Jordan's New Oil Sector: The Cyber Age of Hydrocarbon Security

Nicolai Due-Gundersen
Qasid Arabic Institute
22 Queen Rania (University) Street
Amman, Jordan
duegunn2@hotmail.com

ABSTRACT

The MENA region has traditionally struggled with political precariousness. In the Gulf, oil wealth has provided a symbol of socio-economic disparity and a target for political attacks. Since 9/11, activities of ideologically-driven terrorism have increased. In addition, the so-called Arab Spring has further fuelled contention between the state and aggressive political actors. However, while most attacks by such groups have been physical, the ubiquity of internet dependence in both social and professional settings has given political cells a decentralized and far less tangible weapon that can have systemic socio-economic consequences for hydrocarbon nations. Consequences can range from disruption of refinery output to widespread infrastructural damage and even loss of life. With increasing cyber-attacks on oil infrastructure in the Gulf, many National Oil Companies are seeking to strengthen online security while retaining resource management independence. The Hashemite Kingdom of Jordan provides a proximate and fast growing ICT international recognition as the region's most prolific hydrocarbon exporters [1]. Not surprisingly, the mixed blessing of hydrocarbon reserves has led many such states to become economically dependent on its oil and gas revenues [2]. Given the political climate of the MENA region, wealthy oil nations have often had to consider the possibility of politically motivated physical attacks to hydrocarbon infrastructure, the risk of which has been exacerbated by the so-called Arab Spring [3]. However, a newer, far less tangible threat has begun to emerge in the form of growing cyber attacks, with the potential to sabotage hydrocarbon operations and infrastructure. Successful cyber viruses can compromise refinery and other infrastructural integrity, with effectse ranging from temporary shutdowns to long-term physical damage, environmental pollution and even loss of life [4].

Growing regional concern has prompted Gulf Cooperation Council (GCC) states to host a conference on the current and possible effects to Arab markets of harmful cyber activity. At the first Gulf Information and Security Expo Conference in 2013, political decision makers and IT specialists have asserted the importance of cooperation across regional industries to counter the threat of growing attacks. Such a platform, however, appears to have addressed the more common issue of social media and online payment programs as cyber risks, rather than focusing solely on the effects of such attacks on the oil and gas industry [5].

hub for the outsourcing of cyber security for hydrocarbon sectors. Jordan's nascent ICT development provides flexible opportunities for cyber security advances in the hydrocarbon industry, which must be balanced with the risk of politicizing Jordan and inviting increased terrorist attacks amid the Kingdom's need to formalize comprehensive responses to online threats.

Keywords

Cyber-attacks, oil and gas, Jordan, MENA, terrorism

1. INTRODUCTION

The Middle East has enjoyed near unparalleled historical status as a hub of hydrocarbon wealth. Indeed, the Gulf States of the region, especially Saudi Arabia and Qatar have consistently enjoyed

In response to this intangible threat, certain critics have suggested a systemic approach to a problem shared by both National Oil Companies (NOCs) of affected states and International Oil Companies (IOCs), which often serve as clients of Middle Eastern hydrocarbon goods. By revising existing agreements between IOCs and NOCs, it may be possible to ensure that traditional technology transfers from IOCs to NOCs also include cyber security software, rather than only physical infrastructure [6]. While this approach may allow NOCs to negotiate cyber security arrangements within a familiar context, there are certain potential drawbacks. Most notably, NOCs would be negotiating for access to technology ultimately owned by IOCs. This form of technological dependence, along with the conflicting nature of certain respective objectives held by NOCs and IOCs would in turn undermine a significant NOC goal: independent control and management of its country's hydrocarbon resources [7].

The desire for cyber security independence of oil states must be placed within the (at times) precarious context of the political atmosphere of the MENA region and the political motives of attacks on oil infrastructure. Hence, for an NOC of the Arab world to maximize its technology independence and the relative safety of such software development, one possible solution may be to outsource cyber security advancement to a proximate ICT hub that remains aloof from the entanglements of oil politics. The Hashemite Kingdom of Jordan may provide one such option within the region.

