A Corporation Cyber War Strategy

Dr Amer Nizar AbuAli
Philadelphia University, Jordan, Faculty of Information Technology,
drabuali@yahoo.com

Saeb Sisan
Philadelphia University, Jordan, Faculty of Information Technology,
saebxt@gmail.com

***Abstract-* A corporation cyber war is a new type of attack that will be considered as a more dangerous attack faces the different corporations in each country in the world. The importance of a corporation cyber war now increases more and more, because of its large passive impact on a corporations work. So each country must start to defend against this type of this attack by preparing efficient strategies to reduce impacts of corporation cyber war attack to acceptable level. This paper will mention strategy to defend against corporation cyber war, which can be considered as a first step toward protecting corporations from corporation cyber war threat in efficient way and using understandable approach. Most research papers focus on cyber war between countries while our research contribution focuses on new side by focus on using of cyber war as a tool that can be used by one company against other companies by show how to prevent information warfare between companies from strategically view to help countries to address this issue and we take Jordan as a case study, so this research results can be increased trust on computing for society by increasing security and encourage more investment in information technology through prevent abusing of computers.**

Keywords: Information warfare, Corporation warfare, Cyber

Introduction

Because modern, post-industrial societies have become critically dependent on computer networks to function on a day-to-day basis,

Disruption of those networks could have serious social and economic consequences. In order to better protect society, policymakers will have to re-orient their approach toward cyber security so as to emphasize the genuine cybernetic threat, which is network disruption rather than physical destruction. [7]

A Corporation cyber war attack expected to increase rapidly each year, and there isn’t any optimal solution to solve this problem till now. So the first step must be to study what are a corporation cyber war and its impact on corporations, because the first step to solve any problem is to understand it then to think about a solution for it.

An Information Warfare is defined by 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. Information Systems are also defined in the same paragraph as Information Systems. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information. [1]

The information warfare composes of three types as proposed by [1]; the first type is Personal Information Warfare where it describes attacks against an individual’s electronic privacy. The second type is Corporate Information Warfare; it describes competition, or better said today's war between corporations around the world. The third type is Global Information Warfare, This type of Warfare works against industries, global economical forces or against entire countries or states.

This paper focuses only on corporation cyber war as an ever growing problem. While most researches and books focus on Global Information Warfare and ignore corporation information warfare, so this paper came to focus on this type of attack in more details and how to defend against this type of attack in efficient way.

DOI: 10.5176/2251-3043_3.3.267

The corporate information warfare is not new, it was known in the past by “espionage" is well from the cold war where Russian and American spies tried to gather information about each others. 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 use computers to make there business and those computers, networks has a vulnerabilities that can be used by some corporations to launch corporation cyber war .

The problem of corporation cyber war will cause big problem to many companies and users in different region where The *MacAfee 2009-2010* report says that, many corporations now faces new type of attack that are related to corporations cyber war [2]. A corporation’s cyber war can be used by one corporation to gather important information about another competitor to gain superiority on them, as an example if one of corporations participated in specific tenders and it launches corporation cyber war against other competitors who participated in the same tender then this corporation can gain superiority and gain the tender.

The impact of corporation cyber war ranged from financial losses to reputation losses which may lead to global crisis or may lead to war between countries as worst case.

Therefore, the need to ensure information integrity on many societal levels is growing, especially when the goal is to achieve an advantage over opponents and/or competition. Because of their specific natures, cyberspace and cybercrime create numerous dilemmas in relation to questions of general security. [4]

Attacks can take many forms, ranging from cyber espionage by foreign intelligence services to attempts to interrupt a company’s physical operations. These threats have grown more sophisticated over time, making them more difficult to detect and defend against. [5]

Current and future leaders should take a proactive approach to cyber warfare instead of a reactive one and unite in adjusting the laws of war to cyberspace. [6]

This paper focuses on corporation cyber war in the Middle East in general and chooses Jordan as a case. This paper begins by looking at the strategy format and problem statement of corporation cyber war and then defining the strategy target and mentions the strategy to defend against a corporation’s cyber war.

Problem Statement

This research will try to study all aspects of corporation cyber war to find a best solutions for cyber war, during this research will contain more information about existing theoretical and practical studies of corporation cyber war to develop strategy that can be implemented in any company and to use data loose prevention technology to solve the corporation cyber war attacks.

The research will use the models and framework and may use software development methodology according to available time for research.

