EXTENDING THE DEEP PACKET INSPECTION MODEL TO
THE GCC/MENA REGION

Alfred H. Miller
Higher Colleges of Technology
Box 1626 Fujairah Women’s College, Fujairah, UAE
amiller@hct.ac.ae

ABSTRACT

This study seeks to explore extending the technology acceptance model (DPAM) from a 2011 quantitative study—Modeling Intention to Use Deep Packet Inspection Technology in the United Arab Emirates, to the cyber security practitioner community of the Gulf Cooperation Council (GCC) and greater Middle East North Africa (MENA) Region. Analysis of regression between independent variable model factors of computer self efficacy, attitude toward ICT, perceived usefulness of ecommerce, intention to use ecommerce, societal trust and Internet filtration toward the dependent variable intention to use deep packet inspection, to determine parsimony, using confirmatory factor analysis (CFA), multinomial regression to assess correlation of independent and dependent variables, and assessment of the cross-suitability of DPAM across the MENA/GCC states through a MANOVA assessment. A qualitative component of the instrument enables collection of data about specific hardware and software deployed for deep packet inspection and cyber security systems.

Keywords: Cyber Security, Network Security, Middle East and North Africa (MENA), Gulf Cooperation Council (GCC), Deep Packet Inspection Acceptance Model (DPAM), Deep Packet Inspection (DPI), Cyber Behavior.
INTRODUCTION

Deep packet inspection (DPI) is a cyber security, and data inspection technology solution for dealing with cybercrime. The research is significant given the findings of Matwyshyn, Slaughter-Dafoe, and Paya (2010), that the MENA region’s small and medium business enterprise (SME) sector was inadequately prepared to deal with cybercrime and security threats, such as the Stuxnet malware threat described by Benson (2010), and Sutton (2010).

Security threats and cybercrime are serious problems in the region and jeopardize efforts to establish the region as a hub for international business and trade Mortleman (2009). According to the report of El-Guindy (2012), and the Microsoft Threat Assessment (2012) of the 4th Quarter of 2011, the Middle East and North Africa Region suffers from a much higher Worms, Viruses, Trojans, and Adware malware infection rate than the rest of the world (Microsoft, 2012). A case in point is Egypt, statistically the worst country in the region where malware infections were three times the global average. The top three offenders were viruses infecting 38.3% of machines cleaned with the Microsoft Malicious Software Removal Tool, followed by miscellaneous potentially unwanted software which infected 37.8%, and worms, which had infected 35.8%, of computers (Microsoft, 2012).

Greater deployment of deep packet inspection (DPI), a technical solution used to intercept, analyze, and block network traffic, is recommended. Deep packet inspection identifies and protects against security threats—including worms, viruses, and hacking attacks—that can create extensive security, financial, and logistical problems for governmental entities and businesses. However, using DPI is controversial because it enables governments and other users to spy on individuals and organizations, having triggered legal proceedings in Western societies (Epic.org, 2009; Hanff, 2008, 2009; Jones, 2009; Lawson, 2008). The main commercial uses for DPI include managing network traffic flow, ensuring quality of service, and conducting targeted behavioral advertising in which DPI is employed surreptitiously to acquire marketing data, and build a profile about each individual customer, (Center for Democracy and Technology, 2008; Nakashima & Lebling, 2008).

BACKGROUND OF RESEARCH

From 2009 to 2011, using a series of field studies and two rounds of pilot tests, Miller (2012) validated 24 survey questions, from which the deep packet inspection acceptance model (DPAM) was developed for the UAE. Miller (2012), began with 66 questions, 51
questions from Siddiqui’s (2008) ecommerce acceptance study comparing Saudi Arabia and the UAE, with questions drawn from previously validated instruments, plus 15 additional questions based on findings by the private research group the Open Net Initiative (2009) and upon UAE-based Etisalat’s (2009) (the region’s largest telecom operator), published Internet filtration regimen. For all questions used from the Siddiqui instrument, permission for use was gained from both Siddiqui and the seminal author or representative (Miller, 2012).

Sampling Method
The identified population (i.e., sampling frame) for the purposively selected random sample was the enrolled college students of the HCT campuses of the UAE. The total possible sampling frame consisted of N ≈ 19,370 students, all of whom were Emirati nationals. Participants in the sampling frame tended to be between the ages of 18 and 25. The gender ratio was skewed system wide 65% to 35% in favor of women at Higher Colleges of Technology (Miller, 2012). The 16 campuses selected for possible participation in the study had full-time student populations. Geographic-based area sampling ensured the efficient sampling of the widely dispersed UAE college system. Stratified random sampling, assured representation of at least one campus of each size category in the study, and that the smaller campuses were not under-represented in the test population. A deficiency of the sampling methodology was that while students were targeted by UAE employment law for placement in industries likely to utilize DPI, actual security practitioners were not sampled (Miller, 2012).

