	**Deduction**	**Output**
Lack of Talented Cyber Specialists in Military Organizations.	Being unable to envision the cyber risks.	To plan professional cyber security trainings on theory and hands on.
	Being exposed to cyber incidents and unaware of them for a long time.	To plan cybersecurity lessons in military high schools and academies.
		Station some personnel on job training to scientific organizations and institutes dealing with cybersecurity.
	Being unable to sustain situational awareness among commanders and staff.	To plan cyber threat situational awareness training for commanders and staff to remind that cybersecurity is the commander responsibility.
To Defend Army Critical Information Systems Against cyber Attacks.	Enough workforce assignment of cyber professional and a clear definition of "defense, active defense and offense" in procedures.	To defend information systems 24/7.
		To hire part time or full time civilian contractors, engineers, hackers and malware analysts.
	Building strong coordination with intelligence organizations.	To assign liaison personnel mutually between cyber command and intelligence units.
The Risks of Open Source Intelligence (OSINT) and Social Networks.	Being an easy target to fishing attacks.	To plan cyber exercises to draw attention of leading cyber attacks (fishing, waterhole attacks, etc.)
	Gathering OSINT via social networks with masked and fake social network accounts.	To limit the use of social networks in military organizations.
	Using metadata of uploaded contents and EXIF information of uploaded photos [21]	To assign a content operator to control, erase and change the metadata and other information of contents.

Besides, it develop and compare courses of action and select appropriate decision.

3.2.1 Factor Analysis

Factor analysis or the three-column format is sort of a checklist for staff officers to take all factors into account and deduct to do's from it. It is a frequently used methodology in MDMP and it can be used in all levels of operations. It functions as a checklist for staff officers offering planners to evaluate the operational environment, according to their functionality areas and also put forward the requirements to achieve the desired end state.
It offers a way of ordering the commander's and staffs' thought processes, and generates discipline in identifying the outputs of factor analysis. It is generally prepared in three column format (Critical Vulnerability, Deduction and Output) and named also the same. Factor analysis in table 1 is prepared in cyber means helping the CO planners to help put forward mission, critical activities about its functional area and critical vulnerabilities. The clear definition of these will also help CO and operation planners to analyze the center of gravity both of enemy and friend.

3.2.2 Center of Gravity (COG) Analysis

Among the elements of cyber operational design, CCOG is the key one to reach the desired end state. In center of gravity analysis, there are several questions to be answered: What's the end state that the enemy wants? What kind of activities can the enemy perform to reach the end state? Which requirements support enemy's such activity? And which activities prevent the friend to achieve its end state? In CCOG analysis we can get the advantage of cyber factor analysis that consists of critical friend and enemy capabilities, missions and vulnerabilities.

3.2 Operational Art and Operational Design

3.2.1 Operational Art

According to Joint Pub 1-02, operational art is defined as the use of military forces to reach military objectives (strategic and operational) with design, organization, integration, and use of strategies. [24] Operational art plays a key role in conveying the commander's intuition and strategy into operational design by accounting all related factors of war.

Table 2: A Sample of Cyber Center of Gravity (CCOG) Analysis.

Cyber Center of Gravity (CCOG)	**Critical Capabilities (CC)**
SCADA Systems and Military Information Systems Infrastructure.	To implement cyber attacks against SCADA Systems by manual means (Hiring a person/supporter to use a malware/worm infected hard drive on these systems).
	To infect enemy's military information systems with a computer virus, worm or malware to steal or gather information (Screen shots, key strokes and files) by infiltrating into the systems or spear fishing by using social networks, open source intelligence (OSINT) and social engineering.
	To implement a zero day exploit to database, email, file servers that are connected on internet.
	To implement DDOS attacks.
	To implement cyber-electronic warfare activities in order to get electronic intelligence from frequency logs of command and control systems by using airborne warning/intelligence systems or drones.
Critical Vulnerabilities (CV)	**Critical Requirements (CR)**
Limited use of cyber intelligence activities.	To gather OSINT about SCADA/Cyber Physical Systems and their system requirements by using TOR networks or spoofed IP addresses.
National and international legal challenges and NATO perspective on cyber issues (Accepting it as an act of war or not, ambiguity of cyber rules of engagements etc.)	Preparing a legal frame document that clearly defines the activities, tasks and duties about cyber.
Lack of talented cyber specialists and cyber manpower planning in military organizations.	Reverse engineering and multi criteria analysis of some well known malwares directed to gather information from the systems they infected.
Lack of a roadmap and strategy designed to reach the national cyber security policy, lack of information sharing with institutions, universities and defense firms.	To initiate a collaboration and among technical universities, civil institutions and defense firms about research and development (R&D) in cyber
Lack of a clear task definition of cyber activities among institutions.	Forming a social network team, working 24/7 and solely focusing on Facebook, Twitter, LinkedIn, Vine, Instagram and the others also.
The lack of integration of cyber and intelligence units and the dilemma of whose job that is, limited cooperation between these two functional areas.	To have a national vulnerability database and enough cyber experts and contractors.
The legal challenges.	A great number of zombie computers, botnes.
The difficulty in integrating and implementing cyber and electromagnetic activities in tactical level under a command.	Strong cooperation between intelligence cyber units.

