International Journal of Cyber-Security and Digital Forensics (IJCSDF) 4(4): 482-497
The Society of Digital Information and Wireless Communications, 2015 (ISSN: 2305-0012)

Cyber Warfare Awareness in Lebanon: Exploratory Research

Ale J. Hejase
School of Business, Lebanese American University
Beirut – Lebanon
ale.hejase@lau.edu.lb

Hussin J. Hejase
Faculty of Business Administration, Al Maaref University
Beirut - Lebanon
hussin.hejase@mu.edu.lb

Jose A. Hejase
IBM Systems and Technology Group, Armonk, Texas, United States
jahejase@us.ibm.com

ABSTRACT

Many believe that the coming war is a cyber-war that revolves around cyber weapons; to many others, the world is already at the core of this war. Names like Stuxnet, Duqu, Gauss and Flame have become familiar, malware projects known to experts in the field of cyber weapons. One asks: what type of awareness and preparation students need to deal with the cyber warfare challenges and threats?

Countries have prepared for the aforementioned challenges and threats, while Lebanon is not. This research investigates current status of cyber warfare awareness and clarifies what changes may be incorporated into the Lebanese sectors, including the educational one.

This study is exploratory and uses a survey distributed to 635 students, educators and managers. Findings reveal that in Lebanon, the educated community not only lacks awareness but also knowledge of what is happening in the arenas of cyber warfare, cyber weapons and cyber security.

KEYWORDS

Awareness, exploratory research, cyber-war, cyber warfare, Lebanon

1 INTRODUCTION

"Cyber warfare involves the actions by a nation-state or international organization to attack and attempt to damage another nation's computers or information networks through, for example, computer viruses or denial-of-service attacks" [1]. Likewise, cyber war may be defined as "the use of computers to disrupt the activities of an enemy country, especially the deliberate attacking of communication systems" [2]. In the United States of America, "From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyber weapons, according to participants in the program" [3]. Similarly, in parallel with President Obama's declaration, Ilan Berman, the vice president of the American Foreign Policy Council issued a serious warning: "Over the past three years, the Iranian regime has invested heavily in both defensive and offensive capabilities in cyberspace" [4]. Eugene Kaspersky, one of the main owners of the famous antivirus Russian firm declared that: "The recent discovery of the malware called Flame as well as past incidences of cyber weapons Stuxnet and Duqu are ushering a new period of global conflict that is secretive, precise, and destruction" [5].

The most recent documented cyber-attack was reported on April 10, 2013. That day, the breaking news of The Jerusalem Post read "Anonymous threatens cyber-attack on Israeli sites" [6]. Anonymous indicated that the reason behind their attacks is due to the Isreali's endless human rights' violations. Anonymous is an underground ideology group that has previously launched attacks against organizations that did not support Wikileaks (The release of hundreds of USA State Department's secret cables), and against the Australian Parliament House when it introduced Internet filtering services in Australia [7]. Likewise, HAARETZ, on the same aforementioned date, reported that "Hackers threaten to 'wipe Israel off Internet map' in massive cyber attack" [8]. According to the reported news, the attacks were launched by the Anonymous group of hackers in protest against the Isreali's policies in the West Bank and Gaza.

Cyberwarefare is presented as a powerful weapon in political conflicts, espionage and propaganda [9]. In fact, the history of recorded cyber attacks involving nations dates back to September 6, 2007, when the Isreali Air Force destroyed what they claimed to be a mass destruction complex being built by North Korea. The air raids of that date could not have fullfilled their objectives was it not for the cyber assault employed, and which ended by controlling what the Syrian's air defense radars depicted: the cyber activity made the radar screens look as if the Syrian sky was empty [10]. Prior to this 2007 event, in 1995, the Time Magazine published a remarkable cyber-war scenario narrated by Colonel Mike Tanksley, in which the USA cyber warriors take control of the enemies' phone system and emit propaganda over their radio and television broadcasts [11].

Other incidents of cyber wars were recorded, for example, the Estonian case when their governement's web-based services and many other businesses' sites were subjected to denial of service attacks (DoD) as a result of the outcry from the Russian population in Estonia who rejected the moving of a statue of a Soviet soldier from the city center to a war cemetry [7]. Similarly, in August 2008, the Russians invaded the Republic of Georgia and their troops achieved distiguished successes that were mainly attributed to the skillful cyber attacks. Another significant incident took place in 2007, and was known in 2010, when reports carried the news that the Stuxnet computer virus was deployed against Iran in an attempt to attack the operation of the industrial computers that control the nuclear Uranium enrichment facility at Natanz [12]. Likewise, in September 2011, some Hungarian researchers revealed Duqu, a cyber-weapon that was developed to steal information on industrial control systems [13]. In May 2012, the Russian antivirus Kaspersky Laboratory, upon studying the Stuxnet virus, identified a Stuxnet variant that was called Flame, whose main objective was to spy on computers; for example, searching for keywords in secret files, then making summaries and transmitting them without being detected [13]. Following the discovery of Flame, Kaspersky Laboratories announced the discovery of 'Gauss', a new cyber-espionage toolkit that targets users in the Middle East with the intention of stealing sensitive data such as online banking account credentials [14].