Results
The outcomes by Miller (2011, 2012) to develop the instrument can be described as follows: “a questionnaire study of six variables using randomly sampled data of n = 443, was collected from 18-to-25-year-old Emirati national college students, at the Higher Colleges of Technology—graduates targeted by UAE law, for employment in the finance and telecommunications sectors—industries likely to use DPI. Quasi-experimentally tested data, using the maximum likelihood estimator—robust to non-normality, using confirmatory factor analysis, suggested an acceptable goodness-of-fit into the deep packet acceptance model (DPAM). Reliability assessed using Cronbach’s α was > .80 for all constructs (Miller, 2012). See Table 1 below. Individual constructs were not univariate-normally distributed. See Table 2 below.
Table 1 Reliability Statistics for Instruments

| Constructs                                           | Questions | Number of questions | Cronbach’s α |
|------------------------------------------------------|-----------|---------------------|--------------|
| Computer self-efficacy (CSE)                         | 1-4       | 4                   | 0.872        |
| Attitude toward information and communications technology (ATICT) | 5-8       | 4                   | 0.813        |
| Perceived usefulness of e-commerce (PUEC)            | 8-12      | 4                   | 0.859        |
| Intention to use e-commerce (IUEC)                   | 13-16     | 4                   | 0.875        |
| Societal Trust                                      | 17, 19, 20| 3                   | 0.829        |
| Internet filtration (IF)                             | 18, 21-24 | 5                   | 0.832        |

Table 2 Tests for Univariate Normality

| Constructs                                           | Kolmogorov-Smirnova | Shapiro-Wilk |
|------------------------------------------------------|----------------------|--------------|
|                                                       | statistic df Sig.    | statistic df Sig. |
| Computer self-efficacy (CSE)                         | 0.251 443 ***        | 0.808 443 ***  |
| Attitude toward information and communications technology (ATICT) | 0.260 443 ***        | 0.834 443 ***  |
| Perceived usefulness of e-commerce (PUEC)            | 0.267 443 ***        | 0.857 443 ***  |
| Intention to use e-commerce (IUEC)                   | 0.259 443 ***        | 0.881 443 ***  |
| Societal trust (ST)                                  | 0.232 443 ***        | 0.890 443 ***  |
| Internet filtration (IF)                             | 0.271 443 ***        | 0.784 443 ***  |

Note: *α*. Lillefors significance correction, *** = p-value less than 0.001.

Individual factor loadings ranged from .621 to .885, while construct averages were .792 for computer self-efficacy (CSE), .707 for attitudes toward information and communications technology (ATICT), .770 for perceived usefulness of e-commerce (PUEC), .800 for intention to use e-commerce (IUEC), .781 for societal trust (ST), and .711 for Internet filtration (IF). The goodness-of-fit values obtained were; Normed Chi-Square, ($\chi^2/df$) = 2.602, Comparative fit index, (CFI) = 0.918, Tucker-Lewis index, (TLI) = 0.905, and Root mean square error of approximation, (RMSEA) = 0.060. Significant positive correlation existed between CSE, ATICT, PUEC, and IUEC—highest being CSE and ATICT at $r = 0.537$ and a significant negative correlation between PUEC and IF ($r = -0.137$). Societal trust and CSE, CSE and IF, and IF and ST, were not significantly correlated” (Miller, 2011, 2012). See Table 3 and Table 4 on the next page for respective correlations using EFA and CFA factor loadings. The multivariate distribution
was non-normal according to Srivastava’s test, \( \chi^2 (24) = 178.58, p < 0.001 \), and Mardia’s test \( b_2 p = 18.66, p < 0.001 \).

### Table 3 Primary Data Maximum Likelihood EFA

| Component of constructs | F1   | F2   | F3   | F4   | F5   | F6   |
|-------------------------|------|------|------|------|------|------|
| CSE1                    | 0.020| 0.101| 0.786| 0.083| 0.133| 0.072|
| CSE2                    | -0.048| 0.006| 0.695| 0.133| 0.306| 0.010|
| CSE3                    | -0.079| 0.002| 0.740| 0.125| 0.232| 0.043|
| CSE4                    | -0.001| 0.116| 0.828| 0.074| 0.100| -0.087|
| ATICT1                  | 0.000| 0.254| 0.154| 0.075| 0.647| 0.103|
| ATICT 2                 | -0.022| 0.142| 0.235| 0.126| 0.659| -0.071|
| ATICT 3                 | 0.160| 0.104| 0.263| 0.263| 0.603| 0.081|
| ATICT 4                 | 0.126| 0.102| 0.163| 0.150| 0.661| 0.030|
| PUEC1                   | -0.155| 0.031| 0.073| 0.741| 0.216| 0.061|
| PUEC2                   | -0.062| 0.124| 0.127| 0.586| 0.217| 0.196|
| PUEC3                   | 0.014| 0.096| 0.151| 0.859| 0.065| -0.040|
| PUEC4                   | -0.071| 0.110| 0.064| 0.780| 0.072| 0.015|
| IUEC1                   | 0.126| 0.716| 0.065| 0.076| 0.177| -0.020|
| IUEC2                   | 0.114| 0.792| 0.053| 0.130| 0.188| 0.077|
| IUEC3                   | 0.062| 0.797| 0.030| 0.091| 0.105| 0.104|
| IUEC4                   | 0.103| 0.764| 0.084| 0.059| 0.067| 0.174|
| ST1                     | 0.016| 0.149| 0.021| 0.050| 0.049| 0.676|
| ST2                     | -0.028| 0.056| 0.041| 0.041| 0.003| 0.772|
| ST3                     | -0.002| 0.057| -0.042| 0.063| 0.040| 0.872|
| IF1                     | 0.654| 0.116| -0.021| 0.002| 0.042| 0.020|
| IF2                     | 0.611| 0.068| -0.029| -0.052| -0.036| -0.049|
| IF3                     | 0.644| 0.001| -0.047| -0.032| 0.097| 0.102|
| IF4                     | 0.706| 0.135| 0.002| -0.081| 0.129| -0.013|
| IF5                     | 0.907| 0.044| 0.032| -0.073| -0.046| -0.091|

Note: Factor loadings > 0.5 are in boldface, extraction method: Maximum likelihood, 6 factors extracted, 5 iterations required.