Strategy Format

A corporation cyber war strategy is a typical strategic planning to drive most corporations in the Middle East in general and specially for Jordan strategy. This strategy began by formulating high level strategic driver, which represents the end-vision in terms of target to achieve and challenges to overcome —for the different business corporation sector over the next five years, 2010-2015. A corporation cyber war strategy that defines the specific solutions required—in the form of objectives, outcomes, and the actions needed to achieve them— to realize the strategic drivers. Figure (1) represents an overview of the framework.

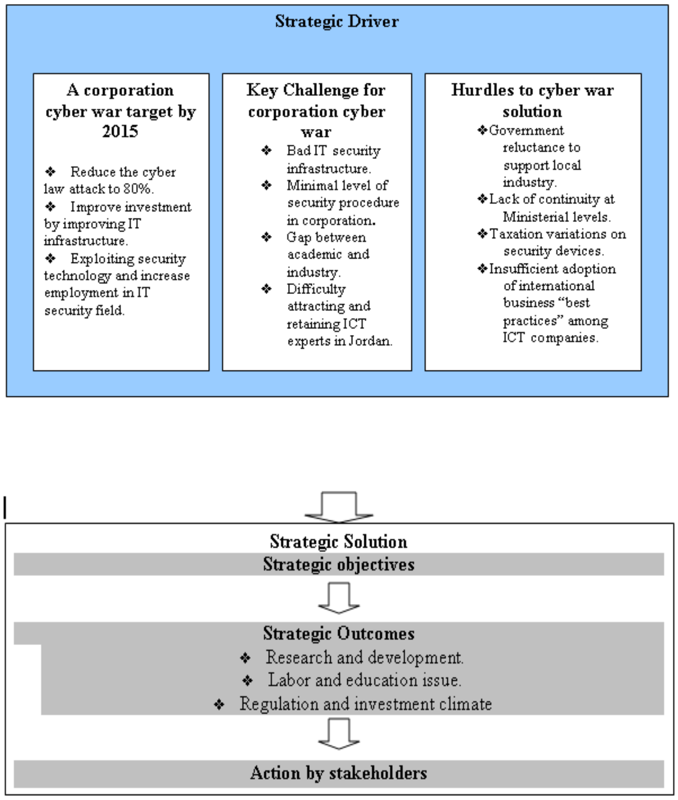

Strategic Driver
A corporation cyber war target by 2015
❖ Reduce the cyber law attack to 80%.
❖ Improve investment by improving IT infrastructure.
❖ Exploiting security technology and increase employment in IT security field.
Key Challenge for corporation cyber war
❖ Bad IT security infrastructure.
❖ Minimal level of security procedure in corporation.
❖ Gap between academic and industry.
❖ Difficulty attracting and retaining ICT experts in Jordan.
Hurdles to cyber war solution
❖Government reluctance to support local industry.
❖Lack of continuity at Ministerial levels.
❖Taxation variations on security devices.
❖Insufficient adoption of international business “best practices” among ICT companies.
Strategic Solution
Strategic objectives
Strategic Outcomes
❖ Research and development.
❖ Labor and education issue.
❖ Regulation and investment climate
Action by stakeholders

Figure 1: Corporation Cyber war Strategy framework.

The remainder of this section provides a brief overview of the elements of the framework. The remainder of the document represents the results in more detail.

Key Challenges In parallel to define the three high-level strategic goals, this paper identifies four key challenges faced by the ICT industry in Jordan that the strategy must address to reach the 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 and most of them don't upgrade their existing security infrastructure periodically.

- Minimal level of security procedures in corporation. Most of companies in the Middle East in different sector don't implement minimum level of security procedures to protect their works, because most of them don't know the real size of threats that can have an effect on their works and their market and they don't follow security standards or have clear pest practices to implement security inside their works and most of corporations don't provide their employees especially in IT departments with latest information, network and computer security courses as well as awareness other employees with knowledge about important of IT security and other related topics.

- Gap between academia and industry. All universities in the Middle East do not produce enough ICT graduates with the competencies required to sustain growth in the industry. In addition to that, industry needs to communicate its skill needs, better cultivate talent, and facilitate a smooth labor market for ICT professionals. Most important reason is that most universities focus on theory but don't provide their graduates with enough knowledge of how to apply those theories in real life application.