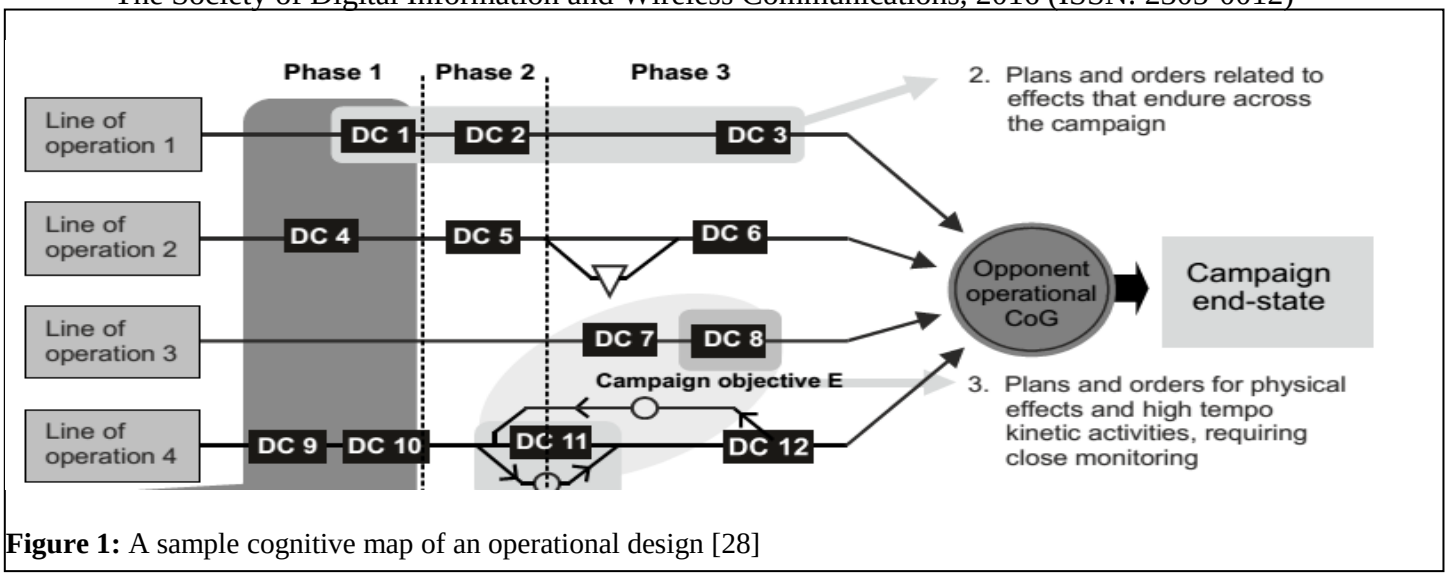

Figure 1: A sample cognitive map of an operational design [28]

3.2.2 Operational Design

Operational design is a methodology having the structure of concepts, a visual and comprehensive map of a campaign or operation in order to attain the desired end state. [25]. The main elements of operational design showed in figure 1are; line of operations (LOO), decisive points (DC), center of gravity (COG), end state are shown in a sample cognitive map of an operational design.

3.2.3 Critical and Creative Thinking

To deal with complex and multidimensional problems and develop solutions, operational designers should apply critical and creative thinking [15]. Critical thinking is a process comprising of conceptualizing, applying, analyzing, synthesizing, and/or evaluating information regardless of how it is gathered, produced, experienced or observed. [26]. While emphasizing on critical and creative thinking in operational design Bloom's Taxonomy of Learning can shed a light on this issue. As shown in figure 2, 1956 old model, developed for educational purposes, is a model that can help us relate critical thinking and creative thinking by associating them with the model's components [27] [15]. It is supposed that the commanders should be in a better level of their subordinates in creative thinking due to their experience, training and knowledge and judgement.