**Conclusions**

From late 2009 through December of 2011 a large quasi-experimental study on acceptance of deep packet inspection was conducted at the UAE’s largest university, the Higher Colleges of Technology (Miller, 2011, 2012). While there were marginal model-fit indices for TLI and CFI measures, RMSEA, and \( \chi^2/df \), results indicated a good model fit, and this was coupled with meaningful factor loadings and correlation coefficients among latent variables. The PASW-18 and MPLUS 5.0 measurement sub-model indicated a
rejection of the null-hypothesis in favor of default acceptance of the alternate hypothesis, for all six research questions. There was a positive relationship between each of the six independent variables (i.e., CSE, ATICT, PUEC, IUEC, ST, and IF) and the dependent variable intention to use deep packet inspection. Culture and not sampling actual cyber security practitioners were limitations of the study (Miller, 2012). See Table 5 below for a summary of fit indices.

| Table 4 CFA Factor Loadings |
|-----------------------------|
| Item | Estimate | Std. Error | Est./Std. Error | P-Value |
| CSE  |          |            |                |         |
| CSE1 | 0.790    | 0.026      | 30.22           | <0.001  |
| CSE2 | 0.774    | 0.029      | 26.586          | <0.001  |
| CSE3 | 0.800    | 0.021      | 38.617          | <0.001  |
| CSE4 | 0.807    | 0.024      | 33.096          | <0.001  |
| ATICT|          |            |                |         |
| ATICT1| 0.672   | 0.032      | 20.791          | <0.001  |
| ATICT2| 0.705   | 0.03       | 23.728          | <0.001  |
| ATICT3| 0.748   | 0.037      | 20.087          | <0.001  |
| ATICT4| 0.703   | 0.033      | 21.607          | <0.001  |
| PUEC |          |            |                |         |
| PUEC1| 0.782    | 0.027      | 29.161          | <0.001  |
| PUEC2| 0.657    | 0.036      | 18.349          | <0.001  |
| PUEC3| 0.842    | 0.022      | 38.891          | <0.001  |
| PUEC4| 0.799    | 0.025      | 31.673          | <0.001  |
| IUEC |          |            |                |         |
| IUEC1| 0.746    | 0.027      | 28.024          | <0.001  |
| IUEC2| 0.841    | 0.021      | 40.308          | <0.001  |
| IUEC3| 0.812    | 0.026      | 31.482          | <0.001  |
| IUEC4| 0.783    | 0.026      | 29.852          | <0.001  |
| Societal Trust | | | | |
| ST1  | 0.696    | 0.036      | 19.428          | <0.001  |
| ST2  | 0.789    | 0.031      | 25.588          | <0.001  |
| ST3  | 0.859    | 0.032      | 27.202          | <0.001  |
| IF   |          |            |                |         |
| IF1  | 0.666    | 0.039      | 17.29           | <0.001  |
| IF2  | 0.621    | 0.036      | 17.333          | <0.001  |
| IF3  | 0.647    | 0.035      | 18.462          | <0.001  |
| IF4  | 0.736    | 0.031      | 23.649          | <0.001  |
| IF5  | 0.885    | 0.02       | 44.562          | <0.001  |
Table 5 Evaluation of Fit of DPAM

| Goodness-of-fit index | Threshold value | Results obtained |
|-----------------------|-----------------|------------------|
| $\chi^2/df$           | 3.000           | 2.602            |
| TLI                   | 0.90-0.950*     | 0.905            |
| CFI                   | 0.90-0.950*     | 0.918            |
| RMSEA                 | 0.080           | 0.060            |

Note. *Values for TLI and CFI within the range of 0.90-0.95 may be indicative of acceptable model fit. From Brown (2006) p. 87, and Kline (2011) p. 204-208.

Implications

While this study was successful in building understanding of this important cybercrime phenomenon in the UAE through a student-based study, further refinement of the proposed model and replication of the study in the UAE, and other countries of the region, should take place. Further research on network security technologies, including impact of culture should be encouraged for the UAE and the Arab World to examine factors that affect DPI’s acceptance for GCC/MENA countries. Furthermore, participants in the study should be requested to volunteer individual knowledge of DPIs implementation in their workplace, and to name if a particular hardware or software was being used (Yu, 2007). D. Saral has recommended further analysis of data using regression to determine if multicollinearity could account for a simpler model with less variable constructs (Saral, DBA and e-MBA Programs Director, Webster University, personal communication, November 25, 2011).

HYPOTHESES

Research Questions

Q1: To what extent, if any, does the deep packet acceptance model apply to the UAE/GCC/MENA cyber security practitioner community?

Statement of Hypotheses

H10: The deep packet acceptance model does not apply to the UAE/GCC/MENA cyber security community.

H1a: The deep packet acceptance model does apply to the UAE/GCC/MENA cyber security community.
For the MENA study, the twenty-four questions validated by Miller (2012) and targeted toward the six DPI constructs are augmented by three additional questions. First, a question from the earlier study is repeated and engages the respondent to state if they are under 18 years old, or older, and one question requests the country in which they are currently residing. The final question is new and asks the respondent if they know or believe that deep packet inspection is being used in their workplace, and the respondent is prompted to give the name/brand or security application being used. The instrument is presented as an online survey via Smart-Survey at http://biga.us.

Computer Self-Efficacy

The first independent variable (X1) CSE, is represented by Likert-type ordinal-based scaled data, operationally defined by four survey questions, and measure one’s proficiency with computer technology. A summation of ratings (i.e. responses) for four questions, shown below in Table 6, was calculated and averaged to yield a single average score for CSE, with Strongly agree valued at 5, Agree at 4, Not sure at 3, Disagree at 2, and Strongly disagree at a value of 1 point. Except where noted for reverse scored items, the scoring
scheme was maintained for all variables.