On the other side of the globe, the traditional enemies are confronting each other: Indians with Israeli help standing against Pakistan in the new cyber battle field [15]. Moreover, the antivirus and computer security company McFee stated in its 2007 annual report that 120 countries have been developing ways to use the web for espionage operations [16]. In fact, the record of incidents contains many other reported cases that point to one conclusion: Cyber warfare incidents are continuously increasing among nations, organizations, terrorists and groups. So far, these incidents have involved a political message that most of the time is ignored by citizens; however, the expectations are that in the future, serious consequences may arise that can generate mass panic that could lead to military interventions [9]. According to Greengard [17], in the past, it was a simple task to recognize an invading army with its planes and tanks; today in the information age, it is very difficult to identify attacking armies formed of bits, bytes or computer network packets.

Even though Eugene Kaspersky had warned of a cyber-terror apocalypse, when he said "It's not cyber war, it is cyber terrorism, and I'm afraid the game is just beginning. Very soon, many countries around the world will know it beyond a shadow of a doubt" [18], a study by Dr. Ian Brown of the Oxford Internet Institute, and Professor Peter Sommer of the London School of Economics, concluded that it is highly unlikely there will ever be a pure 'cyber war' fought solely in cyberspace [19]. Likewise, a recent study as to whether cyber war is really coming concluded that unlike the nuclear theorists of the 1950's, cyber way theorists of this era have never experienced devastating cyber war weapons, and that according to the various existing evidence, cyber war will not take place [20].

Amid all these debates, the art of human hacking or, professionally said, social engineering, appears to be another focus point within the context of cyber war and cyber weapons. Indeed, 'Social Engineering', is "the art or better yet, science, of skillfully maneuvering human beings to take action in some aspect of their lives" [21]. The social engineering weapon in cyber warfare is gaining more terrain every day simply because as information technology companies are improving the vulnerability of their software and hardware products, hackers, malicious intruders, and above all cyber warriors are targeting the weakest link of the chain: the operating people.

The issue of cyber warfare awareness has been tackled in the literature; specifically, Grobler, Van Vuuren and Zaaiman [22] conducted a study to evaluate awareness of cyber security in South Africa. They established that the development of cyber security awareness modules should be implemented in local communities; furthermore, the researchers concluded that by targeting the communities that leave the network vulnerable, the safety of the whole global community network is influenced and improved. Another awareness study by Dlamini & Modise [23], calls for a synergy approach of cyber security awareness mechanisms as the prime barrier against cyber-attacks. The authors argue that the limited role of the government in awareness campaigns limits the wide spread of cyber security awareness; thus, making the cyber counter space more vulnerable.

1.1 Cyber warfare awareness in the world

Today, most states around the globe are trying to develop at least defensive capabilities to face the dangers of cyber wars. Along this track, Canada glows as a nation that has emphasized both mitigation and intervention in case of a cyber-attack [24]. Moreover, the Canadian Emergency Management Act of 2007, established clear management roles and responsibilities to be performed by the different authorities at times of emergency. These roles include: prevention, response, recovery and protection [24]. On the other hand, the EU Member States and EU institutions have set the target that by 2012 there should be a fully operational Computer Emergency Response Team (CERT), which will cooperate with law enforcement agencies to prevent and react to cyber- attacks [25]. On another side of the globe stands South Africa; it is making continuous efforts to develop skills in the cyber warfare arena. In fact, it was reported that in 2004, the South African Council for Scientific and Industrial Research (CSIR) started an information warfare battle laboratory. Furthermore, in order to acquire innovative cyber war talents, South Africa continues to host international conferences on information warfare and security [26].
Whereas, the US and China have developed both defensive and offensive capabilities. For example, "The Echelon system is widely accepted to be the most pervasive and powerful electronic intelligence gathering system in the world", is developed in the US and installed to intercept the information through the Intelsat and Inmarsat satellites that are considered to carry the vast majority of global civilian's, diplomatic' and governments' communications [27].

1.2 Cyber warfare awareness in Lebanon

Where does Lebanon stand in the middle of the aforementioned parties? Answering this question is one of the main goals of this

research. The next sections will evaluate the level of cyber warfare awareness in Lebanon, with special focus on the highly educated sectors of management and academia. The highly educated target research population is chosen because people that work with matters related to information security and cyber warfare are, in general, relatively well-educated and try to keep their skills as sharp as possible [7]. Moreover, the present study offers a wide evaluation of awareness status as to cyber warfare weapons and security measures within Lebanon, with the aim of proposing effective measures that can be applied both at the governmental and academic levels to hamper cyber warfare, making sure that only minor damages ensue as a result. A major goal of this study is to advise both public and private sectors as to the correct path to follow through encouraging the government to set standards which ensure that important networks are protected, and by making the businesses in particular and public in general ready to understand, detect and possibly react whenever a cyber-attack is presented.

2 METHODOLOGY, RESEARCH TOOLS, AND SAMPLE

The researchers used a simple straight forward questionnaire as the main tool to collect data. The aim is to assess the Lebanese public's awareness of cyber warfare and cyber security. The questionnaire is composed of 20 questions: 16 related to the topic and 4 questions on the demographics of the respondents. The questionnaire was divided into three parts as follows:

Part I, History and Background Questions.
It consists of 5 questions (question 1 to 5)

Part II, Technical Questions.