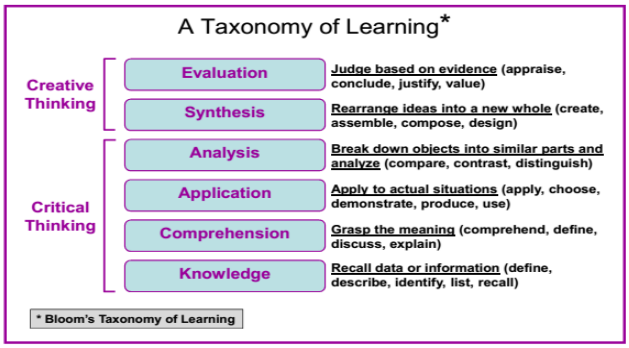

Figure 2: A taxonomy of learning [15].

4 CYBERSPACE OPERATIONS AND CYBER OPERATIONAL DESIGN

4.1 Cyberspace Operations (CO)

Cyberspace operations (CO) are the use of cyberspace capabilities where the main purpose is to attain the objectives in or through cyberspace [29]. With the advent of cyber in the globe theatre, it has become a must for commanders and operation planners to take necessary measures to protect their ICT and critical assets. In military operations, similar to electronic warfare planning and support of operations, CO should also be integrated into these operations according to its level. CO integration into military operations should be planned in detail by following the MDMP. The considerations of CO planners in MDMP are similar to other functional area considerations. With the start of MDMP, CO planners are going to need intelligence requirements about the enemy and environment.

Depending on the commander's intent or CO planners, cyber operational design should be prepared by CO planners before or with the first step of MDMP, receipt of mission. Having a cyber operational design will help CO planners to better integrate their objectives with major military operations.

4.2 Cyber Operational Design (COD)

The designing of cyber operations regardless of the common operation picture (COP) or not within an MDMP, may cause the expected impact become weak and ineffective. Eliciting the art of war and stimulating the critical and creative thinking, operational design put forward the general picture of operation, which is called the cognitive map.

In a cyber cognitive map, cyber operational design, the same elements of operational design are applied. Cyber operational design (COD) consists of cyber line of operations (Government, people and military), Decisive Points (DC), center of gravity (COG) and the end state (Desired End State). All elements of cyber operational design in figure 3 should serve to reach the end state in four phases of which starts with "Confusion Initiation" and ends with "Dominate" phase. The cyber operational design in figure 4 can also be adjusted to all levels of military or governmental organizations by elaborating more than one COG (Operational and Strategic COG) or End State (Military and Governmental End State).

