International Journal of Cyber-Security and Digital Forensics (IJCSDF) 2(4): 1-9
The Society of Digital Information and Wireless Communications, 2013 (ISSN: 2305-0012)

A Detailed Strategy for Managing Corporation Cyber War Security

Walid Al-Ahmad
Department of Computer Science, Gulf University for Science & Technology
Kuwait
alahmed.w@gust.edu.kw

ABSTRACT

Modern corporations depend heavily on information and communication technologies and are becoming increasingly interconnected locally and internationally. This interconnectedness and dependency on information technology make corporations vulnerable to cyber attacks. Corporate managers therefore need to understand the growing cyber war threats and implement appropriate strategies to mitigate the risks. This research work is an attempt to develop a generic and detailed strategy to assist corporations in managing the cyber war security. The implementation of such a strategy will definitely lead to a more secure business environment and as a result will attract foreign investments to the Arab countries in the Middle East. Such a strategy can be considered as a first step toward protecting corporations from cyber war threats in an effective manner.

KEYWORDS

Information warfare, security strategy, security management, cyber war, cyber security, corporation espionage

1 INTRODUCTION

Until recently information cyber war has been commonly regarded as a military concern. Nowadays, it is not only a military and national concern but also a societal issue. In fact, there is a paradigm shift from national cyber war to corporation cyber war. Thus, although the bulk of the cyber war literature addresses the military dimension, information warfare has expanded into non-military areas [1]. Corporation cyber war attacks are expected to increase rapidly and until now there isn't any optimal and satisfactory solution to address this problem. Therefore, the issue of cyber war in the context of corporations warrants further study and investigation. This paper tries to shed light on this topic in an attempt to understand this phenomenon and its impact on corporations in particular and on nations in general. The main objective of this paper is to construct a cyber security strategy for corporations in the Middle Eastern Arab countries to address the cyber war risks. The reason why this strategy is designed for the Arab countries is that they all have many things in common; many of the challenges and hurdles apply to all of them. The author has worked in several countries in the region and is familiar with the security environments, regulations, academic and industrial sectors in these countries.

Many information warfare definitions exist that emphasize the military dimension. A definition of information warfare that applies in both the military as well as the civilian contexts is this one: Information Warfare is defined as "actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks" [2]. Information warfare is can also be classified into three categories: Personal Information Warfare, where it describes attacks against an individual's electronic privacy; Corporate Information Warfare, where it describes competition, or better said today's war between corporations around the world; Global Information Warfare, where it describes the war against industries, global economic forces or against entire countries or states.

In [3], the complex cyber challenge is divided into five levels of security problems: home users and small businesses, large enterprises, critical

infrastructure sectors, national vulnerabilities, and the global information grid of networked systems.

Cyber espionage is to collect information on an opponent's secrets, intentions, and capabilities. It consists of the search for access to classified, personal or corporate data, intellectual property, proprietary information and patents, or results from research and development projects, for reconnaissance, probing, and testing of information and communications technology defenses, and clandestine manipulation of data, information and critical infrastructure for war preparation. Cyber espionage is a real threat to corporations due to the increasing dependency on the cyber space to carry out business.

There is no universally accepted definition of cyber war. One general definition is "cyber war refers to a massively coordinated digital assault on a government by another, or by large groups of citizens. It is the action by a nation-state to penetrate another nation's computers and networks for the purposes of causing damage or disruption." But it adds that "the term cyber ware may also be used to describe attacks between corporations, from terrorist organizations, or simply attacks by individuals called hackers, who are perceived as being warlike in their intent [4]. Another definition is: "Cyber war is symmetric or asymmetric offensive and defensive digital network activity by states or state-like actors, encompassing danger to critical national infrastructure and military systems [4].