With a declared mission to become a renowned ICT hub in the region, Jordan has succeeded in attracting international companies such as Oracle and Microsoft [8]. Furthermore, such firms have often developed emerging data platforms specific to the oil industry [9]. Considering the aforementioned factors, this paper will analyze to what extent the Hashemite Kingdom of Jordan can serve as a proximate hub of ICT development specific to the cyber security needs of NOCs, taking into consideration Jordan's relative political stability and ICT growth, while also examining the domestic cyber security context that may surround Jordan itself. In addition, Jordan's domestic software development potential will be juxtaposed against the international software firms it currently hosts, taking into account the links such firms have with IOCs.

2. The NATURE OF HYDROCARBON DATA

The overall data of the hydrocarbon industry and related companies can be divided into two classes. The first is often termed 'unstructured data', which comprises up to 80% of stored electronic information for the average energy firm. Unstructured data is usually miscellaneous electronic copies of documents, contracts, papers and other physical administrative texts that are kept as both physical records and as soft editions [10]. Due to the simple nature of such data and the presence of physical source material, such data can be easily replicated from the original if electronic copies are lost. The most sensitive and significant data is therefore the second class, 'structured data'. This latter form may comprise only 20% of hydrocarbon data; however, 80% of most energy firm IT budgets are dedicated to such software, which will normally encompass organized tables, diagrams and complex models [11]. The amount spent by the industry on such a narrow database illustrates the importance of such data to hydrocarbon firms, while also underscoring the potential vulnerability to operations such data represents if affected by cyber attacks.

3. THE NATURE OF HYDROCARBON DATA IN THE MIDDLE EAST

Within the Gulf States, certain firms such as Abu Dhabi's Adma-Opco have increased the use of software tools in the planning and operation of hydrocarbon projects. The long-term advantage of such a move is to simplify asset operations in a manner that should both reduce costs and increase profit. Such software can also allow ageing hydrocarbon equipment to be more safely operated at optimal standards [12]. As online solutions evolve to meet the needs of the hydrocarbon industry, increasingly complex structured data such as 3D and even 4D models of oil sites have the potential to replace physical handling and

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

other traditional methods of exploration and production with remote operations [13]. Systems such as Aspentech's HSYS have been adopted by Adma-Opco, seeing major use of online structured data for the complex modeling of hydrocarbon infrastructure and the potential for real-time monitoring of oil and gas projects [14]. With increasing dependence on software in the hydrocarbon industry of the Gulf, growing threats of cyber attacks in a politically volatile region may begin to increasingly affect operations.

Indeed, the Middle East Gulf holds up to 66% of the world's hydrocarbons. With political tensions exacerbated throughout the region by the Arab Spring and increasing reliance on software, it is not unthinkable that many NOCs in the Arab world will be the victims of increasingly political cyber terrorism. This scenario is all the more realistic when considering that many drivers of the Arab Spring have been tech savvy and politically motivated [15].

4. CYBER ATTACKS IN THE MIDDLE EAST

As a case in point, Saudi Arabia's NOC, Aramco, was the victim of an extensive cyber attack on August 15th, 2012, in which a computer virus succeeded in sabotaging the firm's computer network [16]. While the so-called Shamoon virus affected only unstructured data, responsibility for the attack was claimed by a group that alleged political motives, including Saudi Arabia's involvement in both Syria and Bahrain [17]. The attack succeeded in erasing up to three-quarters of Aramco's computer data and resulted in significant financial impact on an NOC with the world's largest oil production output [18]. Another significant case study is the attack on Qatari assets in the same month. As with its Saudi counterpart, Qatar's Ras Gas firm found its computer network infected by a malignant virus [19]. Although Ras Gas officials described the results of the attack as mere "technical difficulties', outside observers noted that the virus created "an unprecedented complete shutdown of its computer network." As experts predict an increase in both frequency and complexity of attacks, both structured and unstructured data may be targeted [20].