It consists of 11 questions (questions 6 to 16)

Part III, Demographics.
It consists of 4 questions (questions 17 to 20)

The sample used in this study is composed of 635 respondents who are relatively educated and conveniently selected based on their education level; therefore, respondents are students from different university environments where the authors have direct academic interests and relations. As indicated before, the authors believe that a topic such as cyber warfare awareness should be investigated within an educated community. All collected questionnaire forms included valid data and none were excluded. Data analysis was performed using SPSS (Statistical Product and Service Solutions, an IBM product acquired by IBM in 2009 (p. 58) [28].

3 RESULTS AND FINDINGS

The related demographic data associated with age, gender, education and institution are shown in Tables 1 through 6. Table 1 shows that the mean respondent age is 22.69 years with a standard deviation of 5.869 years, and minimum and maximum of 17 and 62 years, respectively. As for gender, Table 2 shows that 365 of the respondents are males, forming 57.5% of the total number, and the 270 females form 42.5 percent of the sample. Table 3 shows that the undergraduate university level dominated the educational level of the respondents, with a percentage equal to 73.1%, with only 24.7% holding a Master's degree, and only 2.2% hold a PhD. Considering the main activity executed by the respondents, the analysis concluded that 70.7% of the respondents are students, and the rest are divided among educators, employees and managers with percentages equal to 4.1%, 19.4% and 5.8% respectively, as shown in Table 4. Table 5 illustrates that 32.8% of the respondents were selected from within the American University of Science and Technology, 37.5% belonged to the Lebanese American University, 8.2% from the Islamic University of Lebanon, 12.1% from the Lebanese University, 4.7% from the University of The Holy Spirit (USEK), and finally 4.7% from Saint Joseph University (USJ). Lastly, Table 6 provides information related to respondents' technical fields of specialization; it shows that 91.7% have a business background with 5.2% in engineering and the remaining 3.1% in information technology.

Table 1. Distribution of respondents' ages

	N	Minimum	Maximum	Mean	Std. Deviation
Age on Your Last Birthday	635	17	62	22.69	5.869

Table 2. Distribution of respondents' gender

Gender	Frequency	Percent	Cumulative Percent
Male	365	57.5	57.5
Female	270	42.5	100.0
Total	**635**	**100**	

Table 3. Respondent's current educational level

Educational Level	Frequency	Percent	Cumulative Percent
University	464	73.1	73.1
Masters	157	24.7	97.8
PhD	14	2.2	100.0
Total	**635**	**100**	

Table 4. Respondent's current major main activity

Major Main Activity	Frequency	Percent	Cumulative Percent
Student	449	70.7	70.7
Educator	26	4.1	74.8
Employee	123	19.4	94.2
Manager	37	5.8	100.0
Total	**635**	**100**	

Table 5. Respondents' university entity

University	Frequency	Percent	Cumulative Percent
AUST	208	32.8	32.8
LAU	238	37.5	70.2
Islamic University	52	8.2	78.4
Lebanese University	77	12.1	90.6
USEK	30	4.7	95.3
USJ	30	4.7	100.0
Total	**635**	**100**	

Table 6. Respondents' technical field or specialization.

Technical Field or Specialization	Frequency	Percent	Cumulative Percent
Business	582	91.7	91.7
Engineering	33	5.2	96.9
IT	20	3.1	100.0
Total	**635**	**100**	

3.1 Quantitative Results: Statistics

The central aim of this study is to assess the level of cyber warfare awareness in Lebanon. The authors started by conducting an overall frequency assessment of the aforementioned questionnaire questions. The sample of 635 Lebanese respondents revealed, as indicated in Table 7, that 26.5% has never heard of cyber warfare, and only 4.7% has heard about it within the context of class lectures. The majority, or 29.4%, has heard about cyber warfare from the Internet, while those who are aware of it, 20.5%, their knowledge have been attained from news media. Also, those who have read about the subject by themselves are a minority that did not surpass 0.5%; this is in fact a percentage that is typically recorded for Arab readers [29].

Table 7. Source of hearing of cyber warfare

Source	Frequency	Percent	Cumulative Percent
News Media	130	20.5	20.5
Book/Magazine/Journal	7	1.1	21.6
Internet	187	29.4	51.0
Friends	61	9.6	60.6
Class Lecture	30	4.7	65.4
News Media & Book /Magazine /Journal	3	0.5	65.8
Internet & Book/Journal/Magazine	1	0.2	66.0
News Media, Internet & Book /Journal /Magazine	20	3.1	69.1
Internet & Friends	20	3.1	72.3
Never Heard about Cyber Warfare	168	26.5	98.7
Other	8	1.3	100
Total	**635**	**100**	

Likewise, the results in Table 8 match those of Table 7; they reveal that around 28% never heard of cyber warfare and that 38.6% of the respondents have heard of the negative features of cyber warfare.

Table 8. What was heard of cyber warfare

Attribute	Frequency	Percent	Cumulative Percent
Positive	117	18.4	18.4
Negative	245	38.6	57.0
Neutral	90	14.2	71.2
Positive & Negative	6	0.9	72.1
Never Heard about Cyber Warfare	177	27.9	100.0
Total	**635**	**100**	

The respondents were assessed according to their personal views on how they consider cyber warfare; the results as shown in Table 9, uncover again that around 50% of the respondents believe that it is very dangerous or annoying, and another 26.5% point out that they have never heard of it. Similarly, Table 10 demonstrates that 58.6% of the respondents contend that they are witnessing cyber warfare, while 25% reaffirm that they have not heard of cyber warfare.

