# [**TITLE**]

# **ABSTRACT**

# **INTROUDCTION**

Cybercrime by definition varies from countries to countries. Cybercrime can vary from country to country for example in North Korea it is a crime to access the Internet without the government consensus where else in China follow strict censorship law which bans use of Google search engine. Cybercrime in general is a mean orchestrating a crime by using computer and internet as a mean. Cybercrime can take place at three levels namely in person, organization and governmental level. Cybercrime in person would mean hacking someone account to gain personal information, Cyber Stalking, Defamation, identity theft and blackmailing. Cybercrime involving at organization level includes DDOS (Distributed Denial of Service) which may bring down a website or disrupt services, illegal access of data or stealing information from financial firms and customer’s data. Cybercrime at governmental level would involve cyber terrorism, pornography, human trafficking and affecting public moral. Cybercrime is evolving and there are many vectors of attack emerging in which the existing law need to be either amended or new anti-Cyber laws need to be introduced in order to take the relevant actions against those crimes. The conviction of criminal involved in a cybercrime generally depends on the financial loss or damage caused to the infrastructure or to an individual. As per the Arab News articles one of the loop holes which the Anti-Cyber law in Saudi Arabia does not addresses is the impersonation on Social Media. As Social Media is a popular tool for advertising, communication and marketing it was found that imposters were using it as means to impersonate key figures like celebrities and political figures. Since no financial loss was caused there is no conviction for impersonator on social media **(Tashkandi, 2019)**. On the other hand, the Anti-Cyber Law in Saudi Arabia proved to be effective where 22 people were arrested by the Saudi Presidency of state security who were found guilty for stirring incitement to commit certain act which was deemed criminal in nature by the Saudi law **(Arab News, 2017)**. The outline of this paper to understand the Anti-Cyber Laws in Saudi Arabia which works in conjunction with the Sharia Law, fines and penalties associated with the criminal act, comparing the Anti-Cyber Law with the developed nations and highlighting new emerging threats in the Cyber World which need to be addressed.

# **INTERNET PENETRATION IN SAUDI ARABIA**

|  |  |  |
| --- | --- | --- |
| Classification of Internet Users in Saudi Arabia | Figure in millions | Percentage |
| Population of Saudi Arabia | **33.25** | **100%** |
| Internet Users in Saudi Arabia | **30.25** | **90.98%** |
| Active Social Media Users | **25** | **75.19%** |
| Active User Accessing Social Media from mobile device only | **18** | **54.14%** |

Saudi Arabia has a population of 33.25 million and it has achieved 100% Internet penetration. The classification of Internet users in Saudi Arabia is given below in Table 1. Roughly 90.98% of the population are active internet user in Saudi Arabia. 75.19% users are active social media users which consist of young population of Saudi Arabia and 54.14% of the users are accessing social media through their mobile phones.

*Table 1: Classification of Internet Users in Saudi Arabia* ***[4]***

1. **CYBERCRIME COST IN SAUDI ARABIA**

According to the Ministry of Communication and Information Technology (MCIT), Saudi Arabia the cost of Cyber Crime result in SAR 2.6 billion loss each year **(MCIT, 2019).** According to the Norton Cyber Crime report of 2012 it is estimated that more than 3.6 million people fall victim each year of cybercrime resulting in average loss of SAR 730. In Saudi Arabia 40% of social networking user have been a victim of cybercrime on social networking platform. 20% have been a victim of social or mobile cybercrime. The monetary loss of the cybercrime is expected to increase with emergence of concept like Internet of things (IoT), cashless economy and Smart Cities. New attack like ransomware and hijacking mobile phones has contributed to the increase in financial losses due to Cyber-crime.

1. **CYBERCRIME IN SAUDI ARABIA**

Some of the Major Cyber Crime that has taken place in Saudi Arabia is listed in table 2. These Cybercrimes were carried out on Governmental Organization and Multinational companies.