5. POSSIBLE SOLUTIONS

The most recent, regional responses to such attacks have been limited, including a conference organized by GCC States and talk of purchasing insurance against future cyber attacks by certain NOCs [21]. A more structured approach, however, has recently been discussed within the framework of utilizing existing legal agreements between NOCs and IOCs. Such a solution may present several advantages. Both IOCs and NOCs share the problem of protecting hydrocarbon data against cyber attacks, and the use of traditional regulation mechanisms (i.e. agreements) can present both parties with a familiar framework in which to tackle cyber security concerns and agree on long-term solutions, including technology transfer from e.g. an IOC to an NOC [22]. The latter element is often a key factor in the negotiation of agreements between NOCs and IOCs. It is often the case that IOCs, due to their de facto global nature and commercial size, possess the latest hydrocarbon technologies [23]. Furthermore, with the recent increase of and concern over cyber attacks targeting hydrocarbon assets and operations of the Gulf, it is likely that IOCs will prioritize access to innovative software and associated cyber security mechanisms, including internet options. In other words, much of the technology NOCs may require can already be industry standard for IOCs, providing an opportunity for agreements to act as a standard regulatory framework for cyber software access and access to related security solutions [24].

However, the revision of existing agreements between NOCs and IOCs may not be without its disadvantages. A brief survey of the historical context surrounding such agreements reveals a potentially long process that acted as a forum in which NOCs and IOCs addressed both shared and separate priorities regarding partnership approaches and resource management [25]. The nascent struggle of NOCs to ensure equal (if not dominant) influence and bargaining power over their own resource may be somewhat repeated if

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

existing agreements were to be extensively revised to include not only physical technology transfer but that of less tangible software technology. This and other considerations of NOCs can be further explicated by the simple fact that NOCs and IOCs can have significantly differing (and opposing) goals. As a state business, an NOC will seek to maintain dominant control over its hydrocarbon assets and efficient management of these assets, with the purpose of using hydrocarbon production and profits to address domestic energy and financial demands. IOCs, on the other hand, exist solely as commercial entities. As such, they are primarily motivated by revenue maximization, drawing on the efficiency of global assets, with such efficiency not necessarily being influenced by the domestic energy needs of one specific NOC's operations [26]. Although NOC-IOC partnerships are often required to split the enormous cost of initial projects, the expertise and technology IOCs can provide is often the biggest advantage IOCs boast when negotiating agreements with their domestic counterparts. The NOC requirement for technology access can therefore be a potential hindrance to the maximization of NOC interests, as national oil firms that gain technological footholds through foreign businesses risk becoming dependent on IOCs for their entire cyber security frameworks. Such a scenario may thus reduce NOC power to negotiate balanced agreements with IOCs, maintaining an already existent threat to resource sovereignty that is exacerbated by the political tensions of the Gulf region [27].

6. AN OVERVIEW OF JORDAN'S ICT MISSION

In the early 2000's, the Hashemite Kingdom of Jordan set itself the goal of becoming the Arab hub of software programming [28]. The original target set by the Hashemite government was to place Jordan's ICT industry as the third largest earning sector, with initial job creation of 30,000 occupations specific to ICT and software exports of up to 550 million USD, in addition to ensuring 150 million USD of foreign investment in Jordan's ICT industry [29]. Over the past decade, a focus on ICT educated youth, low labor costs and widespread English usage has succeeded in attracting international tech firms to Jordan's markets, including firms that have developed software solutions for IOCs [30].

Within the context of Middle Eastern politics, Jordan's peace treaty with Israel and cultural/linguistic similarities to its neighbors rounds out its relative stability. Jordan itself has attempted to maximize its appeal to markets of the GCC states, many of which already serve as important export partners [31]. As Jordan continues to push for the regional and international growth of its ICT sector, ICT familiarization and training is becoming an institutionalized norm in the early stages of classroom learning, with international firms such as Oracle and Microsoft providing training forums and technology [32]. In addition, the early training of a potential ICT workforce is being complemented by a National Information Technology Center [33]. The creation of a nationwide institute to coordinate advanced ICT training, software development and national economic growth illustrates Jordan's consideration of ICT development as a long-term and integrated part of its economic strategy, both in public and private spheres, bolstering Jordan's reliance as a public partner or ICT hub.