**Table 6 Questions for Measuring Computer Self-Efficacy**

| Item          | Question                                                                 |
|---------------|---------------------------------------------------------------------------|
| Question 1    | I use the Internet for chatting with ease.                                |
| Question 2    | I can get the information from a website easily for my work.             |
|               | I am confident that I can obtain relevant information through online     |
| Question 3    | sources (e.g. online discussion groups, reputation sites, etc) on the web|
|               | vendors if I am planning to purchase an item online.                     |
| Question 4    | I prefer the sites that have chat room to see what others say about the  |
|               | product and service.                                                    |

Note: Adapted from Siddiqui (2008) who adapted Question 1 from Thompson, Compeau, and Higgins (2006), and Questions 2-4 from Kim, Kim, and Hwang (2009).

**Attitude toward ICT**

The second independent variable (X2) attitude toward ICT, (AICT) is represented by Likert-type scaled ordinal-level response data. Four items operationally define variable X2 and measure one’s attitude toward Information and communications technology. These are shown in Table 7. A summation of all ratings for the four questions relevant to this construct was calculated and averaged to yield a single average score for attitudes toward ICT.

**Table 7 Questions for Measuring Attitude toward ICT**

| Item          | Question                                                                 |
|---------------|---------------------------------------------------------------------------|
| Question 5    | Learning to use the Web for purchasing products or services is easy for   |
|               | me.                                                                       |
| Question 6    | I believe that it is easy to get the Web to do what I want it to do.     |
| Question 7    | My life is better because of the Internet.                                |
| Question 8    | The Web should be accessible just like mail and electricity.             |

Note: Adapted from Siddiqui (2008) who adapted Questions 5-7, from Van Slyke, Lou, Belanger, and Sridhar (2010), and Question 8, from Sagi, Carayannis, Dasgupta, and Thomas (2004).

**Perceived Usefulness of E-commerce**

Four Likert-type scaled interval-level survey response items represent perceived usefulness of e-commerce (PUEC) as independent variable (X3). These are shown in Table 8. A summated total of the ratings for all four questions relevant to this construct were calculated and averaged to yield a single average score for attitudes toward PUEC. Like all
of the independent variables prescribed for this study, data collection was for comparative testing purposes using statistical correlation. Question 12 was a reverse scored inverted response question, used to test testing reliability of the instrument.

### Table 8 Questions for Measuring Perceived Usefulness of E-Commerce

| Item       | Question                                                                 |
|------------|---------------------------------------------------------------------------|
| Question 9 | I expect cheaper prices on the web.                                       |
| Question 10| Using the Web would help me to make a better decision.                    |
| Question 11| Using the Web would help me to buy product I really want.                 |
| Question 12| I believe I will not be able to find a good deal when using the Web for purchase. |

Note: Adapted from Siddiqui (2008) who adapted Question 9-12 from Xu and Cai (2004), originally sourced from Childers, Carr, Peck, and Carson (2001).

### Intention to Use E-commerce

The fourth independent variable (X4), intention to use e-commerce (IUEC), was represented by Likert-type scaled ordinal-level response data and is operationally defined by questions 13 through 16. These are shown in Table 9. This part was the operationalization of the measurement of intention to use e-commerce as an independent variable. An average score for IUEC was obtained by computing the aggregated score for these four items and dividing by four. Question 15 was a reverse scored inverted response question. It was in the survey as a tool used to test reliability of the instrument.

### Table 9 Questions for Measuring Intention to Use E-Commerce

| Item       | Question                                                                 |
|------------|---------------------------------------------------------------------------|
| Question 13| I would pay to download information if it saves me time.                  |
| Question 14| I believe Internet will make my shopping more efficient.                  |
| Question 15| Although I will likely use information from the Web quite extensively, I don’t see myself directly using Web purchasing in the future. |
| Question 16| I expect that I will use Web purchasing quite extensively in the future.  |

Note: Adapted from Siddiqui (2008) who adapted Question 13-14 Van Slyke, Lou, Belanger, and Sridhar (2010), and Questions 15-16 from Thompson, Compeau, and Higgins (2006).

### Societal Trust

Societal trust (X5) was represented by three Likert-type scaled response data items, and was operationally defined by questions 17, 19, and 20. These are shown in Table 10. As with the other variable response measurement items, the aggregated total score was
averaged by dividing using on the number of items, to yield a value that represented the score or value for that particular construct. Question number 19 was a negatively worded question, where the scoring needed to be inverted, and added to the aggregated score, before being divided by three, to yield the average value for this construct. Question 18, A nation should be able to control the web content that crosses its border, was originally a societal trust question. However Question 18 loaded onto Internet filtration, instead of societal trust, and was shifted to the Internet filtration construct.

### Table 10 Questions for Measuring Societal Trust

| Item     | Question                                                                 |
|----------|--------------------------------------------------------------------------|
| Question 17 | The government should not stop any product that is legal and is paid for on the Internet from coming in to the country. |
| Question 18 | I am not living in a high trust society.                                  |
| Question 19 | My friends are generally trustworthy.                                    |

Note: Adapted from Siddiqui (2008) who adapted Question 17 from Sagi, Carayannis, Dasgupta, and Thomas (2004), and Question 19-20 from Gefen (2000).