|  |  |  |  |
| --- | --- | --- | --- |
| Year | Name | Description | Damage Assessment |
| 15th August 2012 | Shammon | It is a very destructive wiper malware. Wiper is the class name of malwares that wipe out hard drives. Usually, wiped data is not recoverable. Shamoon was the most famous wiper so far. | Infected as many as 30,000 of its Windows- based machines. Despite its vast resources as  Saudi Arabia’s national oil and gas firm, Aramco, according to reports, took almost two weeks to  recover from the damage. The virus erased data on the infected computers by replacing all of it  with an image of a burning American flag **(Bronk, C., 2013)** |
| 2016/2017 | Shammon 2.0 | It is a very destructive wiper malware. Wiper is the class name of malwares that wipe out hard drives **(Falcone, R., 2017)**. | Saudi staterun Al Ekhbariya TV reported that 15 government entities and private organizations had been hit with Shamoon 2. |
| 30th November 2016 | StoneDrill | StoneDrill has several “style” similarities to  Shamoon, with multiple interesting factors and techniques to allow for the better evasion  of detection **(Kaspersky,2017)**. |  |
| 20th November 2017 | Advanced Persistent Threat (APT) | The malicious PowerShell  utilizes HTTP tunneling to communicate with the command and control domains. The HTTP  requests and responses contains data exfiltrated from infected machines or commands to be  executed by the threat actor **(Alabdulatif, 2018)**. |  |
| 15th August 2015 | Cyber of Emotions | A Saudi group hacked more than 24  government sites within two hours, after government officials ignored messages about a possible  attack **(Alriyadh, 2014)**. | Targeted Government website and compromised several accounts |
| December 2017 | Triton | security firm FireEye reported an incident at a critical infrastructure  organization where an attacker deployed malware designed to manipulate industrial safety  systems. The targeted systems provided emergency shutdown capability for industrial processes **(Alabdulatif, 2018)**. | The attacker gained remote access to Safety Instrumented System (SIS) engineering workstation  and deployed the TRITON attack framework to reprogram the SIS controllers. During the incident,  some SIS controllers entered a failed safe state, which automatically shut down the industrial  process and prompted the asset owner to initiate an investigation |

*Table 2: Cyber-attacks in Saudi Arabia*

## **ANTI-CYBER LAW LEGISLATION IN SAUDI ARABIA**

According to the United Nation Conference on Trade and Development 2018 the World Wide Cyber Law legislation globally is given in table 3:

|  |  |
| --- | --- |
| Countries with Legislation | 72% |
| Countries with draft legislation | 9% |
| Countries with no legislation | 18% |
| Countries with no Data | 1% |

*Table 3: Cyber Crime Legislation World Wide (UNCTAD, 2018)*

According to the UNCTAD 135 out of which 95 countries are developing and transition economies which had enacted legislation. 30 countries had no cybercrime legislation **(UNCTAD,2018)**.

## *Cyber Crime Legislation in the GCC countries*

The GCC (Gulf Cooperative Council) consist of six countries in the middle east namely Saudi Arabia, Kuwait, United Arab Emirates, Qatar, Bahrain and Oman. The Table 4 given below the Cyber Law Legislation enacted in the GCC countries

|  |  |  |
| --- | --- | --- |
| *Country* | *Legislation Enacted* | *As per the United Nation conference on trade and development* |
| Saudi Arabia | March 2007 | Legislation |
| Oman | February 2011 | Legislation |
| UAE | August 2012 | Legislation |
| Bahrain | September 2014 | Legislation |
| Qatar | September 2014 | Legislation |
| Kuwait | July 2015 | Draft Legislation |

*Table 4: Cyber Crime Law legislation in the Middle East* ***(Hakmeh,J.,2018)***

The body of law in Saudi Arabia is the Sharia. The sharia is based on the collection of sources which is derived from the holy Quran and Sunnah. The acts which are prohibited under the sharia law are punishable by penalties laid out by the holy Quran and sharia. Penalties can include imprisonment, monetary compensation or deprivation of certain rights. The major factor that a judge will take into consideration the damage suffered by the victim and whether the damage was deliberate or unintentional. In general, proven damages are taken into consideration by the judiciary body **(Mohamed, B. et al.,2013)**.

The Secondary source consist of ijtihad(Where a religious scholar tries to reach a religious verdict). Ijtihad mainly consist of consensus (Ijmaa) and analogy(Qiyas). The consensus mean where a religious scholar tries to reach a verdict which is not provided in the Quran and Sunnah. The general consensus decision is hold valid unless it does not contradict the Quran and Sunnah **(Algarni,A., 2006)**

* 1. *Cyber Readiness Index in Saudi Arabia*

According to the CRI(Cyber Readiness Index) 2.0 is based on namely seven pillars namely national strategy, incident response, e-crime and law enforcement, information sharing, investment in research, development and diplomacy and trade, defense and crisis response. According to the assessment Saudi Arabia is still lacks in the 7 pillars of Cyber Readiness Index but has performed well in being Cyber Ready **(Global Cyber Security Index, 2018)**.