Given the fact that many existent hydrocarbon data systems operate online, it is also worth noting Jordan's software development plans and focus on internet development and access rivaling proximate states, including through the use of fiber optic cables [34].

7. JORDAN'S SOFTWARE AND INTERNET DEVELOPMENT

Through both the National Information Technology Center (NITC) and other public bodies, Jordan is currently building its specialization in ICT related fields. The nascent state of the ICT industry as a whole thus gives Jordan greater flexibility than other long-established ICT hubs to respond to the cyber needs of regional and international markets [35]. Furthermore, in a region that often experiences fluctuating and unreliable internet speeds, Jordan's

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

investment in fiber optic cable networks is likely to attract more international tech firms and can provide a stable hub from which proximate states can outsource their ICT needs [36].

With regards to data protection especially, Jordan's NITC has acted as a consultant and manager for the securing of data related to public bodies. This expertise is gradually filtering into Jordan's Information and Communications Technology Association (int@j), a national mediator between domestic public interests and the private business of regional and international commercial bodies [37]. Because int@j is also heavily focused on software development and includes membership of diverse data service providers, it has the potential to act as a 'tech firm hub' that can connect e.g. GCC clients, including NOCs with Jordanian and international software developers and data security providers. Through using int@j as an existent but nascent framework, it may therefore be possible to tailor software development and related services around the hydrocarbon concerns of proximate NOCs. Such a prospect may be more flexible than traditional solutions through NOC-IOC agreements and ensure NOC independence and control over cyber security mechanisms developed for clients of int@j by its members [38].

8. INT@J: UNITING PUBLIC AND PRIVATE INTERESTS

Jordan's Int@j consists primarily of domestic ICT specialists and bodies, with the central goal of advancing Jordan's ICT abilities and presence in both regional and domestic markets. While harboring an initial (and continuing) focus on software and core technology development, int@j has also expanded to become an umbrella association between the private and public sectors [39]. In addition, int@j extended this framework in 2011 to place greater weight on representing the interests of international tech firms in Jordan. Hence, int@j acts as Jordan's sole ICT mediator between not only the public and private sector but national and regional/international software development, expertise and goals within the Hashemite Kingdom. It is this latter aspect of int@j that may allow it to serve as an appropriate platform for NOC software development [40].

Because of close business ties with GCC states, int@j can act as a 'skeleton' that encompasses business and cultural practices similar to the Gulf States, while also allowing NOC clients of the Gulf the freedom of choosing between international firms located within Jordan (and members of int@j) or domestic firms. Although this scenario may present the risk of competition between international tech firms and Jordan's own offerings, such potential rivalries must be put into a certain context. As previously mentioned, certain international tech firms already develop hydrocarbon software for IOCs. Hence, should NOCs choose to outsource their cyber security needs to such firms, it is possible that developed products may be based on existent platforms already in use by IOCs. This scenario, in turn, may thus hinder the hydrocarbon data independence of NOCs, if Gulf States ultimately use and store data on platforms shared by their international counterparts [41]. On the other hand, should NOCs outsource their software needs to Jordanian firms, the nascent yet rapid growth of Jordan's ICT sector may allow for more tailored cyber security solutions, run on local and exclusive platforms to which IOCs will lack de facto access. Such a framework can allow NOCs to retain their data independence and therefore assist them in their goal to ensure resource management independence. With a dynamic yet structured and stable ICT sector, NOCs may be able to use Jordan's software developers as part of an overall management strategy to control their relations with IOCs outside the traditional framework of NOC-IOC agreements. This latter advantage of domestic developers presents a significant consideration for how NOCs may approach int@j, encouraging NOCs to outsource to domestic members, while IOCs will continue as business clients of international members of int@j [42].