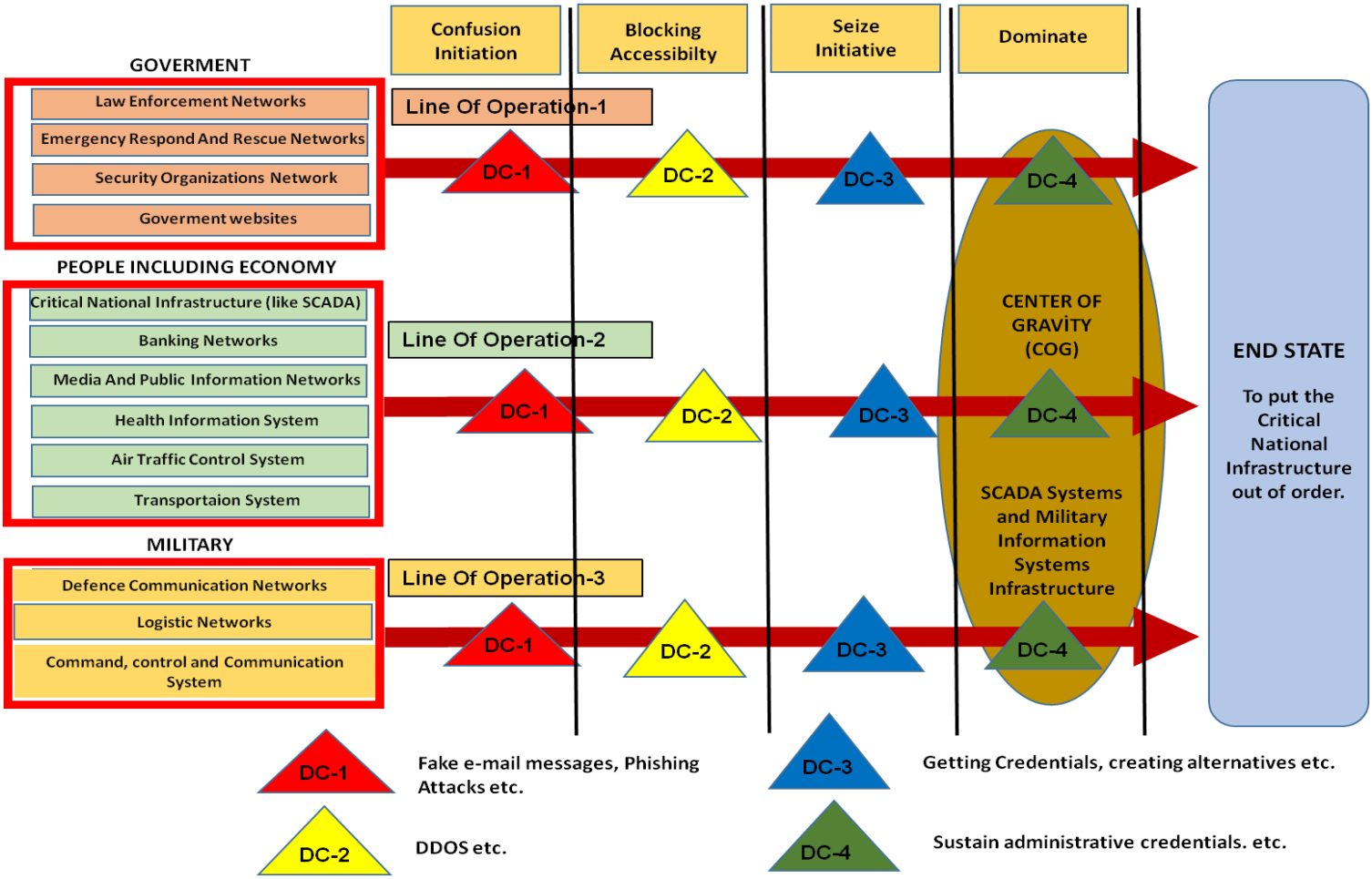

Figure 3: A Sample Cognitive Map of Cyber Operational Design.

5 CONCLUSION

In complex, multidimensional and multivariable security environment, it has become a must to get prepared all kinds of threats. What is becoming obvious that, with the evolving and cutting edge technology most of the threats are somehow emerging or being transferred with information systems. National Critical Infrastructures of countries are operating in networks, government and military organizations' data centers are working with software and hardware that even the system administrators can't control over them thoroughly. With the increasing use of smart devices, phones, appliances and even cars people become more and more interconnected with technology every day. Increasing use of social networks and all other improvements as a natural consequence of technological evolutions have facilitated the work of intelligence agents and cyber criminals. To gather information via open source and social networks like Facebook, twitter, LinkedIn, Instagram and the others have become an easy job even for a standard internet user. What the government and military organizations should do in this changing security environment is to scrutinize the current plans and procedures to support the flexibility of operations to adapt to new, unforeseen threats and risks that we sooner or later may be exposed to.

We assume that cyber incidents will continue to play a significant role in global theatre and institutions should be well prepared to withstand and defend their critical assets which are mostly on our networks, databases and command control systems. In this context, we make an analogy of ill-structured problems with cyber threats/attacks that are complicated, hard to detect and targeted. Therefore by emphasizing the importance of design and its elements, we propose a cyber operational design to be used in cyberspace operations to envision the cyber threats, cyber attacks, cyber intelligence and espionage activities both conceptually and comprehensively. We believe that by having a cyber operational design, the operation planners and cyber professionals will come to a common point where they can understand and contribute each other well and this cooperation will then provide a stronger, foreseeable institutional and national cybersecurity.

6 REFERENCES

[1]. Handel, M. I. (2005). *Masters of war: classical strategic thought*. Routledge.

[2]. Handel, M. I., (1991) Sun Tzu and Clausewitz: The Art of War and On War Compared, Strategic Studies Institute U.S. Army War College Carlisle Barracks, Pennsylvania.

[3]. Pamphlet, T. R. A. D. O. C. (2010). TRADOC Pamphlet Cyberspace Operations Concept Capability Plan2016-2028. Washington, DC: DoD.