Table 9. Consideration given to cyber warfare

Consideration	Frequency	Percent	Cumulative Percent
Very Dangerous	253	39.8	39.8
Accidental	26	4.1	43.9
Annoying	65	10.2	54.2
Not a Big Issue	48	7.6	61.7
Heroic	64	10.1	71.8
Never Heard about Cyber Warfare	168	26.5	98.3
Other	11	1.7	100.0
Total	**635**	**100**	

Table 10. Witnessing Cyber Warfare

Witnessing Cyber Warfare	Frequency	Percent	Cumulative Percent
Yes	372	58.6	58.6
No	104	16.4	75.0
Never Heard about Cyber Warfare	159	25.0	100.0
Total	**635**	**100**	

Through question number five, the respondents were assessed as to whom they believe is responsible for taking measure against cyber war and cyber-attacks. Table 11 indicates that the government got the major vote with 58.7%, while 25% of the respondents negated having heard of cyber warfare. In fact, the results of the first five assessment questions of the questionnaire converged to prove that around one quarter of the sample are completely ignorant of matters related to cyber warfare; that is within an adult educated community as per the aforementioned demographics.

Table 11. Responsibility to React Against Cyber War & Cyber Attacks

Responsible Agent	Frequency	Percent	Cumulative Percent
Government	373	58.7	58.7
Business Organizations	41	6.5	65.2
Both Government & Business Organizations	46	7.2	72.4
Never Heard about Cyber Warfare	157	24.7	97.2
Other	18	2.8	100.0
Total	**635**	**100**	

The rest of the questionnaire revolves around technical issues related to cyber warfare and cyber-attacks. Questions 6 to 8 asked about three well-known cyber weapons that were discovered during the past four years, namely, Stuxnet, Duqu and Flame [5]. For the last years, these cyber weapons have been extensively covered by the public international media that emphasized the birth of new period of global conflict that is secretive, precise, and destructive [3]. Unfortunately, the three questions carried very negative awareness results among the 635 educated adult respondents; these results, as depicted in Tables 12, 13 and 14, show that 79.7%, 82% and 65.4% ignore having any knowledge pertaining to Stuxnet, Duqu and Flame, respectively. Only 26.9% of the respondents are aware of the recent cyber-attack weapon called “Flame”.

Table 12. Respondents' awareness related to Stuxnet

Stuxnet is	Frequency	Percent	Cumulative Percent
A Computer Brand	11	1.7	1.7
A Network Card	39	6.1	7.9
A Computer Cyber Game	42	6.6	14.5
A Computer Warm	21	3.3	17.8
I Don't Know	506	79.7	97.5
Other	16	2.5	100.0
Total	**635**	**100**	

Table 13. Respondents' awareness related to Duqu

Duqu is	Frequency	Percent	Cumulative Percent
A Japanese Weapon	26	4.1	4.1
A Chinese Car Brand	14	2.2	6.3
A Cyber Game	51	8.0	14.3
A Computer Warm	16	2.5	16.9
I Don't Know	521	82.0	98.9
Other	7	1.1	100.0
Total	**635**	**100**	

Table 14. Respondents' awareness related to Flame

Flame is	Frequency	Percent	Cumulative Percent
A Computer Virus	171	26.9	26.9
An American Gun	19	3.0	29.9
A Korean Rocket	11	1.7	31.7
A Computer Worm	5	0.8	32.4
I Don't Know	415	65.4	97.8
Other	14	2.2	100.0
Total	**635**	**100**	

Question number 9 was: Do you support Lebanese government's expenditure on training and equipping "cyber warriors" to defend Lebanon against outside attacks? Surprisingly, the word "warriors" stole the attention of most respondents, drawing their attention away from the real theme/ structure of the question. Thus, as shown in Table 15, around 75% of the respondents oppose the spending on equipping cyber warriors, out of which 50.2% declared a strong opposition. Moreover, 20.5% took a neutral position, revealingly demonstrating the low awareness level in the domain.

Table 15. Respondents' answers to Lebanese Gov.'s Spending on Training Cyber Warriors

Opinion	Frequency	Percent	Cumulative Percent
Strongly Support	11	1.7	1.7
Support	16	2.5	4.3
Neutral	130	20.5	24.7
Oppose	159	25.0	49.8
Strongly Oppose	319	50.2	100.0
Total	**635**	**100**	

The researchers, one more time, were astonished of the fact that the 635 educated adults are ignorant of what is going on around the world in relation to cyber-attacks and cyber security [6], [25] and [4]. In fact, Table 16 shows that the majority expressed their opposition or at least neutrality to matters related to the belief that the coming wars will be based on cyber-attacks.

Table 16. Respondents' answers on: Future wars will be based on cyber attacks

Opinion	Frequency	Percent	Cumulative Percent
Strongly Support	13	2.0	2.0
Support	44	6.9	9.0
Neutral	196	30.9	39.8
Oppose	239	37.6	77.5
Strongly Oppose	143	22.5	100.0
Total	**635**	**100**	

According to Hadnagy [21], Social Engineering is a major weapon used nowadays to gain control over information systems and open the road for cyber-attacks. When respondents were asked about it, Table 17 illustrates that only 9.4% are able to link social engineering to its real nature: the studying of the physical surroundings of a person.