9. POTENTIAL DRAWBACKS OF JORDAN'S ICT SECTOR

Although the Hashemite Kingdom of Jordan boasts several advantages for hydrocarbon

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

software development, including cultural and geographic proximity to Gulf States, certain negative factors must be considered as potential obstacles for Jordan's ICT growth. As this paper has discussed, Jordan's nascent status as an ICT hub may allow for tailored solutions, but also acts as a natural deterrent to specialization within specific ICT fields. Until local competence has been fully realized, specific subsectors of ICT markets may not structurally grow at the rate needed for Jordan to highlight its potential strengths, including that of hydrocarbon cyber security [43]. While NOCs may still be able to use international tech firms in Jordan for their cyber security needs, the sharing of software platforms with wealthier IOCs may be undesirable for NOCs due to how such a scenario may affect resource management independence, including through NOC-IOC negotiations and agreements.

Setting aside the aforementioned hindrance, there is also the long-term prospect of inadvertently bringing oil politics into Jordan. Should the Hashemite Kingdom develop a successful business niche within GCC markets, it may find itself targeted by politically motivated groups that regard Jordan at the very least as a commercial benefactor of GCC policies within the region, or even as an ally in what such hacking groups view as unwarranted interference in the politics of other Arab states.

Finally, an ongoing concern that affects most of the MENA region is the continuing failure to respond to the rise of cyber threats through appropriate security mechanisms and a thorough adjustment of office and business cultures. With the growth of ICT use throughout the region, there is likely to be a corresponding rise in cyber threats such as malware and viruses. Experts in Jordan have cited the increase in identifiable cyber threats as evidence of ongoing weaknesses in Jordan's ICT sector. In 2012, attacks were projected to more than double between 2010 and 2013 [44]. Such risks are compounded both by the increased sharing of data across business networks and the use of social networking sites in professional environments. The latter element may act as the most pervasive delivery method of malware and other harmful software that can access both personal and company data [45]. Both local and international security firms have warned Middle Eastern ICT companies and Jordanian developers especially, of their vulnerability to such threats due to the lack of updated solutions and security mechanisms [46].

It is worth mentioning that Jordan has attempted to address the rising threat of cybercrimes through a revision of its current legal framework [47]. Introduced in 2010, the Information System Crimes Law No (30) (ISC) is Jordan's first law addressing cybercrimes specifically [48]. The ISC Act lists and defines several cyber acts as criminal offenses with specific penalties for each crime [49]. Such offenses include, inter alia, unauthorized access of information systems; facilitation or support of terrorist acts; illegally accessing national security, safety and national economy information; and illegally accessing national security, safety and national economy information for the purposes of destruction or copying [50]. Although hydrocarbon and commercial interests are not mentioned in the Act, a list of cyber offenses and greater legal powers for Jordan's police and judiciary can be regarded as an improvement to Jordan's previous Electronic Transactions Act (ET Act) of 2001 [51]. The Electronic Transactions Act was limited in scope to e-commerce rather than online criminal activities, allowing the ISC Act to complement the ET Act with a specific framework to address cyber offenses [52].

However, the ISC Act has several drawbacks, the most glaring of which is that there remains a lack of a structured permanent framework for the ISC Act to investigate and prosecute cyber offenses [53]. Further, the traditional legal process within Jordan does not grant digital evidence of a criminal offense equal weight when compared to physical material presented as evidence in related cases [54]. In addition, with cybercrime a contemporary phenomenon, there remains a lack of cyber specialization within Jordan's legal culture and for its related professions, from lawyers and judges to police officers [55]. This lack of systemic specialization in the nature of

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

cyber threats remains a weakness in Jordan, forcing the Kingdom's legal bodies to turn to the more extensive cyber legislation of proximate countries for guidance to their own legal frameworks regarding cyber threats [56].