Whereas most researches and books focus on military information warfare and ignore corporation information warfare, the focus in this paper is on Corporate Cyber Warfare as an ever growing problem. With the growing corporation dependency on information technology, corporate infrastructures are increasingly the primary targets of cyber attacks. In fact, the corporate information warfare is not new, but the new dimension of this type of attack is changing the methods and tools used in corporation's cyber war, because most of corporations today depend heavily on computers and networks to run their businesses. The computers, networks and information systems used by corporations are usually vulnerable to many security attacks, which in turn allow corporations to spy on each other by exploiting these vulnerabilities.

The MacAfee report states that many corporations nowadays face new types of attacks that are related to corporations' cyber war [5]. One key reason for corporations to use cyber warfare is to carry out industrial espionage to gain competitive advantage. As an example, if one corporation participated in specific tenders and launched a corporation cyber war against other competitors who participated in the same tender, this corporation can gain superiority and may win the tender. The impact of corporation cyber war ranges from financial losses to reputation losses which may lead to a global crisis or a war between countries in the worst case.

Therefore, corporations should start to look beyond reactive, tactical cyber defense to proactive, strategic cyber defense. As a first step towards this goal, a cyber war strategy must be in place.

There have been several efforts to develop cyber war strategies in the context of military, but little or no such efforts have been done in the context of corporations [6 - 9]. Some countries in the region, such as Jordan for example [10], have developed Information and Communication Technology strategies; information security is usually a part of such strategies. This paper also focuses on corporation cyber war strategies in the Arab countries. This paper presents a cyber war strategy that can be implemented by corporations in collaboration with governments to protect the information and IT infrastructure from cyber war attacks. The strategy shows the required steps and activities corporations should implement to defend against cyber attacks.

The rest of the paper is structured as follows: section 2 outlines the general drivers of the strategy proposed by this paper. Section 3 then explains the elements of a strategic solution that can be achieved by the strategy. Section 4 highlights the necessary requirements for implementing the proposed strategy. Finally, section 5 concludes this paper.

2 STRATEGY DRIVERS

A corporation cyber war strategy is a typical strategic plan and as such should clearly specify the strategic goals and identify the obstacles and challenges facing these goals. Thus, this strategy begins with identifying the high level strategic drivers in terms of desired future situation (goals) and challenges and obstacles to overcome. The strategy is developed for the private sector in the Middle East Arab countries - the different business sectors. The strategy can be designed for a period of say five years depending on the available resources and commitment from all stakeholders. Figure 1 represents an overview of the strategy drivers.

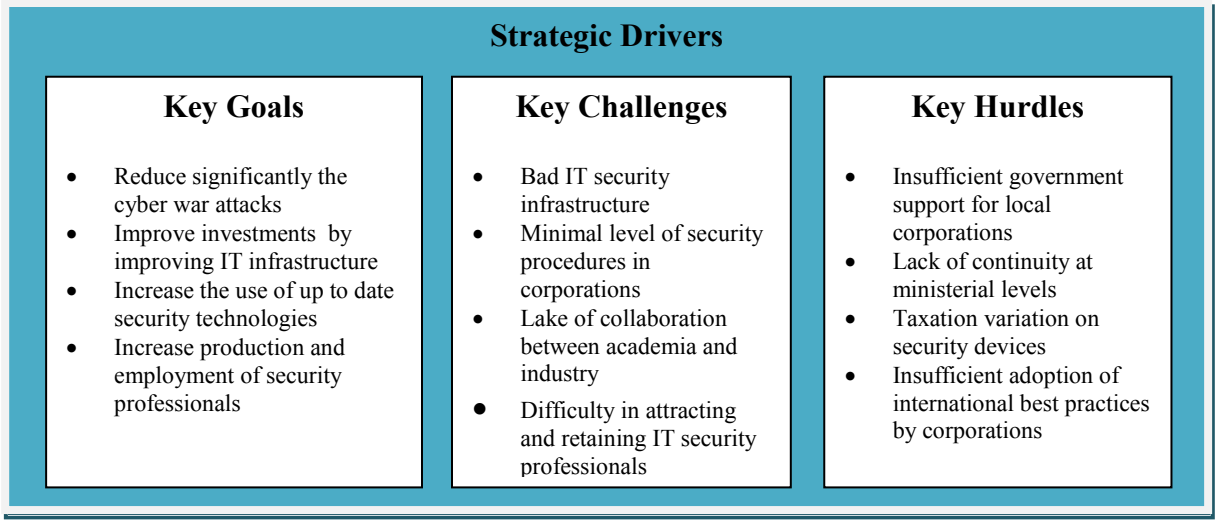

Figure 1. Cyber War Strategy Drivers.