Table 17. Respondents' awareness of Social Engineering

Social Engineering	Frequency	Percent	Cumulative Percent
Branch of Civil Engineering	24	3.8	3.8
The Construction of Social Networks	285	44.9	48.7
The Studying of the Physical Surroundings of a Person	60	9.4	58.1
Do not Know	126	19.8	78.0
Other	140	22.0	100.0
Total	**635**	**100**	

To close the cyber warfare awareness cycle, a series of tertiary familiarity short answers were required from each respondent on a specific well documented and commonly known cyber-attack. The statistical results are depicted in Table 18, which shows spam and junk mail are the most familiar attacks to 85.5% of respondents, and pharming i.e. tricking the computer user to supply confidential information (p. 279) [30] is the least familiar with 22.2%.

Table 18. Familiarity with various cyber attacks

Familiarity with	Familiar	Unfamiliar	No Answer
Spam and Junk Mail	543 85.5%	79 12.4%	13 2.0%
Denial of Service	227 35.7%	381 60.0%	27 4.3%
Smurfing	189 29.8%	419 66.0%	27 4.3%
Cyber Harassment	320 50.4%	291 45.8%	24 3.8%
Cyber Pornography	347 54.6%	263 41.4%	25 3.9%

Cyber Espionage	216 34.0%	390 61.4%	29 4.6%
Phishing	180 28.3%	430 67.8%	25 3.9%
Trojan Horse	348 54.8%	267 42.1%	20 3.1%
Ping	278 43.7%	330 52.0%	27 4.3%
Hacking	528 83.2%	91 14.3%	16 2.5%
Pharming	141 22.2%	464 73.1%	30 4.7%

On asking the respondents if cyber-attacks will replace classical bombs, Merkava tanks, Stealth jets, Patriot and Fajr rockets, etc…, as shown in Table 19, the percentage of neutral and unlikely respondents are around 60% with only 10.2% expressing that there is a strong likelihood that this will be the case.

Table 19. Cyber-attacks will replace common classical weapons

Cyber Attacks Replaces Common Weapons	Frequency	Percent	Cumulative Percent
Very Unlikely	52	8.2	8.2
Unlikely	141	22.2	30.4
Neutral	181	28.5	58.9
Likely	196	30.9	89.8
Very Likely	65	10.2	100.0
Total	**635**	**100**	

Respondents were asked in question 14 about their expectations as to their major concern if Lebanon faces a cyber-attack. The statistics of their answers is depicted in Table 20, which shows that the main concern is the disruption of banking and financial services (35.6%) followed by disruption of Internet services (31.2%).

Table 20. Major concern if Lebanon faces a cyber-attack

Major Concern if Lebanon Under Cyber Attack	Frequency	Percent	Cumulative Percent
Disruption of Internet Services	198	31.2	31.2
Disruption of Telephone Services	46	7.2	38.4
Disruption of Banking and Financial Services	226	35.6	74.0
Disruption of Airplane Services	31	4.9	78.9
All Disruption of Services	90	14.2	93.1
Other	44	6.9	100.0
Total	**635**	**100**	

Question 15 is related to the future view of the respondents regarding their belief that Lebanon would engage in a cyber-war sometime during the next ten years. As shown in Table 21, the percentage of neutral and unlikely respondents is around 43%, with around 18.3% only assuring that it is very likely that Lebanon will get engaged in such a conflict. Table 22 shows the respondents' answers with respect to the measures they deploy to limit cyber-attacks.

The results show that most respondents have deployed antivirus (84.7%) and firewall (73.7%) measures. Similarly, the table shows that least deployed measure is periodical penetration tests (22.5%).

Table 21. Answers to: Lebanon will engage in cyber war in coming 10 years

Believing Lebanon Will Engage in Cyber War in Coming 10 Years	Frequency	Percent	Cumulative Percent
Very Unlikely	33	5.2	5.2
Unlikely	70	11.0	16.2
Neutral	170	26.8	43.0
Likely	246	38.7	81.7
Very Likely	116	18.3	100.0
Total	**635**	**100**	

Table 22. Familiarity with various cyber attacks

Measures Employed to Limit Cyber Attacks	Yes Employed	Not Employed	No Answer
Antivirus	538 84.7%	41 6.5%	56 8.8%
Software Firewalls	468 73.7%	79 12.4%	88 13.9%
Data Encryption	249 39.2%	203 32.0%	183 28.8%
Data Recovery Strategies	336 52.9%	151 23.8%	148 23.3%
Training & Awareness	297 46.8%	218 34.3%	120 18.9%
Periodical Penetration Testing	143 22.5%	282 44.4%	210 33.1%
Intrusion Detection/Protection Systems	273 43.0%	205 32.3%	157 24.7%
Systems Accountability	159 25.0%	256 40.3%	120 34.6%

3.2 Quantitative results: tests of dependency

The cross tabulation of "Lebanese government's spending to train cyber warriors" against "Future wars are based on cyber-attacks" indicated that the two items are associated as a significant relationship was present with chi-square = 287.787, df = 16, and significance p = 0.000. The null hypothesis that there is no association between "Lebanese government's spending to train cyber warriors" and "Future wars are based on cyber-attacks" cannot be supported.