10. FINAL REMARKS AND CONCLUSION

The rise of cyber threats against the Gulf's hydrocarbon industry presents a new challenge that will be difficult to contain and adds another facet to NOC considerations of independent resource management. Although it may be possible for NOCs to gain cyber security software through negotiations with IOCs, such a solution (whether negotiated through agreements or otherwise) will not guarantee the resource management independence that NOCs crave. This paper has provided an overview of a regional alternative for GCC states. Jordan's cultural similarities and a fast developing software sector may provide an outsourcing hub that can cater to GCC hydrocarbon needs while providing Jordan with a new market and what may be its first ICT specialization opportunity. The fact that many oil states of the Gulf already share close business ties to Jordan make such an option more appealing.

While Jordan continues to develop its own ICT sector, it may also be possible for int@j to manage Gulf NOC needs and the development of appropriate (but not necessarily exclusive) hydrocarbon software for such NOCs by international tech firms that are int@j members, allowing Jordan to pave the way for new business once its ICT sector has fully developed both in terms of specialization and security. It is, of course, this latter aspect that may act as the most immediate obstacle to Jordan's ICT growth and success in garnering regional clients. With the rise of cyber attacks, Jordan and its neighbors must respond fast to establish comprehensive cyber security solutions. While Jordan may not be as much of a target for cyber attacks as oil states, a new business, with the prospect of serious growth may act as a double-edged sword for Jordan, bringing both the possibility of further market diversification and profit but also inviting the risk of Jordan joining its GCC counterparts as victims of increasing cybercrime or even cyber terrorism, which may have long-term effects on the country's stability in an already precarious region.

The recent ISC Act of 2010 demonstrates Jordan's recognition of cybercrimes as serious security threats and a willingness to address the flipside of commercial growth in the ICT sector. However, a lack of extensive experience with cyber offenses within Jordan's legal framework may limit the effectiveness of the ISC Act in addressing cyber threats to both Jordanian interests and the interests of hydrocarbon states on Jordanian soil. To strengthen its existent cybercrime legislation, Jordan may wish to examine the recent cyber laws of the United Arab Emirates (UAE). In response to the rise of cyber threats, the UAE enacted two laws in 2012 that broaden the range of prosecutable cyber offenses within its borders [57]. Both laws strengthen the legal framework of the UAE's courts and legal agents, granting courts the power to confiscate devices, deprive access to IT related equipment, shut down illegal webpages and deport foreigners guilty of cyber related offenses [58]. To further bolster its new laws, the UAE has also established the National E-Security Authority, a legal unit dedicated specifically to combating cybercrime on both a federal and emirate level, with its powers also extending into the private sector [59]. A similar framework for Jordan's ICT sector may strengthen the Kingdom's business ties within an expanding market and maintain its reputation for security.

11. REFERENCES

[1] U.S. Energy Information Administration. 2013. *Saudi Arabia-Overview*. Available online at: http://www.eia.gov/countries/cab.cfm?fips=SA

[2] U.S. Energy Information Administration. 2013. *Qatar-Overview*. Available online at: http://www.eia.gov/countries/cab.cfm?fips=QA

[3] Revenue Watch Institute. *Qatar*. Available online at: http://www.revenuewatch.org/countries/middle-east-and-north-africa/qatar/overview

[4] Lion, Hashimi. 2011. "Saudi Arabia's Political Risks". Arabia Today. Available online at: http://arabia2day.com/local/saudi-arabias-political-risks/

[5] Canty, Daniel. 2013. "Cyber threat to oil and gas companies is growing." Available online at: http://www.arabianoilandgas.com/article-10983-cyber-threat-to-oil-and-gas-companies-is-growing/#.UbMjhthmOO8

[6] Zawya. 2013. "GCC security software market growing by 14% annually as high profile cyber attacks motivate companies to invest in information security." Available online at: http://www.zawya.com/story/GCC_security_software_market_growing_by_14_annually_as_high_profile_cyber_attacks_motivate_companies_to_invest_in_information_security-ZAWYA20130502111838/

[7] S. Baig "Restructuring Oil and Gas Governing Agreements
Narrowing Cyber Security Gaps in Persian Gulf" OGEL 4 (2013)