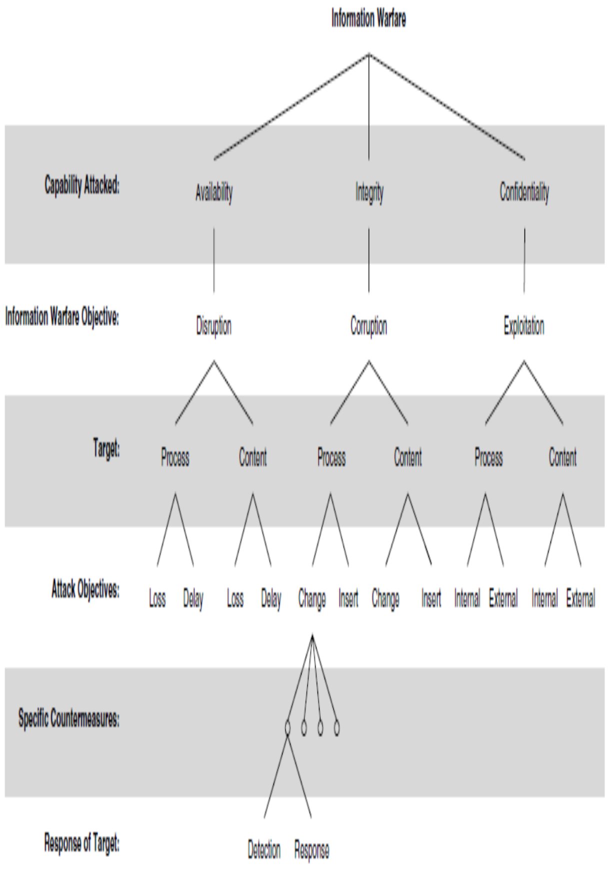
- Difficulty attracting and retaining ICT experts in the Middle East. Countries in the Arab world are at a competitive disadvantage in the regional and international labor market in some ways. It needs to be more competitive to sustain high-value industry productivity and growth.

Strategic Goals

This strategy will develop three primary strategic goals to be achieved over five years that will help Jordan to move forward in its efforts to use ICT to improve the life of all Jordanians. These goals are:

- Reduce the cyber law attack to 80%.

By defining nature of cyber war attack we can know the method that enemy take to launch the attack and then to design countermeasure for this attack see figure below for details



det Figure 1: Classification by confidentiality, integrity, and availability [reprinted with permission from Waltz, E. (1998) *Information Warfare: Principles and Operations*, Artech House, Norwood, MA].

Figure 2: Classification of attacks.

- Improve investment by improving IT security infrastructure.

By studying existing infrastructure in a corporation we can make risk assessment and then rebuild some old infrastructure and replace it with new efficient way.

- Exploiting security technology and increasing employment in IT security field.

Also the strategy focuses on increasing awareness about the impact of corporation cyber war and how it can have an effect on corporations.

The strategy aims to achieve these goals within five years and some part of those goals by the end of 2011 according to national ICT strategy 2007-2011.

Hurdles

In addition to the four key challenges faced by the corporation in the Middle East in general especially in Jordan, this strategy identifies a number of systemic hurdles to the growth of corporations (and all industries, to different extents):

- ❖ Government reluctance to support local industry. Because the Government is such a large part of Jordan's economy, its actions as producer and consumer—as well as its policymaking, regulation, and executive roles—have a significant impact on the industry. Government could do more to support local industry—without compromising its mandate to serve 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 such as the National ICT 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.
- ❖ Taxation variations on security devices. Jordan at a competitive disadvantage in the regional and international labor market because it is considered high, and many taxation variation are on IT security devices and on internet and this are large weaknesses that will prevent corporation from improve and upgrade existing IT infrastructure they have.
- ❖ Insufficient adoption of international business "best practices" among ICT companies. Most corporations don't follow or implement specific security standards, and don't follow best security practices to protect its work in efficient way.

The several strategic objectives and outcomes identified in corporation cyber war Strategy will help the government and a corporation to overcome these hurdles and achieve the high-level strategic objectives.

Pillars

A corporation cyber war strategy identified four dimensions or pillars of strategic activity necessary to fulfill the strategic goals:

- ❖ Research and development.
- ❖ Labor and education issue.
- ❖ Regulation and investment climate**.**

Each challenge and hurdle poses requirements for action in one or more of the pillars. The pillars serve to organize the individual expertise that developed the strategy and to differentiate the strategic activities recommended by a corporation cyber war strategy.

Strategic Objectives and outcomes

A corporation cyber war strategy decomposes the three high level strategic objectives into many objectives that must be achieved in order to fulfill the three high-level objectives. These strategic objectives are, by their nature broad—requiring outcomes from multiple pillars and by multiple actors.