According to Melissa Hathaway there is a still a need of trained judges, prosecutor, lawyers and law enforcement to successfully tackle the issues related to Cyber Crime and investigate and prosecute the perpetrator based on Digital Evidence **(Hathaway, M. et al., 2017).**

* 1. *Saudi Anti Cyber-Law*

The Saudi Anti-Cyber Law Royal Decree No. M/17 was presented in March 2007 and has 16 articles in total. The Articles provide the description of the Cyber Crime and associated penalties related to those crimes. This is provided in Table 5 presented below **(Saudi Arabia, Anti-Cyber Law, 2007)**:

|  |  |  |  |
| --- | --- | --- | --- |
| Article | Crime | Penalties | Imprisonment Term |
| Article 3 | 1. Spying, interception of data transmitted through the network or computer without legitimate authorization 2. Unlawful access with the intention to threaten or blackmailing a person 3. Unlawful access to website/Hacking/Defacing or hijacking the URL 4. Invasion of privacy related to hijacking mobile phone cameras 5. Defamation and imposing damages by mean of Information Technology**(Saudi Arabia, Anti-Cyber Law, 2007)** | Fine not exceeding up to five hundred thousand riyals | Not exceeding more than a year |
| Article 4 | 1. Acquisition of movable property or bonds for oneself or others or signing such bonds through fraud or use of false name or identity. 2. Illegally accessing bank or credit data, or data pertaining to ownership of securities with the intention of obtaining data, information, funds or services offered**(Saudi Arabia, Anti-Cyber Law, 2007)**. | Fine not exceeding up to two million Saudi Riyals | Not Exceeding more than 3 years |
| Article 5 | 1. Unlawful access to computers with the intention to delete, erase, destroy, leak, damage, alter or redistribute private data 2. Causing the information network to halt or breakdown, or destroying, deleting, leaking or altering existing or stored programs or data. 3. Obstruction of access to, distortion, and causing the breakdown of services by any means **(Saudi Arabia, Anti-Cyber Law, 2007)**. | Fine not exceeding up to three million Saudi Riyals | Not Exceeding more than 3 years |
| Article  6 | 1. Production, preparation, transmission, or storage of material impinging on public order, religious values, public morals, and privacy, through the information network or computers. 2. The construction or publicizing of a website on the information network or computer to promote or facilitate human trafficking. 3. The preparation, publication, and promotion of material for pornographic or gambling sites which violates public morals. 4. The construction or publicizing of a web site on the information network or computer to trade in, distribute, demonstrate method of use or facilitate dealing in narcotic and psychotropic drugs **(Saudi Arabia, Anti-Cyber Law, 2007)**. | Fine not exceeding up to five million Saudi Riyals | Not Exceeding more than 5 years |
| Article 7 | 1. The construction or publicizing of a website on the information network or on a computer for terrorist organizations to facilitate communication with leaders or members of such organizations, finance them, promote their ideologies, publicize methods of making incendiary devices or explosives, or any other means used in terrorist activities. 2. Unlawful access to a web site or an information system directly, or through the information network or any computer with the Intention of obtaining data jeopardizing the internal or external security of the State or its national economy **(Saudi Arabia, Anti-Cyber Law, 2007)**. | Fine not exceeding up to five million Saudi Riyals | Not Exceeding more than 10 years |

*Table 5: Anti –Cyber Law in Saudi Arabia and the respective penalties for those Cyber Crime,* **(Saudi Arabia, Anti-Cyber Law, 2007)**