[8] Luxner, Larry. 2000. "Jordan stakes its claim to become online regional hub". Available online at: http://www.africasia.com/archive/me/00_06/jordan_stake.htm

[9] Information and Communications Association of Jordan. 2012. *Jordan ICT Sector Profile*, p. 8. Available online at: http://intaj.net/sites/default/files/jordan_ict_sector_profile.pdf

[10] Haines, Leslie, Lyle Don. 2004. "The Digital Oilfield Today" in *The Digital Oilfield*. Oil and Gas Investor

[11] Perdue, Jeanne M. 2004. "Changing Times-at IT Speed" in *The Digital Oilfield*

[12] Grondahl, Stig. 2006. "ADMA-OPCO chooses DNV Software for deliverance of asset integrity management solutions." Available online at: http://www.dnv.com/press_area/press_releases/2012/admaopco_chooses_dnv_software_for_deliverance_of_asset_integrity_management_solutions.asp

[13] Changing Times-at IT Speed", p. 11; Decou, Reynold. 2004. "How El Paso Production went Digital" in *the Digital Oilfield*

[14] Chaudhari, Sunil. 2006. "Maximising profit through real-time performance management". Available online at: http://www.aspentech.com/uploadedFiles/News/Articles/2013/FY13%20Feb%20-%20Chemical%20Weekly%20India%20-%20Maximising%20profit%20through%20real-time%20performance%20management-signed.%20PressBox.%20MDB.%20EDM.pdf

[15] Qurban, Mohammad A., Joydas, T.V., Manikandan, K.P., Krishnakumar, P.K., and Wafar, Mohideen, "Oil–related activities and environmental concerns in the Gulf"

[16] Finkle, Jim. 2012. "Exclusive: Insiders suspected in Saudi cyber attack." Reuters. Available online at: http://www.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idUSBRE8860CR20120907

[17] U.S. Energy Information Administration. 2013. *Saudi Arabia-Analysis.* Available online at: http://www.eia.gov/countries/cab.cfm?fips=SA

[18] Paganini, Pierluigi. 2012. "RasGas, new cyber attack against an energy company"

[19] Bindemann, Kirsten, Production-Sharing Agreements: An Economic Analysis, Oxford Institute for Energy Studies

WPM 25, October 1999

[20] 2000. "Jordan Stakes its Claim to Become Regional Online Hub." Available online at: http://www.thefreelibrary.com/JORDAN+STAKES+ITS+CLAIM+TO+BECOME+REGIONAL+ONLINE+HUB.-a062685698

[21] Information & Communications Technology Association. 2012. *Jordan ICT Sector Profile: Analysis, Achievements, Aspirations*

[22] 2013. "Queen discusses ICT role in education." Jordan Times. Available online at: http://jordantimes.com/queen-discusses-ict-role-in-education

[23] Government of Jordan. *National Information Technology Center: General Information*. Available online at: http://images.jordan.gov.jo/wps/wcm/connect/gov/eGov/Government+Ministries+_+Entities/National+Information+Technology+Center/General+Information/

[24] *NITC: Internet Services*. Available online at: http://www.nitc.gov.jo/isp.html, translated from original Arabic

ISBN: 978-0-9891305-5-4 ©2014 SDIWC

[25] Int@j. 2012. "Education and specialization key to growth of Jordan's IT industry." Available online at: http://www.intaj.net/content/education-and-specialization-key-growth-jordan%E2%80%99s-it-industry

[26] Ghazal, Mohammad. 2012. "Jordan, region need better preparation for rising tide of cyber attacks." Available online at: http://jordantimes.com/jordan-region-need-better-preparation-for-rising-tide-of-cyber-threats

[27] Faqir, Raed S.A. 2013. "Cyber Crimes in Jordan: A Legal Assessment on the Effectiveness of Information System Crimes Law No (30) of 2010", in *International Journal of Cyber Criminology* (7): 1

ISBN: 978-0-9891305-5-4 ©2014 SDIWC