The remainder of this section provides a brief overview of and explains the elements of the strategy drivers.

2.1 Strategic Goals

This strategy will develop four primary strategic goals to be achieved over a period of say five years that will help the Middle East countries to move forward in their efforts to use IT, thereby improving the standard of life of their citizens and creating an attractive environment for investments. These goals are:

- *Reduce significantly the cyber war attacks*. Unfortunately, there is little information and statistics about the security situation in the Arab countries. However, it is for sure not a good one. Each country is required to determine the percentage of reduction to cyber war attacks based on the current situation and the desired one.
- *Improve investments by improving IT security infrastructure.* As a return on investment of reducing cyber war attacks, the business environment will hopefully attract foreign investments and thereby creating new jobs and improving the economy.
- *Increase the use of up to date security technologies.* Corporations are required to increase the utilization of recent advancements in the cyber security technologies and counter measures.
- *Increase production and employment of security professionals.* Corporations should raise awareness about the impact of corporation cyber war on corporations. They should increase the employment of highly skilled security professionals.

2.2 Strategy Key Challenges

This paper identifies four key challenges faced by corporations in the Arab world that must be addressed in a proper way in order to accomplish the strategy goals:

- *Bad IT security infrastructure*. Many small, middle and large corporations don't have good IT security infrastructure; most of them think

that if they have only antivirus and firewall they will be protected. Also, many of them don't upgrade their existing security infrastructure periodically.

- *Minimal level of security procedures in corporations*. Most of companies in the Arab world, in the different sectors, don't implement minimum level of security procedures to protect their works. There are several reasons for that: most companies don't know the real size of threat that can have an impact on their business; also the majority don't follow security standards or have clear best practices to implement security; most corporations don't provide their employees, especially in IT departments, with latest information, network and computer security awareness and training programs.
- *Lack of collaboration between academia and industry*. Universities in the Arab countries do not produce the required skilled IT graduates with the competencies to meet the needs of corporations, especially in the area of information security. In addition to that, industry needs to communicate its skill needs to academic institutions and facilitate a smooth labor market for IT security professionals. More importantly, most universities focus on the theory and neglect the practical aspects of information security and this should absolutely change.
- Difficulty attracting and retaining IT experts in some of the Arab countries. In fact, countries in the Arab world are at a competitive disadvantage in the regional and international labor market in terms of the quality of education and technology expertise.

2.3 Strategy Key Hurdles

The strategy also identifies a number of systemic hurdles that may obstruct the growth of corporations:

- *Insufficient government support for local corporations*. Governments are required to do more, in terms of policymaking, regulation, and executive roles, to support local corporations – at the same time serving the best interests of taxpayers and the community as a whole in these roles.
- *Lack of continuity at ministerial levels.* Frequent changes in government leadership make it difficult to institutionalize any long-term strategy. Also there isn't clear coordination between different ministries like ministry of planning, ministry of justice, ministry of trade and ministry of information and communication, etc.
- *Taxation variations on security devices*. Some Arab countries in the Middle East are at a competitive disadvantage in the regional and international labor market due to high and many taxation variations on IT security devices and on the Internet; this is a weakness that will prevent corporation from improving and upgrading their existing IT infrastructure.
- *Insufficient adoption of international best practices by companies.* Most corporations don't follow or implement specific security standards, and don't follow best security practices to protect its work in an efficient way.