### Internet Filtration

Internet filtration (X6) was represented operationally by five Likert-type scaled, ordinal-level response format questions that the respondent answered about his or her feelings about how necessary they thought it was to filter Internet content. The questions pertaining to Internet filtration were survey items 18, and 21 through 24, and are shown in Table 11. Question 18, originally assigned to the societal trust construct, loaded onto Internet filtration in pilot testing. In addition to the empirical support, a reconsideration of face validity of the question, performed in the context of a focus group, supported shifting the question to internet filtration. Question 18, A nation should be able to control the web content that crosses its border, was removed from the societal trust construct, and aligned instead with IF. The average for the Internet filtration construct, equaled the aggregated total, of five items, divided by five.
Table 11 Questions for Measuring Internet Filtration

| Item    | Question                                                                 |
|---------|--------------------------------------------------------------------------|
| Question 20 | A nation should be able to control the web content that crosses its borders. |
| Question 21 | Blogging sites should be blocked.                                         |
| Question 22 | Content that insults any recognized religion should be blocked.           |
| Question 23 | Terrorism content should be blocked.                                      |
| Question 24 | Top Level Domain for Israel (.il) should be blocked.                      |

Note: Adapted from Siddiqui (2008), who adapted Question 18 from Sagi, Carayannis, Dasgupta, and Thomas (2004), and Question 21-24 which was adapted from Etisalat (2009) and ONI (2009).

Intention to Use DPI

The dependent variable (Y) is a latent variable that measures the propensity of the targeted group (security practitioners) to use DPI technology. Intention to use DPI is measured operationally by the correlations of the set of variables identified in the model shown in Figure 1 that were thought to influence intention to use DPI. Questions about CSE (items one through four), attitudes towards ICT (questions five through eight), PUEC (items nine through 12), intention to use e-commerce (items 13 through 16), societal trust (items 17, 19, and 20), and feelings about Internet content filtration (items 18, 21 through 24) are compared to the respondent response to a Likert-type, scaled response question to obtain ordinal-level type data. This type of data is suitable for a factor analysis used to determine the goodness-of-fit of the proposed model to predict any intention to use DPI, (Boomsma, 2000; Brown, 2006; Pham & Jordan, 2009). Table 12 shows the scoring method applied to Question 25.

Table 12 Question for Intention to Use Deep Packet Inspection

| Item    | Question                                           |
|---------|----------------------------------------------------|
| Question 25 | Use of Deep Packet Inspection at my workplace.   |
| Score   | 5        4        3        2        1        |
| Reply   | Already use Would like to use Not sure Prefer not to use Will not use |

Note: Respondents were also asked to write in a comment this follow-up question: “If you know the brand of the DPI application, or its trade name and are willing to share please place it in the comment box. For example your firm may use Network User Behavior Analysis Securify Monitor by McAfee or an application by Nortel Security Lab.” (see http://biga.us in Miller, 2012).
SAMPLING STRATEGY

The proposed sampling strategy utilized to reach cyber security practitioners is purposive sampling via Web-based and email advertising. Respondents are directed to complete the online survey at http://biga.us. Cyber security practitioners in the MENA Region are potentially a difficult group to reach and a snowball approach is warranted for leads showing interest in the research topic.

Proposed methods include:

- Distribution via the Smart-Survey Website; a mass email campaign targeting the MENA region of approximately 219,000 addresses purchased from an e-commerce trading company based in India. Alternatively another option is to use the 298,000 addresses available from, http://www.reachgulfbusiness.com/middle_east/index.htm
- The business leads pack available at http://www.targetgulf.com/cgi-bin/purchase.asp has 100,000 trade leads from the Middle East, including Bahrain, Egypt, Iran, Jordan, Kuwait, Lebanon, Oman, Qatar, Saudi Arab, Syria, Yemen and United Arab Emirates-UAE.
- Adknowledge Inc.’s Bid System; targetable pay-per-click advertising
- LinkedInAds; targeting based on job function, geographic, and age factors utilizing a pay for click bid system, with lead generation and click-through-rate optimization.
- Regional targeting of cyber-professional through LinkedIn connections and groups.
- MENA Targeted Google Adwords.
- AlJazeera.net, via http://www.netadvantage.net/; a per-impression scheme
- Free advertising targeting the MENA audience, such as sooq.palmoon.net.

DATA ANALYSIS

The DPAM practitioner data shall be analyzed along three tangents; first, correlation by confirmatory factor analysis using the maximum likelihood estimator (MLM), robust to non-normality, and appropriate for ordinal-level data (Brown, 2006). Second, using multinominal logistic regression, with respondent reported opinion of DPI use at their workplace, as the dependent variable (DV), and the six factors from DPAM as independent variables (IVs); determine if correlation exists between variables and assess if multicollinearity exists, allowing for a simpler model with less variable constructs (Zhang, 2009). Finally, each variable in the model will be tested quasi-experimentally within framework using, regression-based MANOVA, to test for individual country-alignment
within DPAM. A power analysis with G-Power 3.1 for six countries from the Gulf Cooperation Council, using the protocol in Table 13, and procedure illustrated in Figures 2 and 3, revealed a minimum of 20 samples required per country for MANOVA (Zhang, 2009).

### Table 13 Protocol of Power Analysis

| F tests - MANOVA: Repeated measures, within-between interaction | Options                          | Analysis | A priori: Compute required sample size |
|---------------------------------------------------------------|----------------------------------|----------|---------------------------------------|
| Options                                                      | Pillai V, O’Brien-Shieh Algorithm | Input    | Effect size f(V) = 0.20                |
|                                                              |                                  | α err prob = 0.05                         |
|                                                              |                                  | Power (1-β err prob) = 0.80               |
|                                                              |                                  | Number of groups = 6                      |
|                                                              |                                  | Number of measurements = 6                |
| Output                                                       | Noncentrality parameter $\lambda$ | = 23.8000000                             |
|                                                              | Critical F                       | = 1.5256186                               |
|                                                              | Numerator df                     | = 25.0000000                              |
|                                                              | Denominator df                   | = 565                                      |
|                                                              | Total sample size                | = 119                                      |
|                                                              | Actual power                     | = 0.8042870                               |
|                                                              | Pillai V                         | = 0.1923077                               |

Note: From G*Power 3.1.2 Faul, Erdfelder, Lang, and Buchner (2007); small-medium effect size as per Cohen (1992).