The cross tabulation of "Cyber-attacks replace Common weapons" against "Believing Lebanon will engage in cyber war in the coming 10 years" indicated that the two items are associated as a significant relationship was present with chi-square = 67.937, df = 16, and p = 0.000. The null hypothesis that there is no association between "Cyber-attacks replace common weapons" and "Believing Lebanon will engage in cyber war in the coming 10 Years" cannot be supported.

3.3 Quantitative results: correlations

A set of Pearson correlations were computed to determine if there are any significant linear relationships between some of cyber warfare statements. The correlation between respondents' age and their familiarity with the topic of social engineering came up to be 0.022 with p = 0.577. This means that the null hypothesis that there is no correlation between age and familiarity with social engineering

cannot be rejected. It seems that knowledge of social engineering is not significantly tied to age. In fact, the researchers tried to check if older respondents are more familiar with the subject of Social Engineering; the correlation computed between respondent's age and familiarity with the topic of Social Engineering was 0.022 with p = 0.577, indicating that the null hypothesis cannot be rejected. It appears that Social Engineering is vague to most respondents, irrelevant of age.

3.4 Quantitative results: factor analysis

A Principal Component Analysis (PCA) was conducted on items of the questionnaire in order to designate the content they reflect. The researchers started with questions "Future wars are based on cyber-attacks" and "Cyber-attacks replace common weapons". The correlation between both questions came up to be 0.313 with p = 0.000, the Kaiser-Meyer-Olkin (KMO) coefficient is 0.5, which is satisfactory for factor analysis; moreover, the Bartlett's test gave a chi-squared of 65.399 with p = 0.000. This means that the there exists a correlation between the two questions and that some common grouping exists. The two questions were grouped in one component; thus, producing a reasonably clear factor (Cyber-attacks), where the loadings are 0.810 for both questions.

Similarly, PCA was conducted on items related to awareness on Stuxnet, Duqu and Flame where the bivariate correlations were in excess of 0.305, KMO was 0.626 and the Bartlett's test gave a chi-squared of 245.5 with p = 0.000, which means that the three items do have some common grouping. One factor (Cyber weapons) appeared to represent the three items with loadings 0.793 for Stuxnet, 0.801 for Duqu and 0.680 for Flame.

3.5 Reliability analysis

As is known, reliability refers to the consistency and stability of the findings obtained from the study. The researchers used the Cronbach alpha technique in order to assess the internal reliability of the linked items of the questionnaire. The tertiary scale of question number 12, which contains 11 items related to the familiarity of the respondent with different aspects of cyber-attacks, produced an alpha of 0.863, which is highly acceptable. The inspection of Table 23 suggests that none of the items can be eliminated to improve alpha. Similarly, question 16, which deals with eight measures that are employed to limit cyber-attacks, produced a Cronbach's alpha of 0.855, which is again a highly acceptable value for the tertiary scale considered. Moreover, the study of Table 24 that is related to this question shows that the elimination of any of the items does not improve the internal reliability.

Table 23. Item-total Statistics for familiarity with cyber attacks

Familiar with Cyber Attacks	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Alpha if Item Deleted
Spam, Junk Mail	16.03	12.302	.572	.851
Denial of Service	15.51	11.976	.501	.855
Smurfing	15.45	12.115	.490	.856
Cyber harassment	15.66	11.516	.604	.847
Cyber Pornography	15.70	11.356	.645	.844
Cyber Espionage	15.49	11.733	.573	.850
Phishing	15.43	11.804	.598	.848
Trojan Horse	15.71	11.586	.599	.848
Ping	15.59	11.770	.533	.853
Hacking	16.00	12.268	.535	.853
Pharming	15.37	12.248	.495	.855

Table 24. Item-total Statistics for measures to limit cyber attacks

Measures to Limit Cyber Attacks	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Alpha if Item Deleted
Antivirus	12.74	15.476	.503	.848
Software Firewalls	12.58	14.632	.555	.843
Data Encryption	12.09	13.792	.616	.836
Data Recovery Strategies	12.28	13.716	.627	.834
Training & Awareness	12.26	14.162	.605	.837
Period. Penetration Testing	11.88	14.193	.624	.835
Intrusion Detect/Protect	12.17	13.719	.647	.832
Systems Accountability	11.89	14.151	.601	.837

3.6 Internal validity

Internal validity is the degree to which the results are valid within the confines of the study (p. 426)[31]. To test for internal validity, correlation coefficients between each item scores and the average of all other items scores are calculated. A significant correlation is an indication that the results are valid within the confines of the study. Now, because there have been different arguments related to the application of Pearson's correlation to ordinal data, both Spearman's and Pearson's correlations were calculated, and Tables 25 and 26 show that they are relatively equal with identical significance levels.

Table 25 shows the correlations of the average of the three cyber weapons' assessments against each assessment by itself. All show relatively high significant correlations, which is a positive indication of acceptable internal validity. A similar approach was used to assess the internal validity of the measures utilized by respondents to limit cyber-attacks; again, the significant relatively high correlations shown in Table 26 indicate that internal validity is assured.

Table 25. Correlations between items and their average

		Stuxnet	Duqu	Flame
Average Stuxnet-Duqu-Flame	Spearman Correlation Coefficient	0.615	0.617	0.867
	Pearson Correlation Coefficient	0.694	0.707	0.834
	Sig. (2-tailed)	0.000	0.000	0.000

Table 26. Correlations between items and their average.