A corporation cyber war further decomposed these objectives into many strategic outcomes that represent fulfillment of the objectives. (A few outcomes are replicated if they tie equally to multiple strategic objectives.) Each outcome is associated with a pillar based on the dimension of activity Measured-assigned one or more performance indicators to most—and be fulfilled by one or more actions, or projects, to be conducted by various stakeholders. Also the strategy will prioritize the outcomes as high, medium, or low, based on their contribution to the strategic objectives. The strategy also designated the sector (either government, industry, education, or higher education, other business corporation) 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.

A. Actions

The strategy decomposed all outcomes into actions or specific projects to be conducted by one or more stakeholders to achieve the outcomes. For each project, we identified one lead stakeholder, e.g., private companies themselves, the Ministry of ICT (MoICT), Ministry of Higher Education and Scientific Research (MoHESR), universities themselves, the Telecommunications Regulatory Commission (TRC), the Ministry of Finance (MoF), the Ministry of Industry and Trade (MIT), etc., and any other stakeholders that 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 has listed the actions in the form of a project plan.

And the strategy will add successive levels of detail to each action/project as appropriate.

G. Summery of this section

In order for Jordan to come to grips with the challenges it faces today, it needs for Government and corporation to sustain an active partnership, each of them taking ownership of its role in addressing the issues that exist in government, business and society. This strategy is intended to mark the first steps toward such a partnership and through collaboration between corporation and Government. By seeking out interactive, creative approaches to the problems facing the country, a corporation sector can spur growth in the economy, social development, and improvement in government.

H. Methodology

The main methodology used to design the strategy is from management "top-down" brainstorming to define the strategic drivers ((high-level strategic, goals, key challenge, and hurdles).

Implementation and governing the strategy

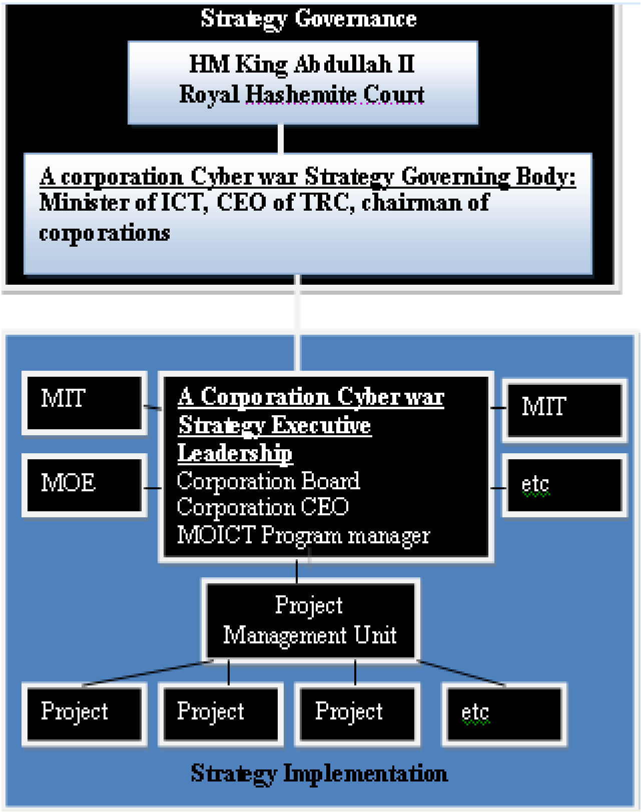


Figure 3: corporation cyber war Strategy framework.

The following sub-sections describe each element. Once His Majesty, King Abdullah II approves the final version of this document, representing the consensus of the industry and key Government stakeholders, it will be necessary for HM to activate implementation of the strategy. The high-level strategic objectives, , outcomes, and actions constitute a "project plan," or the list of actions required to achieve the strategic objectives and outcomes. Activation of the strategy will entail directing a corporation cyber war sponsors to lead maintenance of this project plan. It will also entail directing a corporation cyber war sponsors and Government stakeholders—especially MoICT, TRC, Jordanian military and security enforcement agency, MoHESR, MoF,MOJ, and MIT—to participate and execute 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 sponsors will work with the Government to secure and track cooperation of these stakeholders.

Rational for the strategy

The Research and development Pillars.

Jordan as a developing country faces lack of scientific research percentage in general and in corporation cyber war scientific research and development topics, because most of people don't take corporation cyber war as a real threat that may affect on businesses environment. They don't know the huge impacts for cyber war on investment infrastructure, the main problem that faces information security scientific research is limited budget that assigned for research and development that refer for the following reasons:

- Private sector isn't interested in the importance of scientific research on their work; most of corporations don't have specific department or sections for research and development especially for IT security field. The National Agenda identified key performance indicators related to overall research and development, and set targets for its development, including the increase of overall R&D spending to 1% of GDP in 2012.