1. **COMPARISON OF SAUDI CYBER LAW WITH DEVELOPED COUNTRIES**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cyber Crime** | **Saudi Arabia** | **United Kingdom** | **United States of America** |
| Unauthorized access | Article 3 | Computer Misuse Act 1990  Section 1**(United Kingdom, Cyber Prosecution guidance,2019)** | Computer Fraud Abusive Act, section 1030 |
| Hacking | Article 3 | Computer Misuse Act 1990  Section 2**(United Kingdom, Cyber Prosecution guidance,2019)** | Computer Fraud Abusive Act, Section 1030 |
| Invasion of Privacy | Article 3 | Regulation of Investigatory Powers Act | Privacy Act of 1974 |
| Defamation | Article 3 | **(Defamation Act, 2013)** | Section 230 of the Communication Decency Act |
| Illegal access of data | Article 4 | Data Protection Act  Section 55**(United Kingdom, Cyber Prosecution guidance,2019)** | Computer Fraud Abusive Act, Section 1030 |
| Denial of Service | Article 5 | Computer Misuse Act1990  Section 3**(United Kingdom, Cyber Prosecution guidance,2019)** | Computer Fraud Abusive Act, Section 1030 |
| Pornography | Article 6 | Section 2 of the obscene publication act**(United Kingdom, Cyber Prosecution guidance,2019)** | Child Pornography prevention Act |
| Privacy Law |  | Data Protection Act | Federal Trade Commission Act |
| Identity theft |  | Fraud Act 2006 | Identity theft and Assumption Deterrence Act |
| Human Trafficking | Article 6 | **(Human Trafficking and Exploitation Act, 2015)** | Human Trafficking Prevention Act |
| Cyber Terrorism | Article 7 | Computer Misuse Act1990  Section 3ZA**(United Kingdom, Cyber Prosecution guidance,2019)** | Section 814 of the Act ‘Deterrence and prevention of Cyberterrorism’ |
| Facilitation | Article 8,9 and 10 | Computer Misuse Act1990  Section 3A**(United Kingdom, Cyber Prosecution guidance,2019)** | Computer Fraud Abusive Act, Section 1030 |

1. **DISCUSSION AND ANALYSIS**

As technology grows at a rapid rate so does surface of attack grows. Hackers are always out there hunting for vulnerabilities in system and now with the IoT(Internet of things) where every smart device will be connected to the cloud this give away a large surface of attack which has grown even larger in coming years. There is more sophisticated attack like ransomware and Cyber terrorist attack. With the changing nature of the Cybercrime adequate law should be in place to address these issues. In Saudi Arabia there is need to address laws on Identity theft. There should be laws to safe guard and protect the privacy of customer data. According to **(Global Cybersecurity Index,2018),** Cyber Security Index 2018 Saudi Arabia has introduced Parental control service regulatory framework in 2018 which provide guideline on how to report abuses on social media.

Based on Global Cyber Security Index 2018 Report by the International Telecommunication Union **(Global Cybersecurity Index,2018),** shows the CGI score for the above three countries covering the five pillars based on conceptual framework by International Telecommunication Union (ITU) which aim to build an International cooperation amongst countries regarding cybersecurity and build current and future initiative. According to the Conceptual Framework proposed by International Telecommunication Union (ITU) given below is the description of the five pillars:

Legal: Provide means of measurement based on legal institution and framework to address issues on Cyber Security and Cyber Law

Technical: Provide means of measurement based on existing technical institution that provide framework dealing with Cyber Security

Organizational: Provide measurement based on existing policy coordination institution and strategies for development of Cyber Security practices nationwide.

Capacity Building: Measurement based on the amount of research and development, education, training program, campaign raising awareness on Cyber Security and certified professional which can aid in capacity building.

Cooperation: Measurement is based on existence of partnership, cooperative framework and information sharing. **(Global Cybersecurity Index,2018)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Country | GCI Score | Legal | Technical | Organizational | Capacity Building | Cooperation |
| United Kingdom | 0.931 | 0.200 | 0.191 | 0.200 | 0.189 | 0.151 |
| United States of America | 0.926 | 0.200 | 0.184 | 0.200 | 0.191 | 0.151 |
| Saudi Arabia | 0.881 | 0.187 | 0.179 | 0.158 | 0.198 | 0.160 |

*Table 7: Comparison the CGI score for the three countries* **(Global Cybersecurity Index,2018)**

1. **CONCLUSION**

There is need for new Anti Cyber Law in Saudi Arabia to deal with identity theft, Laws to protect the online privacy of consumer, protection of children from abuse on social media websites. Social Media is used to incite violence and spread false rumors. There should be strict regulation and laws that hold certain activities on social media accountable. There is a need for training of judges on Cyber Laws. Adoption of new Cyber Law legislation such as ‘Right to be forgotten’ **(Richi, 2019),** and ‘DHS Cyber Hunt and Incident Response Team Act (S.315)’ introduced in 2019 **(Abrams, 2019).**

REFERENCE

1. Tashkandi, H, ‘Impersonation: Social media users suffer as cybercrime goes unpunished’, Arab News, February 02,2019.

<https://www.arabnews.com/node/1445646/saudi-arabia>

1. ‘22 people arrested for 'incitement' and violating Saudi Anti-Cyber Crime Law’, Arab News, October 05, 2017.