Measures to Limit Cyber Attack		Antivirus	Software Firewalls	Data Encryption	Data Recovery Strategies	Training & Awareness	Periodical Penetration	Intrusion Detection/Protec	Systems Accountability
Average of all Measurement items	Spearman Correlation	0.401	0.531	0.731	0.696	0.626	0.737	0.721	0.729
	Pearson Correlation	0.604	0.667	0.728	0.737	0.712	0.724	0.749	0.710
	Sig. (2-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000

Similarly, internal validity is reflected when a relatively high and significant correlation has been identified between the average of the data of questions 13 and 15 respectively: "Cyber-attacks replace common weapons" and "Believing Lebanon will engage in cyber war in the coming 10 years" with the data that corresponds to each of questions 13 and 15. Table 27, demonstrates that these correlations are high and significant; thus, implying acceptable internal validity of the aforementioned items. Further, Table 28 reflects, through the high and significant correlations, the aspects on internal validity that tie questions 9 and 10 being "Lebanese Government should spend to train cyber warriors" and "Believing Lebanon will engage in cyber war in the coming 10 years" respectively.

Table 27. Correlations between items and their average

		Cyber Attacks Replaces Common Weapons	Believing Lebanon Will Engage in Cyber War in Coming 10 Years
Average Questions 13 & 15	Spearman's Correlation	0.798	0.752
	Pearson Correlation	0.797	0.776
	Sig. (2-tailed)	0.000	0.000

Table 28. Correlations between items and their average

		Lebanese Gov. Spending to Train Cyber Warriors	Future Wars are based on Cyber Attacks
Average Questions 9 & 10	Spearman's Correlation	0.820	0.843
	Pearson Correlation	0.837	0.835
	Sig. (2-tailed)	0.000	0.000

It is worth re-emphasizing the fact that in all internal validity tables, Table 25 through Table 28, both Pearsons's and Spearman's correlations are calculated, and the values look to be relatively similar and significant. Jamieson [32] stated clearly, and based on different references, that Likert scales fall within the ordinal level of measurement; thus, Spearman's rho is to be considered. Moreover, in her paper she emphasizes the fact that the responses in Likert scales cannot have equal intervals between the pairs of adjacent responses. An answer to Dr. Jaimeson's article was published by Pell [33] where he concluded that it is acceptable in many cases to consider Likert scales' responses as interval levels of measurement and, thus, use Pearson's correlation (p. 970). The authors of this study do agree that when the sample is sufficiently large, as in the current case, both correlations may work and do produce similar results.

4 CONCLUSIONS AND RECOMMENDATIONS

Are Lebanese students in general and Lebanese graduates in particular ready to assume their leading and executive positions? Are they aware and prepared for the cyber warfare challenges and threats? Well, the results of this study do pose a serious warning to both the public and private sectors. The following facts support the aforementioned statement: 26.5% of the respondents never heard of cyber warfare while the grand majority or 73.5% gained their knowledge of it from the Internet and the news media. 79.7%, 82%, and 65.4% refute having any knowledge pertaining to Stuxnet, Duque, and Flame, respectively. Only 26.9% are aware of Flame. 85.5% of the respondents are most familiar with spam and junk mail, while 22.2% are least familiar with pharming. Respondents' concern as related to cyber- attacks is manifested in disruption of

banking and financial services (35.6%) and disruption of Internet services (31.2%).
In fact, the Lebanese educated community is still not prepared to deal with one of the most serious threats of the century. This research has shown the shortcomings and the poor awareness level that encompasses Lebanon.

Regarding the respondents' belief that Lebanon would engage in a cyber-war something during the next ten years show that only 18.3% agree, although, the current research's findings show the statistical significance of the relationship between "Lebanon's government should spend to train cyber warriors" and "believing Lebanon will engage in cyber-warfare in the next ten years". The researchers' most shocking outcome is manifested in that the grand majority of the sampled 635 educated adults are ignorant of what is going on around the world in relation to cyber-attacks and cyber security.

According to Rid [34] "traditional political violence can maintain trust in institutions and states; violence in cyberspace can only undermine such trust" (p. 82). He also contends that "cyber-attacks can maliciously affect software and business processes, without interfering with physical industrial processes, remaining nonviolent but something still causing greater damage than a traditional assault" (p. 84).

Government, businesses and educational institutions should join efforts to at least start an awareness campaign that may reach all ears in order to get the terms cyber warfare, cyber-attacks, cyber security and cyber weapons into the dictionary of every day words, simply because "the threat of a cyber-attack is ever present and will not go away (p. 87) [34]. The next action is the move by private as well as governmental sectors to activate a well-designed plan to train experts who are able to interfere whenever a cyber-attack may present itself. Rid [34] asserts that the "Pentagon announced that it would boost the staff of its Cyber Command from 900 to 4,900 people, most of whom would focus on offensive operations" (p. 86).

5 ACKNOWLEDGEMENT

The authors would like to acknowledge the constructive criticism and editing performed by Mrs. Henriette Skaff, senior editor at AUST's Publications Department.

6 REFERENCES

[1] RAND. Cyber Warfare, http://www.rand.org/topics/cyber-warfare.html, 2012/11/19.