![Figure 2 Distributions Plot of Power Analysis. From G*Power 3.1.2 Faul, Erdfelder, Lang, and Buchner (2007).](image-url)
Assessment Grid for Gulf Cooperation Council States

| Independent variables | Bahrain | Kuwait | Oman | Qatar | Saudi Arabia | UAE |
|-----------------------|---------|--------|------|-------|--------------|-----|
| Computer self-efficacy |         |        |      |       |              |     |
| Attitudes toward ICT  |         |        |      |       |              |     |
| Perceived usefulness of e-commerce |   |        |      |       |              |     |
| Intention to use-commerce |   |        |      |       |              |     |
| Societal Trust        |         |        |      |       |              |     |
| Internet filtration   |         |        |      |       |              |     |

Figure 3 Conceptual Construct Model: Relationship Matrix for MANOVA to Test DPAM, see Field (2009).

Furthermore, to strengthen the analysis, the Satorra-Bentler Scaled $\chi^2$ test statistic corrects for non-normality in the data (Brown, 2006). The ordinal-type data is compatible with CFA, used to evaluate the model in the SPSS and MPlus statistics software platforms, and based upon the LISREL method, see Brown (2006), Field (2009), Garson (2009), Jackson (2000), Schermelleh-Engel, Moosbrugger, and Müller (2003), and Trochim and Donnelly (2008). The Kolmogorov-Smirnov (K-S) and Shapiro-Wilk (S-W) tests of univariate normality are proposed to determine if the distribution is deviated significantly from a comparable normal distribution. The sample is significantly different if $p < .05$, and not significantly different from a normal distribution if the computed value of $p > .05$. The K-S and S-W tests are sensitive to large sample sizes; significant results with small deviations from normality, should be interpreted in conjunction with histograms, scatterplots, and Q-Q plots to check for skew, kurtosis, and outliers (DeCarlo, 1997a; Field 2009; Kline 2011). Both Mardia’s test and Srivastava’s test are suitable for analysis of multivariate normality, see DeCarlo (1997b), Enomoto, Okamoto and Seo (2010), Mardia (1974), Mardia and Foster (1983), Okamoto and Seo (2008), Srivastava (1984), and
Srivastava and Hui (1987).

The use of MLM, a goodness-of-fit modeling technique robust to non-normality, is proposed as appropriate for ordinal data analysis and for interval data assessed by default as ordinal Brown (2006) to generate a solution likely to produce the correlation matrix observed in the data (Zhang, 2009). Sample size is critical with MLM, via statistical power calculation and requires $n \geq 400$, for a robust statistical measurement; see Schermelleh-Engel et al. (2003).

A regression analysis establishes discriminant and convergent validity by comparing correlation results among similarly tested variables. Discriminant validity refers to the degree of difference contained in the measures of different latent variables, while convergent validity is the degree of sameness for variables that should have some correlation (Benson & Selen, 2009). Evaluation of DPAM includes an assessment of both discriminant and convergent validity.

CONCLUSION

The study which produced the Deep Packet Acceptance Model (DPAM) used United Arab Emirate (UAE) National students. These participants were proficient with modern technology, and from the Higher Colleges of Technology, the nation’s largest university. The school is a government university, and graduates are mandated through legislation, as being likely to gain employment in decision making positions in key UAE industries, which would be those likely to use DPI. However, to build credibility, DPAM should be replicated with data collected from cyber security practitioners with actual work experience in the field. By collecting data to define application of deep packet inspection in the workplace, from UAE, GCC and MENA Region cyber security practitioners, the real-world validity of DPAM as a predictor of deep packet acceptance, a cyber security technology can be assessed.

In addition to the technology acceptance related factors, of CSE, attitude toward ICT, perceived usefulness of e-commerce, intention to use e-commerce; societal trust and Internet filtration are assessed though cultural measurements and included in the model. Furthermore, an open ended question at the end of the survey allows cyber security practitioners to specify if particular hardware or software is being used such as F5’s (2012), Local Traffic Manager (LTM) and Global Traffic Manager (GTM) switches, or the Network User Behavior Analysis Securify Monitor by McAfee (2009). A better understanding of intention to use DPI could enable a multitude of stakeholders to promote
DPI, as technology to support firewalls through an effective analysis of e-business, cyber security, and user privacy concerns, and identify, through further applied research, what content and applications fit the market needs of the MENA/GCC.