<https://www.arabnews.com/node/1172601/saudi-arabia>

1. Mohamed, B. and Elamin, B., 2013, Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future. Journal of Information and Knowledge Management.
2. <https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/>
3. Saudi Arabia, Ministry of Communications and Information Technology, 2019. Cyber Crime Costs Saudi Arabia SR 2.6 Billion a year. Available at:

<https://www.mcit.gov.sa/en/media-center/news/92479>

1. United Nations Conference on trade and development, Cyber Crime Legislation Worldwide, 2018. Accessed at:

<https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx>

1. Hakmeh, J,(2018). Cyber Crime Legislation in the GCC Countries Fit for Purpose? Chatham house, The Royal Institute of International Affairs, pp 7. Available at:

<https://www.chathamhouse.org/sites/default/files/publications/research/2018-07-04-cybercrime-legislation-gcc-hakmeh-final.pdf>

1. Global Cyber Security Index, 2018. International Telecommunication Union. Available at:

<https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf>

1. Algarni, A. (2006), Fraud and Counterfeiting in the Information Age, Riyadh: King Fahad Security College Research Centre (in Arabic).
2. Hathaway, M., Spidalieri,F. and Alsowailm, F. ‘Kingdom of Saudi Arabia Cyber Readiness at a glance’, Potomac Institute for Policy Studies. Available at:

<https://potomacinstitute.org/images/CRI/CRI2_0_SaudiArabiaPofile.pdf>

1. Bronk, Christopher. 2013. "The Cyber Attack on Saudi Aramco." Survival: Gobal Politics and Strategy 81-96
2. Falcone, R., 2017. ‘Second Wave of Shamoon 2 Attack identified’, Paloalto Network. Accessed at:

<https://unit42.paloaltonetworks.com/unit42-second-wave-shamoon-2-attacks-identified/>

1. Kaspersky, 2017. FROM SHAMOON TO STONEDRILL Wipers attacking Saudi organizations and beyond. Accessed at:

<https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07180722/Report_Shamoon_StoneDrill_final.pdf>

1. Alriyadh. 2014. Breakthrough the Ministry of Justice official account in Twitter. Accessed at: <http://www.alriyadh.com/984899>
2. Alabdulatif, A, 2018. ‘Cyber Crime and analysis of laws in Kingdom of Saudi Arabia’. Thesis University of Houston, pp 20-23. Accessed at : <http://hdl.handle.net/10657/3107>
3. Kingdom of Saudi Arabia, 2007. ‘Anti-Cyber Crime Law’ Royal Decree No. M/17. Available at:

<https://www.wipo.int/edocs/lexdocs/laws/en/sa/sa047en.pdf>

1. United Kingdom, Cyber Prosecution guidance, 2019. Accessed at:

<https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance>

1. Defamation Act, Chapter 26, 2013, United Kingdom, Accessed at : <https://www.legislation.gov.uk/ukpga/2013/26>
2. Human Trafficking and Exploitation Act,2015, United Kingdom, Accessed at:

<http://www.legislation.gov.uk/asp/2015/12/contents/enacted>

1. Computer Fraud Abusive Act, section 1030, 2008. United States of America. Accessed at:

<https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf>

1. International Telecommunication Unit (ITU), Global Cyber Security Index, 2018. Available at: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>. (Accessed at: August 02,2019)
2. Richi Jennings, 2019. ‘EU Right to be forgotten: France fails, Google gains on privacy pull back’. Available at: <https://techbeacon.com/security/eu-right-be-forgotten-france-fails-google-gains-privacy-pullback>. (Accessed at September 27,2019)
3. Lawrence Abrams, 2019. ‘The Week in Ransomeware – September 27th 2019 –Quiet before the storm?’. Available at: <https://www.bleepingcomputer.com/news/security/the-week-in-ransomware-september-27th-2019-quiet-before-the-storm/>. (Accessed at: September 27,2019)