The strategic objectives and outcomes identified in the proposed cyber war strategy will help governments and corporations to overcome these hurdles and challenges and achieve the high-level strategic objectives. In the end, both challenges and hurdles should be eliminated or reduced to an acceptable level.

3 A STRATEGIC SOLUTION

A corporation cyber war strategy defines the specific solution required - in terms of objectives, outcomes, and actions needed to achieve them - to address the strategic drivers. The different components that make up the strategy solution are shown in figure 2.

3.1 Strategic Objectives and Outcomes

A corporation cyber war strategy decomposes the four high level strategic objectives into many objectives that must be achieved in order to fulfill these objectives. These strategic objectives require outcomes from multiple pillars and by multiple actors.

A corporation cyber war further decomposes these objectives into many strategic outcomes that represent fulfillment of the objectives. Each outcome is associated with a pillar based on the nature of activity measured and be fulfilled by one or more actions, or projects, to be conducted by various stakeholders. The strategy also designates the sector that would ultimately be responsible for achieving the outcome. Although most of the outcomes require multiple sectors, in each case one sector must be ultimately accountable for each outcome.

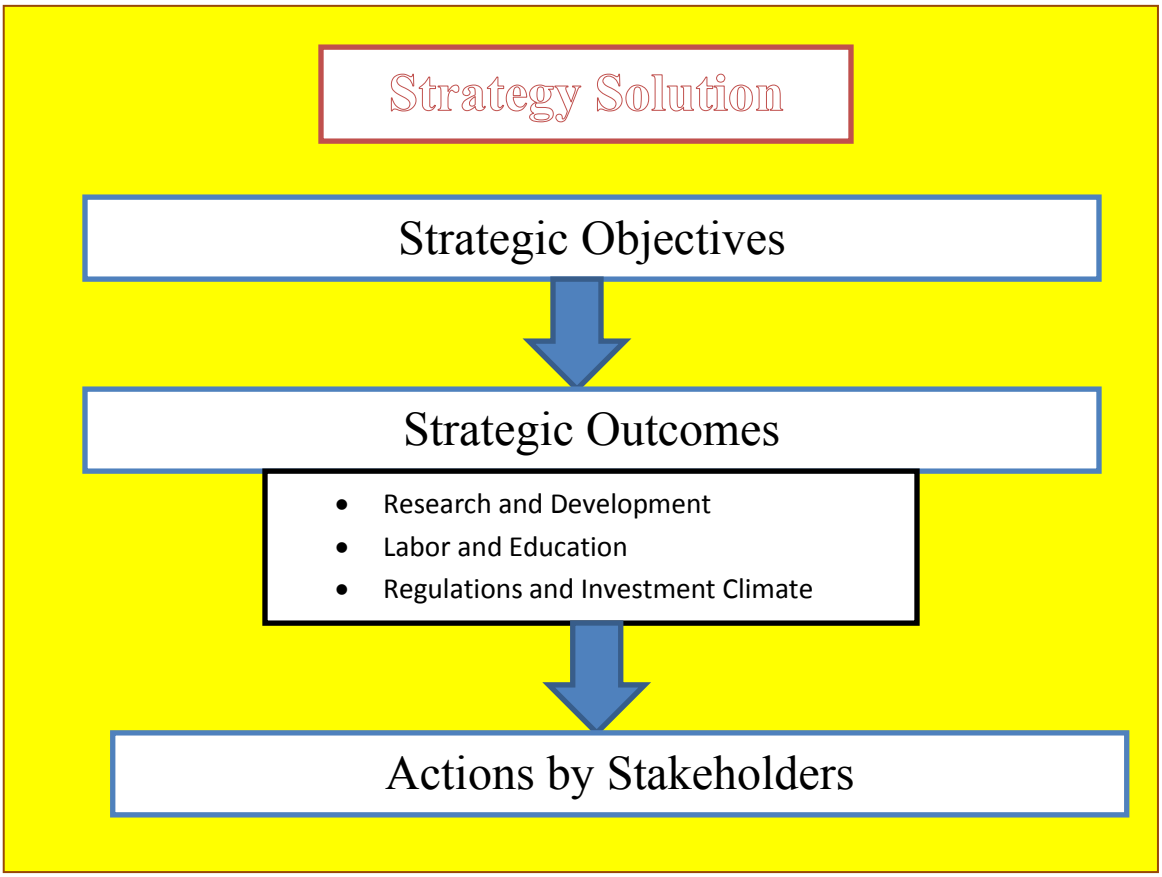

Figure 2. A Cyber War Strategy Solution.