- The corporation cyber war is considered as a new topic, because there are no tangible effects on businesses so many corporations doesn't consider it as a real threat for them.

- IT security changing rapidly, so it's difficult to track all new security topics and most corporations don't know what is the output of those researches and how its outcomes can be implemented.

Government start to face cyber threat in general but it doesn't take enough steps to face corporation cyber war threat in proper way.

Jordan’s National Agenda also set a number of objectives that are aimed at developing technology-related R&D activities. Some of these are5:

□□ Provide funding to strengthen the links between economic sectors and university R&D programs.

□□ Provide incentives for private companies to participate in R&D.

□□Enhance patent registration and intellectual property protection.

□ □Support R&D through direct financing and ensure links between investors and researchers

□ □Improve the overall quality of human resources capabilities.

In order to achieve those objectives the following steps must be taken first:

The barriers between corporations and universities must be removed for the innovation and research to move into marketable products and jobs. There are needs to establish partnership between public and private sector. Increase awareness of cyber war threat and its impacts on public and private sector.

The Labor and education issue Pillars.

The second pillar of the strategy is Labor Issues & Education. To achieve this pillar we must understand the challenge that faces Jordan in this field:

- Increasing number of ICT graduates who have strong theoretically background but they don’t have appropriate skills especially in information, network and computer security fields because of lack of cooperation between universities and industry.
- Jordan suffers from an emigration of its highly qualified workforce to other countries. Because of low salaries in private and public sector.
- Public and private sector don’t provide scholarship for ICT employee to obtain higher degree in ICT 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 objectives must be done:

- Improving quality of higher education rather than quantity especially in information, network and computer security.
- Increasing salaries of qualified ICT graduations.
- Encourage ICT employee to complete higher degree in information, network and computer security field.
- Monitor quality of information, network and computer security education in universities. *The Regulation and investment climate Pillars.*

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

- Improving new laws that handle corporation cyber war threat, and put appropriate penalties on any person or corporation who participate to launch it.
- Improving regulations to facilitate improving information, network and computer security by enforce security standards like ISO or local standards and encourage corporations to implement latest security technology without taxes.
- Each corporation must be responsible on any threat action that launch from or to it.

Strategy Details

The following tables list the strategic objectives, strategic outcomes, and actions, as defined in the previous section.

Table 1. Strategic Objectives and Outcomes

The following tables list the strategic objectives tied to the three high-level strategic objectives, and the strategic outcomes tied to the strategic objectives. The Pillar with primary relevance to the outcome is also listed.

Strategic objectives	**Outcomes (Pillars)**
1) Reduce the cyber war attack to 80%	
1.1) Increase awareness of corporation cyber war.	1.1.1) conducting cyber war session for public and private sector.(The Labor and education issue Pillars)
	1.1.2) conducting corporation cyber war threat session and courses for corporation's employees.
1.2) enhance security practices inside corporations.	1.2.1) enforce implementing security certificate according to nature of business for each corporations (The Regulation and investment climate Pillars)
	1.2.2) establishes and enable secure infrastructure for both public and private sector. (The Regulation and investment climate Pillars)
1.3) improve response for cyber war threat	1.3.1) enforce all corporations that face cyber war threat to inform centralized cyber war center that are located in ministry of IT and communication. (The Regulation and investment climate Pillars)
	1.3.2) Establish scientific research center for corporation cyber war that focus on impacts and how to efficient response to cyber war threat and methods used to launch this attack.(The Research and development Pillars)
1.4) Increase Budget for security research.	1.4.1) Establish collaboration between universities, public and private sectors to fund security research.