[4]. Goztepe, K., Kilic, R., & Kayaalp, A. (2014). Cyber Defense In Depth: Designing Cyber Security Agency Organization For Turkey. Journal of Naval Science and Engineering, 10(1), 1-24.

[5]. Goztepe, K. (2012). Designing Fuzzy Rule Based Expert System for Cyber Security. International Journal of Information Security Science, 1(1), 13-19.

[6]. Singh, A. K., & Sahu, R. (2008). Integrating Internet, telephones, and call centers for delivering better quality e-governance to all citizens. Government Information Quarterly, 25(3), 477-490.

[7]. Güngör, V. C., Sahin, D., Kocak, T., Ergüt, S., Buccella, C., Cecati, C., & Hancke, G. P. (2011). Smart grid technologies: communication technologies and standards. Industrial informatics, IEEE transactions on, 7(4), 529-539.

[8]. Choo, K. K. R. (2008). Organised crime groups in cyberspace: a typology. Trends in organized crime, 11(3), 270-295

[9]. Kay M., J. (2014) "ISIS Tactics Illustrate Social Media's New Place In Modern War", [online], http://techcrunch.com/2014/10/15/isis-tactics-illustrate-social-medias-new-place-in-modern-war/

[10]. Boz, G. (2014) "ISIS and Social Media", [online], Ankara Strategy Institute, http://www.ankarastrateji.org/haber/isis-and-social-media-1399/

[11]. Newman, N., Dutton, W. H., & Blank, G. (2012). Social media in the changing ecology of news: The fourth and fifth estates in Britain. International Journal of Internet Science, 7(1), 6-22.

[12]. Hejase, A. J., Hejase, H. J., & Hejase, J. A. (2015) Cyber Warfare Awareness in Lebanon: Exploratory Research. International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 482-497

[13]. Al-Ahmad, W. (2013). A Detailed Strategy for Managing Corporation Cyber War Security. International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2(4), 1-9.

[14]. Liang, Q., & Xiangsui, W. (1999). Unrestricted warfare (pp. 551-563). Beijing: PLA Literature and Arts Publishing House.

[15]. Joint Staff, J-7 (2011) Planner's Handbook for Operational Design, Joint and Coalition Warfighting Suffolk, Virginia.

[16]. Lussier, J. W., Shadrick, S. B., & Prevou, M. I. (2003). Think Like a Commander prototype: Instructor's guide to adaptive thinking (No. ARI-RP-2003-02). Army Research Inst. for the Behavioral and Social Sciences Alexandria VA.

[17]. FM 5-0. (2010) The Operations Process, Headquarters Department of The Army.

[18]. FM 101-5. (1997) Staff Organization and Operations, Headquarters Department of the Army Washington, DC.

[19]. Kober, A.E. (2010) Bridging the Planning Gap: Linking Conceptual Army Design to Military Decision-Making, School of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth, Kansas.

[20]. Grigsby Jr, W. W., Gorman, S., Marr, J., McLamb, J., Stewart, M., & Schifferle, P. (2012). Integrated Planning the Operations Process, Design, and the Military Decision Making Process. Military Review, 92(4), 15.

[21]. Catalkaya H., Karaman M. (2015). Institutional Cybersecurity: The Risk of Open Source Intelligence (OSINT) and Social Networks, International Conference on Military Security Studies (ICMSS-2015), Istanbul.

[22]. Kem J.D. (2012) Planning for Action: Campaign Concepts and Tools, U.S. Army Command and General Staff College U.S. Army Combined Arms Center Fort Leavenworth, Kansas.

[23]. Goztepe, K., Kahraman, C. (2015) A New Approach to Military Decision Making Process: Suggestions from MCDM Point of View, International Conference on Military and Security Studies-2015, Istanbul, 118-122.

[24]. Joint Publication 1-02 (1994) Department of Defense Dictionary of Military and Associated Terms, Headquarters Department of Defense.

[25]. McCauley, D. (2011). Design and Joint Operation Planning. Canadian Military Journal, 12(1), 30-40.

[26]. Scriven M., Paul R. (1987) "National Council for Excellence in Critical Thinking", 8th Annual International Conference on Critical Thinking and Education Reform, Summer 1987.

[27]. Bloom, B., & Englehart, M. F. E., Hill, W., & Krathwohl, D.(1956). Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain.

[28]. Joint Publication 5-0 (2011) Joint Operation Planning, Headquarters Department of Defense.