3.2 Strategy Pillars

The corporation cyber war strategy identifies three pillars of strategic activity necessary to fulfill the strategic goals, namely:

- Research and development
- Labor and education
- Regulation and investment climate

Each of the challenges and hurdles requires actions to be carried out in one or more of the pillars. The pillars organize the individual expertise identified by the strategy and categorize the strategic activities recommended by the corporation cyber war strategy. Next follows a brief discussion of these three pillars.

A) RESEARCH AND DEVELOPMENT

Most of the Arab countries in the Middle East face lack of scientific research funding percentage in general and in corporation cyber war scientific research and development topics, in particular. Most people don't take corporation cyber war as a real threat that may affect the businesses environment. They underestimate the impacts of cyber war on investment infrastructures. The main

problem that faces information security scientific research is limited funds assigned for research and development due to the following reasons:

- The private sector does not appreciate the importance of scientific research on their work; most of corporations don't have a specific department or section for research and development, especially in the IT security field. Some of the countries in the region increased the overall research and development spending as a percentage of the GDP, but this remains far below in comparison with many other countries.
- The corporation cyber war is considered as a new topic. Because there are no tangible effects on businesses in terms of return on investment, many corporations are reluctant to invest in cyber war research and development.
- IT security changing rapidly. It is difficult to track all new security topics and most corporations don't know what the output of those researches is and how the outcomes and recommendations can be implemented.

In order for governments to successfully develop and implement cyber security technology-related research and development activities, they have to provide funding to strengthen the links between industry and academia. They also can provide incentives for private companies to participate in research and development as well as support research and development by funding research projects.

In order to achieve these objectives, the barriers between corporations and universities must be removed. There are needs to establish partnership between public and private sectors and increase awareness of cyber war threat and its impacts on public and private sector.

B) LABOR AND EDUCATION

The second pillar of the strategy is labor issues and education. To address this pillar, it is imperative to understand the challenges that face Arab governments in this field:

- Increasing number of IT graduates who have strong theoretical background but don't have appropriate skills especially in information, network and computer security fields because of, mainly, lack of cooperation between universities and industry.
- Some countries suffer from an emigration of its highly qualified workforce to other countries due to low salaries in private and public sectors.
- Public and private sectors don't provide scholarship for IT employee to obtain higher degree in IT security fields.
- Absence of monitoring university programs especially in information, network and computer security programs to meet its objectives.

To overcome these challenges the following steps must be taken:

- Improving quality of higher education rather than quantity, especially in information, network and computer security.
- Increasing salaries of qualified IT graduates.
- Encourage IT employees to complete higher degree in information, network and computer security field.
- Monitor quality of information, network and computer security education in universities.

C) REGULATION AND INVESTMENT CLIMATE

The regulation and investment climate is a more important pillar that must be taken into account when designing a strategy for corporation cyber war; most current laws are not designed to handle current cyber war threats and breaches. Also, the existing regulations don't facilitate improvement of security in corporation because it puts barriers instead of facilitating corporations work. So to improve the regulation and investment climate, the following steps must be taken:

- Establish new legislations and enhance existing laws that handle corporation cyber war risks, and put appropriate penalties on any person or corporation that in involved in cyber war breaches.
- Improve regulations to facilitate improving information, network and computer security by enforcing security standards like ISO or local

standards and encourage corporations to implement latest security technology without or with minimal taxes.