Strategic objectives	**Outcomes (Pillars)**
Improve investment by improving IT infrastructure.	
2.1) improve current IT infrastructure	2.1.1) improve old and last to date IT infrastructure for public sector. (The Research and development Pillars)
	2.1.2) improve old and last to date IT infrastructure for private sector. (The Research and development Pillars)
	2.1.3) review current technology and compare them with current technology using cost benefit analysis. (The Research and development Pillars).
2.2) Prevent anti-competitive behavior in the broadband market (Connectivity Pillar)	(2.2.1) Create a competition board, with Competition Directorate representation, within TRC (TRC, MIT, private companies (licensees)) (Q3 2007) (The Regulation and investment climate Pillars)
2.3) Gradually reduce sales taxes on internet access to the same level as other basic goods (Connectivity Pillar)	2.3..1) Lower tax rate (MoF, MoICT) (The Regulation and investment climate Pillars)
2.4) Eliminate sales tax to lower out-of-pocket cost for computer security devices (Regulation & Investment Climate Pillar)	2.4.1) Conduct a study detailing revenue impacts and presents a recommendation for adjusting taxation of computer security. (The Research and development Pillars).
2.5) Reduce barriers to Jordanian companies' ability to sell services over the internet to consumers in other countries (Regulation & Investment Climate Pillar)	2.5.1) Formulate and present to Parliament e-security laws, regulations, and processes (MoICT) (Q4 2008). 2.5.2) Implement digital signature laws and regulations

	(MoICT) (Q4 2008) 2.5.3) Implement PKI processes and technology (MoICT) (The Regulation and investment climate Pillars)
(2.4.8) Improve the academic sector's contributions to industry R&D (Research & Development Pillar)	2.4.8.1) Increase academic research relevant to ICT industry needs (universities)

Strategic objectives	**Outcomes (Pillars)**
Exploiting security technology and increasing employment in IT security field**.**	
3.1) improve current IT Security infrastructure	3.1.1) improves old and last to date Security IT infrastructure for public sector. (The Research and development Pillars)
	3.1.2) improve old and last to date IT security infrastructure for private sector. (The Research and development Pillars)
	3.1.3) review current security technology and compare them with existing security technology using cost benefit analysis. (The Research and development Pillars).
3.2) Preparing good alternative solution	3.2.1) prepare alternative for each type of security threats.
	3.2.2) Improve disaster recovery locations for both private and public sector. (The Research and development Pillars).
3.3) Evaluate efficiency of security countermeasure.	3.3.1) improve assessment and evaluation procedure for new security product and exiting security product. (The Research and development Pillars).
	3.3.2) Establish security lab to test all security products before launching it to local market, this must be done by customer protection department with coordination with MOCIT. (The Research and development Pillars).
3.4) Improve skills of security IT employees	3.4.1) encourage and offer courses for IT security employee to develop their skills, and enhance their capability to cope new security challenges. (The Research and development Pillars).
3.5) improve security procedures.	3.5.1) enforce appoint IT security specialist in each private and public sector. (The Regulation and investment climate Pillars)
3.6) Ensure that university students have a good computer security background	3.6.1) Ministry of higher education must ensure that the level of academic programs of security in universities is acceptable and each university offers courses in security must have security labs and appropriate infrastructure. 3.6.2) private sector must coordinate with academic world by enabling security students to practice security skills in practical way. (The Regulation and investment climate Pillars)

Conclusion

This strategy will help Jordan as a public sector to protect all corporations working inside or outside Jordan as well as improve investment in JORDAN, because it will help offering secure environment for investment in Jordan.

In order to realize the benefits promised by Information and Communications security Technology, Jordan's public and private sector must work closely together.

This strategy will be first step toward defend against corporation cyber war attack, but there are needs to develop this strategy by reviewing it periodically to cope with new type of corporation cyber war that may appear in future.

References

[1]. Reto E. Haeni , Information Warfare an introduction, 1997.

[2]. MacAfee report 2009-2010,**ttp://sanjose.bizjournals.com/sanjose/stories/2010/01/25/daily74.html**

[3]. National ICT strategy for Jordan, 2007-2011.

[4]. IGOR BERNIK, Information Warfare Effects on Businesses in Slovenia, 2013.

[5]. Blake Clayton and Adam Segal ,ENERGY BRIEF Addressing Cyber Threats to Oil and Gas Suppliers,2013

[6]. Adiya Kostyuk & Marielle Ali, THE CYBER DOGS OF WAR: JOINT EFFORTS OF FUTURE WORLD LEADERS IN THE PREVENTION OF CYBERWARFARE,2013.

[7]. Daniel K. Rosenfield, RETHINKING CYBER WAR, Critical Review: A Journal of Politics and Society Volume 21, Issue 1, 2009 pages 77-90.

Dr. Amer Nizar AbuAli is an Associate professor in CIS department, Faculty of Information Technology, Philadelphia University. He has more than 18 years of teaching, projects supervision and research experience. He has attended and participated in many international conferences. He is a peer reviewer for many conference and journal.

Saeb Sisan is an Instructor in SE Department, Faculty of Information Technology, Philadelphia University.