REFERENCES
Agarwal, R., & Selen, W. (2009). Dynamic capability building in service value networks for achieving service innovation. Decision Sciences, 40(3), 431-475. http://dx.doi.org/10.1111/j.1540-5915.2009.00236.x
Benson, P. (2010, November 18). Computer virus Stuxnet a ‘game changer,’ DHS official tells Senate. CNN Tech. Retrieved September 28, 2013, from http://www.cnn.com/2010/TECH/web/11/17/stuxnet.virus/index.html.
Boomsma, A. (2000). Reporting analyses of covariance structures. Structural Equation Modeling, 7(3), 461-483. http://dx.doi.org/10.1207/S15328007SEM0703_6
Brown, T. A. (2006). Confirmatory Factor Analysis for Applied Research. New York, NY: The Guilford Press.
Childers, T.L., Carr C.L., Peck J., & Carson, S. (2001). Hedonic and utilitarian motivations for online retail shopping behaviour. Journal of Retailing, 77(4), 511-535. http://dx.doi.org/10.1016/S0022-4359(01)00056-2
Cohen, J. (1992). Quantitative methods in psychology: A power primer. American Psychological Association, Psychological Bulletin, 112(1), 155-159. http://dx.doi.org/10.1037/0033-2909.112.1.155
Cronbach, L.J. (1951). Coefficient alpha and the internal structure of tests. Psychometrika, 16(3), 297-334. http://dx.doi.org/10.1007/BF02310555
DeCarlo, L.T. (1997a). On the meaning and use of kurtosis. Psychological Methods, 2(3), 292-307. http://dx.doi.org/10.1037//1082-989X.2.3.292
DeCarlo, L.T. (1997b). Univariate and multivariate tests of skew and kurtosis, a list of the 5 cases with the largest Mahalanobis distances, a plot of the squared distances, critical values for a single multivariate outlier. [SPSS Macro] Retrieved September 28, 2013, from http://www.columbia.edu/~ld208/normtest.sps.
El-Guindy, M.N. (2012). Middle east among most malware infected nations. Netsafe. middle east; Cybersafety and cybersecurity in the middle east. Retrieved September 28, 2013, from http://netsafe.me/2012/03/11/middle-east-among-most-malware-infected-nations/.
Enomoto, R., Okamoto, N. & Seo, T. (2010). On the distribution of test statistic using Srivastava's skewness and kurtosis. *Journal of Statistical Planning and Inference, 140*(10), 2809-2816. http://dx.doi.org/10.1016/j.jspi.2010.03.003

Epic.org. (2009). *Deep packet inspection and privacy*. Retrieved September 28, 2013, from http://epic.org/privacy/dpi/.

Etisalat. (2009). *Blocked content*. Retrieved September 28, 13, from http://www.yumpu.com/en/document/view/12353774/prohibited-content-categories-etisalat

F5 (2012). *BIG-IP® Local traffic manager*. Retrieved September 28, 2013, from http://www.f5.com/products/big-ip/big-ip-local-traffic-manager/overview.

Faul, F., Erdfelder, E., Lang, A.G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. *Behavior Research Methods, 39*(2), 175-191. http://dx.doi.org/10.3758/BF03193146

Field, A. (2009). *Discovering Statistics Using SPSS* (3rd ed.). London, England: Sage Publications.

Garson, D.G. (2009). *Structural equation modeling: Statnotes*. Retrieved September 28, 2013, from http://www.statisticalassociates.com/sem.htm.

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *The International Journal of Management Science, 28*(6), 725-737. http://dx.doi.org/10.1016/S0305-0483(00)00021-9

Hanff, A. (2008). A critical evaluation of the 2006/2007 trials of Phorm Inc. Technology by BT PLC. *No deep packet inspection*. Retrieved September 13, 2013, from https://nodpi.org/documents/phorm_paper.pdf.

Hanff, A. (2009, December 31). *No deep packet inspection – A Review 2009* [Web log post]. Retrieved September 13, 2013, from https://nodpi.org/2009/12/.

Harris, L., Sohn, D., Morris, J., Cooper, A., (2008). Keeping the Internet open innovative and free. *CDT: Center for Democracy & Technology*. Retrieved September 28, 2013, from http://cdt.org/speech/20080213_FCC_comments.pdf.

Jackson, G. B. (2000). Assessing the methodology of the study. *Tools for preparing a literature review*. Retrieved September 28, 2013, from http://www.gwu.edu/~litrev/a06.html.

Jones, B. (2008). *Deep packet inspection and your privacy online*. Retrieved September 28, 2013, from http://torrentfreak.com/deep-packet-inspection-080629/.
Kim, Y.H., Kim, D.J., & Hwang, Y. (2009). Exploring online transaction self-efficacy in trust-building in B2C electronic commerce. *Journal of Organizational and End User Computing, 21*(1), 37-59. http://dx.doi.org/10.4018/joeuc.2009010102

Kline, R.B. (2011). *Principles and Practice of Structural Equation Modeling* (3rd ed.). New York, NY: The Guilford Press.

Lawson, P. (2008). Re: Bell Canada/Bell Sympatico use of deep packet inspection: PIPEDA complaint. *Canadian internet policy and public interest clinic*. Retrieved September 28, 2013, from http://www.cippic.ca/uploads/Bell-DPI-PIPEDAcomplaint_09May08.pdf.

Mardia, K.V. (1974). Applications of some measures of multivariate skewness and kurtosis in testing normality and robustness studies. *Sankhya, Series B, 36*(2), 115-128. Retrieved September 28, 2013, from http://www.jstor.org/stable/25051892.

Mardia, K.V., & Foster, K. (1983). Omnibus tests of multinormality based on skewness and kurtosis. *Communications in Statistics: Theory and Methods, 12*(2), 207-221. http://dx.doi.org/10.1080/03610928308828452

Matwyshyn, A.M., Slaughter-Defoe, D., & Paya, C. (2010, March 18). *Information security: Why cybercriminals are smiling*. Arabic *Knowledge@Wharton*. Retrieved September 28, 2013, from http://knowledge.wharton.upenn.edu/article/information-security-why-cybercriminals-are-smiling/.

