Chapter 8
Cyber Security Crime and Punishment:
Comparative Study of the Laws of Jordan, Kuwait, Qatar, Oman, and Saudi Arabia

Evon Abu-Taieh
The University of Jordan-Aqaba, Jordan

Auhood Alfaries
King Saud University, Saudi Arabia

Shaha Al-Otaibi
Princess Nourah Bint Abdulrahman University, Saudi Arabia

Ghadah Aldehim
Princess Nourah Bint Abdulrahman University, Saudi Arabia

ABSTRACT

Cyberspace and the existence of the internet allows different types of crimes to appear. Hence, there is a need for new laws to be set with a collective, comprehensive, view of crime and a global understanding. This article studies 5 different countries' laws pertaining to cybercrimes namely: Jordan, Oman, Kuwait, Qatar, and Saudi Arabia. These different countries issued different laws at different times, some in 2007 others are as new as 2015. The article looks at the laws from an academic definition of different crimes, and also describes the laws from a perspective of each country.

INTRODUCTION

Cyber-crime is a global worry that touched the world, the new technology of internet and smart tools spawned new types of crime and they are on the rise. In the UK, (NCA, 2016) stated that "cybercrime now accounts for more than 50% of all crimes in the UK." Worldwide "According to the PandaLabs report, 18 million new malware samples were captured in this quarter alone, an average of 200,000 each

DOI: 10.4018/978-1-5225-7912-0.ch008

day" (Pandasecurity, 2016). "Policing, especially in cyberspace, is no longer the exclusive preserve of law enforcement. The private sector, academia, and citizens themselves all need to be involved," the Interpol chief said (Interpol, 2016). Furthermore, "ensuring that police around the world are provided with the basic equipment and training they need". According to a study conducted by Cukier there is a hack attempt every 39 seconds (Cukier, 2018). There is a 600% increase of attacks against IoT devices from the year 2016 to 2017, also average number of malicious mobile apps blocked each day is 24,000 (Symantec, 2018). Nearly 700 million people in 21 countries experienced some form of cybercrime (Symantec, 2018). Crimes are spreading to the entire world, since the whole world is interconnected. One the Major destructive malware attacks is Shamoon use against Saudi Arabia in 2012 and 2016 according to Symantec (2018).

Saudi Arabia ranked number 5 according to (Symantec, 2018) in email malware rate followed by Kuwait as 8. Saudi Arabia ranked number 1 according to (Symantec, 2018) in Spam rate by country followed by Kuwait as 6 and Oman 7.

According to (Stalling, 2011) attacks on computers can be categorized into two categories: Passive and active attacks. Passive attacks imply interception of data or information hence threatening the secrecy, which can be classified to release of contents and traffic analysis. On the other hand, active type of threat can be categorized into four categories: masquerade, replay, modification of message, and denial of service. The masquerade active attack implies impersonating an entity. Replay involves retransmission of data to produce "unauthorized effect" (Stalling, 2011). The modification of message as the name implies is to alter/delay a message to produce an unauthorized effect. The denial of service is to prevent "a normal use or management of communications facilities" (Stalling, 2011). Defining the different types of threats academically does not make the act illegal. Hence, laws, rules, regulations must define such acts as criminal acts in order to make such act punishable by law.

Furthermore, other uses of data, information, and websites were made illegal by different laws and regulations according to countries: transfers, copy and modifications to data, information, websites that pertains to financial matters, sex, national security, national economy, and public safety of the country. Uses of websites and other electronic sources for the purpose of human trafficking, drugs, and terrorism were made illegal.

RELATED WORK

Some fourteen related researches were found pertaining to the issue of cyber law. Below each was summarized to convey the importance of this topic. Lunker (2018) Presented in a research report titled "Cyber Laws: A Global Perspective" that the rapid growth of technology and internet have led to growth of crime that has no borders and are none-physical in real world. Simply "creating a new realm of human activity and undermining the feasibility and legitimacy of applying laws based on geographic boundaries" (Lunker, 2018) such thing will deter people from conducting business on internet, and promulgate lack of trust, furthermore bringing the wheel of production to dead halt. Horsman (2017) discusses the dire need for policing social network through both law and the owners of the social network. The author coined the term "regulatory gaps," sharing a range of crimes starting with bullying over the social networks to harassment, and stalking. In fact, the author called for "regulating social network crime and online offender tracking." Polanski (2017) called to customary law for the lack of governing laws and