[2] Oxford Dictionary, http://oxforddictionaries.com, 2013.

[3] Sanger, D. E.: Obama Order Sped Up Wave of Cyberattacks Against Iran. The New York times, June 1 (2012).

[4] Donohue, B.: Air Force Openly Seeking Cyber-Weapons, http://threatpost.com, 2012/8/28.

[5] Francisco, K. B.: Kaspersky Lab Raises Awareness on Cyber Warfare, http://www.hardwarezone.com, 2012/7/12.

[6] Harkov, L.: Anonymous threatens cyber attack on Israeli sites. The Jeruslaem Post, April 10 (2013).

[7] Andress, J., Winterfeld, S.: Cyber Warfare. Elsevier, Waltham, MA: Syngress, 2011.

[8] Oded, Y.: Hackers threaten to 'wipe Israel off Internet map' in massive cyber attack. HAARETZ, April 10 (2013).

[9] Goel, S.: Cyberwarfare: connecting the Dots in Cyber Intelligence". Communications of the ACM,132-140 (2011).

[10] Clarke, R. A., Knake, K. R.: Cyber War. Harper Collins, New York (2010).

[11] Washington, D. W.: ONWARD CYBER SOLDIERS. TIME Magazine, August 21, p. Cover (1995).

[12] Finkle, J.: Researchers say Stuxnet was deployed against Iran in 2007. http://www.reuters.com, 2013/2/26.

[13] Kushner, D.: (2013, March). The Real Story of Stuxnet. http://spectrum.ieee.org, 2013/4/20.

[14] Kaspersky Lab.: Kaspersky Lab Discovers 'Gauss' – A New Complex Cyber-Threat Designed to Monitor Online Banking Accounts, http://www.kaspersky.com, 2012/8/9.

[15] Shah, F.: Indo-Israeli Cyber Warfare against Pakistani nuclear program. Asian Tribune, 12(363) (2009), http://www.asiantribune.com, 2009/9/8.

[16] Brodkin, j.: Government-sponsored cyberattacks on the rise, McAfee says, http://poliquicks.com/2010/02/14/cyber-warfare, 2007/11/29.

[17] Greengard, S.: The New Face of War. Communications of the ACM 53 (12), 20-21 (2010).

[18] Guneev, S.: End of the world as we know it: Kaspersky warns of cyber-terror apocalypse, http://rt.com/news/kaspersky-fears-cyber-pandemic-170/, 2012/6/6/.

[19] Brown, I.: Study: unlikely there will ever be a pure 'cyber war', http://www.ox.ac.uk/media/news_stories/2011/111701.html, 2011/1/17.

[20] Rid, T.: Cyber War Will Not Take Place. The Journal of Strategis Studies,35 (1), 5-32 (2012).

[21] Hadnagy, C.: Social Engineering. Wiley Publishing, Inc., Indianapolis, IN, USA (2011).

[22] Grobler, M., Van Vuuren, J. J., Zaaiman, J.: Evaluating Cyber Security Awareness in South Africa. Proceedings of the 10th European Conference on Information Warfare and Security". Tallinn, Estonia: Institute of Cybernatics at the Tallinn University of Technology, 113-121 (2011).

[23] Dlamini, Z., Modise, M.: Cyber Security Awarenesss Initiatives in South Africa. 7th International conference on Information Warfare and Security. Seattle: Academic Conferences Intrenational (2012).

[24] Loiseau, H., Lemay, L.: Canada's Cyber security Policy: a Tortuous Path Toward a Cyber Security Strategy. In D. Ventre (ed.) Cyber Conflict, Wiley, Hoboken, NJ, 1- 44 (2012).

[25] Ducci, S.: Moving Toward an Italian Cyber defense and Security Strategy. In Ventre, D. (ed.) Cyber Conflict, Wiley, Hoboken, NJ, 165-191 (2012).

[26] Van Niekerk, B., Maharaj, M.: A South African Perspective on Information Warfare and Cyber Warfare. In Ventre, D. (ed.) Cyber Conflict, Wiley, Hoboken, NJ, 279-296 (2012).

[27] Web, D. C.: Echelon and the NSA. In Janczewski, L.J., A. M. Colarik, A.M. (eds.) Cyber warfare and Cyber Terrorism, Information Science Reference, Hershey, PA, 453-468 (2008).

[28] Hejase, A. J., Hejase, H. J. Research Methods: A Practical Approach for Business Students (2nd edition). Masadir Inc., Philadelphia, PA, 58 (2013).

[29] Ayish, M.: Arabs need to turn the page on poor reading habits, http://www.thenational.ae, 2010/11/11.

[30] Hejase, A. J., Hejase, H. J.: Foundations of Management Information systems. Dar Sader, Beirut, Lebanon 279 (2011).

[31] Burns, R.B., Burns, R.A.: Business Research Methods and Statistics Using SPSS. SAGE, London 426 (2008).

[32] Jamieson, S.: Likert scales: how to (ab)use them". Medical Education (38), 1212-1218 (2004).

[33] Pell, G.: Use and misuse of Likert scales. Medical Education (39), 970 (2005).

[34] Rid, T.: Cyberwar and Peace: Hacking Can Reduce Real-World Violence, Foreign Affairs 92(6), 77-87 (2013).