3.3 Actions and Actors

The strategy decomposes all outcomes into actions or specific projects to be conducted by one or more stakeholders to achieve the outcomes. For each project, the strategy identifies one lead stakeholder, e.g., private companies, a ministry, and any other stakeholders who should have a role.
Some of the projects are very broad, and others are very narrow, but all must be specific enough to be executed. The strategy lists the actions in the form of a project plan and adds successive levels of detail to each project as appropriate.

4 STRATEGY IMPLEMENTATION

Tables 1 – 4 summarize the strategic objectives, strategic outcomes, pillars, and actors, as defined by the strategy.
In fact, the high-level strategic objectives, outcomes, and actions constitute a project plan to achieve the strategic objectives and outcomes. Activation of the strategy will entail directing a corporation cyber war sponsors and governments to lead the execution and monitoring of the projects assigned to them. For those projects assigned to a stakeholder other than a corporation cyber war sponsors —and hence for which a corporation cyber war sponsors cannot direct the stakeholder to execute the project— a corporation cyber war sponsor will work with the government to enforce cooperation of these stakeholders.

Table 1. Strategic Goal 1- Plan

Goal 1: Reduce significantly the cyber war attacks			
Strategic Objectives	**Outcomes**	**Pillars**	**Actors**
Increase awareness of corporation cyber war security	Conduct cyber war awareness sessions for public and private sectors	Labor and education	Academia and Corporations
	Conduct corporation cyber war threat sessions and courses for corporations' employees	Labor and education	Academia and Corporations
Enhance corporations' security practices	Enforce implementing security certification according to nature of business for each corporation	Regulation and investment climate	Government and Corporations
	Establish and enable secure infrastructure for both public and private sectors	Regulation and investment climate	Government and Corporations
Improve response to cyber war attacks	Enforce corporations facing cyber war threats to report cyber war attacks to a centralized center such as a national CERT	Regulation and investment climate	Government and Corporations
	Establish a scientific research center for corporation cyber war that focuses on impacts and how to efficiently respond to cyber war threats and methods used to launch these attacks	Research and development	Academia and Corporations
Increase budget for security research	Establish collaborations between universities, public and private sectors to fund security research	Research and development	Government and Corporations

Table 2. Strategic Goal 2- Plan

Goal 2: Improve investment by improving IT infrastructure			
Strategic Objectives	**Outcomes**	**Pillars**	**Actors**
Improve current information and communication technology infrastructure	Improve information technology infrastructure for public sector	Research and development	Government
	Improve information technology infrastructure for private sector	Research and development	Corporations

	Review current technology and compare them with current technology using cost benefit analysis	Research and development	Academia and Corporations
Prevent anti-competitive behavior in the broadband market	Create a competition board with Competition Directorate	Regulation and investment climate	Government
Gradually reduce sales taxes on Internet access and related technologies	Lower tax rate	Regulation and investment climate	Government
Eliminate sales tax to lower cost of computer security devices	Conduct a study to recommend adjusting taxation of computer security technologies	Regulation and investment climate & Research and development	Government and Academia
Reduce barriers to the use of e-Commerce locally and internationally	Formulate and present to Parliament e-security laws, regulations, and processes	Regulation & investment climate	Government
	Implement digital signature laws and regulations	Regulation and investment climate	Corporations
	Implement PKI processes and technologies	Regulation and investment climate	Corporations
Improve the contributions of academia to industry research and development	Increase academic research relevant to information technology industry needs	Research and Development	Academia, Corporations, and Government