McAfee Inc. (2009). *McAfee network user behavior analysis (Securify) monitor*. Retrieved September 28, 2013, from http://www.mcafee.com/us/resources/data-sheets/ds-network-user-behavior-analysis.pdf.

Microsoft (2012). *MicroSoft security intelligence report: Regional threat assessment*. Retrieved September 28, 2013, from http://www.microsoft.com/security/sir/threat/#!introduction.

Miller, A.H. (2011, December). Network security research: Deep packet inspection acceptance in the United Arab Emirates. *Paper presented at International Conference on Computer Science and Information Technology (ICCSIT’2011): International Conference on Latest Trends in Engineering & Technology (ICLTET’2011)*, Pattaya, Thailand. Retrieved September 28, 2013, from http://psrcentre.org/images/extrainages/1211292.pdf.
Miller, A.H. (2012). *Modeling intention to use deep packet inspection in the United Arab Emirates* (Doctoral Dissertation). Northcentral University, Prescott Valley Arizona. Retrieved September 28, 2013, from http://disexpess.umi.com/dxweb#download?type=pdf&dpubno=3492475.

Mortleman, J. (2009, August 16). *IT security: From cottage industry to organised crime*. Retrieved September 28, 2013, from http://www.ameinfo.com/206157.html.

Nakashima, E., & Lebling, M. (2008, July 17). Lawmakers probe web tracking: Panel examining ad technology for privacy concerns. *Washington Post*. Retrieved September 28, 2013, from http://www.washingtonpost.com/wp-dyn/content/article/2008/07/16/AR2008071602378.html?wpisrc=newsletter.

Okamoto, N. & Seo, T. (2008). On the distribution of multivariate sample skewness. *Technical Report (TR08-01)*. Retrieved September 28, 2013, from the Hiroshima Statistical Research Group website, http://www.math.sci.hiroshima-u.ac.jp/stat/TR/TR08/TR08-01.PDF.

Open Net Initiative (2009). *Blocked content*. Retrieved September 28, 2013, from https://opennet.net/research/profiles/uae.

Pham, T.L., & Jordan, E. (2009). Information technology resources and business performance: An Australian context. *Asia Pacific Management Review, 14*(4), 407-426. Retrieved September 28, 2013, from http://apmr.management.ncku.edu.tw/comm/updown/DW0911102980.pdf.

Sagi, J., Carayannis, E., Dasgupta, S., & Thomas, G. (2004). ICT and business in the new economy: globalization and attitudes towards eCommerce. *Journal of Global Information Management (JGIM), 12*(3), 44-64. http://dx.doi.org/10.4018/jgim.2004070103

Schermelleh-Engel, K., Moosbrugger, H., & Müller, H. (2003). Evaluating the fit of structural equation models: Tests of significance and descriptive goodness-of-fit measures. *Methods of Psychological Research Online 2003, 8*(2), 23-74. Retrieved September 28, 2013, from http://www.cob.unt.edu/slides/paswan/busi6280/Y-Muller_Erfurt_2003.p.

Siddiqui, H.N. (2008). *Investigation of intention to use e-commerce in the Arab countries: A comparison of self-efficacy, usefulness, culture, gender, and socioeconomic status in Saudi Arabia and the United Arab Emirates* (Doctoral dissertation), Nova
Southeastern University, Florida, USA. Retrieved September 28, 2013, from http://search.proquest.com/docview/194127355.

Srivastava, M.S. (1984). A measure of skewness and kurtosis and a graphical method for assessing multivariate normality, *Statistics & Probability Letters*, 2(5), 263-267. http://dx.doi.org/10.1016/0167-7152(84)90062-2

Srivastava, M.S. and Hui, T.K. (1987). On assessing multivariate normality based on Shapiro-Wilk W statistic, *Statistics & Probability Letters*, 5(1), 15-18. http://dx.doi.org/10.1016/0167-7152(87)90019-8

Sutton M. (2010, September 29). *The Stuxnet conspiracy*. Retrieved September 28, 2013, from http://www.arabianbusiness.com/the-stuxnet-conspiracy-352109.html.

Thompson, R., Compeau, D., & Higgins, C. (2006). Intentions to use information technologies: An integrative model. *Journal of Organizational and End User Computing (JOEUC)*, 18(3), 25-46. http://dx.doi.org/10.4018/joeuc.2006070102

Trochim, W.M.K., & Donnelly, J.P. (2008). *The research methods knowledge base* (3rd ed.). Mason, OH: Cengage Learning.

Van Slyke, C., Lou, H., Belanger, F., & Sridhar, V. (2010). The influence of culture on consumer-oriented electronic commerce adoption. *Journal of Electronic Commerce Research*, 11, 30-40. Retrieved September 28, 2013, from http://www.csulb.edu/web/journals/jecr/issues/20101/paper3.pdf
government/government-bodies-offices/14104720-1.html.

Xu, Y., & Cai, S. (2004, June). A conceptual model of customer value in e-commerce. *Paper presented at the 13th European Conference on Information Systems: The European IS Profession in the Global Networking Environment, ECIS 2004*, Turku, Finland. Retrieved September 28, 2013, from http://is2.lse.ac.uk/asp/aspecis/20040178.pdf.

Yu, F. (2007). *High speed deep packet inspection with hardware support* (Doctoral dissertation, University of California, Berkeley). Retrieved September 28, 2013, from http://www.eecs.berkeley.edu/Pubs/TechRpts/2006/EECS-2006-156.pdf

Zhang, J. (2009). Multivariate data analysis using SSPS. [Power Point Slides] *Scribd*. Retrieved September 28, 2013, from http://www.scribd.com/doc/11485761/Multivariate-Data-Analysis-Using-SPSS.