Table 3. Strategic Goal 3- Plan

Goal 3: Increase the use of up to date security technologies			
Strategic Objectives	**Outcomes**	**Pillars**	**Actors**
Improve current information technology security infrastructure	Improve information technology security infrastructure for public sector.	Research and development	Government and academia
	Improve information technology security infrastructure for private sector	Research and development	Corporations and academia
	Review current security technology and compare with existing security technologies using cost benefit analysis	Research and development	Academia and Corporations
Prepare for good alternative solutions	Prepare alternatives for each type of security threats	Research and development	Academia and Corporations
	Improve disaster recovery locations for both private and public sectors	Research and development	Academia and Corporations
Evaluate efficiency of security countermeasures	Improve assessment and evaluation procedures for new and existing security products	Research and development	Corporations and Academia
	Establish security labs to test all security products before launching it to local market	Research and development	Corporations and Academia
Improve security procedures	Enforce appointment of information technology security specialists in private and public sectors	Regulation and investment climate	Government and Corporations

Table 4. Strategic Goal 4- Plan

Goal 4: Increase production and employment of security professionals			
Strategic Objectives	**Outcomes**	**Pillars**	**Actors**
Improve skills of security employees	Encourage and offer courses for IT security employees to develop their skills, and enhance their capability to cope with new security challenges	Labor and education	Corporations
Ensure that university students have good computer security knowledge and skills	Ensure that the level of academic programs of security in universities is acceptable, and that each university offering courses in security must have security labs and appropriate infrastructure	Labor and education	Government and Academia
	Private sector must coordinate with academia to allow security students to practice security skills by implementing internship programs	Labor and education	Corporations and Academia

In order for an Arab country in the Middle East region to address the current challenges, the government and corporations should maintain an active partnership by taking ownership of its role in addressing the issues facing the government and corporations. Thus, this strategy is intended to mark the first step toward such a partnership and through collaboration between corporations and governments. By seeking out proactive and creative approaches to the problems facing a country, corporations can contribute to the growth in the economy, social development, and improvement in government.

As dependence on IT and the Internet grow, governments and corporations should make proportional investments in network security, incident response, security awareness and technical training, and collaboration.

5 CONCLUSIONS

This paper has outlined a strategy for corporations to protect their IT infrastructure (information and information systems, networks, etc.) from cyber war attacks. As a result, the Arab countries in the Middle East can improve local and foreign investments by offering secure environments. In order to realize the strategy and fully benefit from it, both the public and private sectors must work closely.

This strategy can be considered as a first step toward an effective and adequate approach to cyber security management. In terms of comprehensiveness, the strategy might require revision by experts in the field to determine whether or not it includes all relevant elements. Even after adoption by a country, the strategy should be reviewed periodically to cope with new changes in the threat environment as well as other factors that influence corporation cyber war. Finally, the strategy is to be adopted and implemented in one of the Arab countries to prove its usefulness and effectiveness.

6 REFERENCES

[1] K. Knapp and W. Boulton, "Cyber-warfare threatens corporations: expansion into commercial environments," Information Systems Management, vol. 23 Issue: 2, pp.76-87, 2006.

[2] R. Haeni, Information Warfare an introduction, 1997, retrieved from http://www.trinity.edu/rjensen/infowar.pdf.

[3] G. Bush,. "National Strategy to Secure Cyberspace," 2003, retrieved from http://www.whitehouse.gov/pcipb

[4] F. Schreier, "On Cyberwarfare,", 2012, retrieved from http://www.dcaf.ch/Publications/On-Cyberwarfare

[5] MacAfee Report, retrieved from http://sanjose.bizjournals.com

[6] L.Tinnel, S. Saydjari, and D. Farrell, "Cyberwar Strategy and Tactics: An Analysis of Cyber Goals, Strategies, Tactics, and Techniques," Proceedings of the 2002 IEEE Workshop on Information Assurance, 2002."

[7] R. Parks and D. Duggan, "Principles of Cyber-warfare," Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, 2001.

[8] A. Colarik and L. Janczewski, "Developing a Grand Strategy for Cyber War," Proceedings of the 17th International Conference on Information Assurance and Security, 2011.

[9] A. Sharma, "Cyber Wars: Paradigm Shift from Means to Ends," Strategic Analysis, vol. 34 Issue 1, pp. 62-73, 2010.

[10] Jordan ICT Strategy, retrieved from www.moict.gov.jo, 2013.