# Comparison between Saudi Arabia and USA: Prevention and Dealing with Cyber Security

**Sonia Ibrahim, Nada Alkenani, Banan Alghamdi, Amal Alfgeeh, Salwa alghamdl, Yusra Alzhrani, Amani Almuntashiri, Rawan Alghamdi, Abeer Salawi, Wejdan Ahmed Alghamdi, Mohammed. I. Alghamdi**

College of Computer Science and Information Technology, Department of Engineering and Computer Sciences, Al-Baha University

Emails: soniabrahim301@gmail.com, 442020945@stu.bu.edu.sa, banan.s1s1@gmail.com, amalalfgih@hotmail.com, 442021118@stu.bu.edu.sa, yosra977@hotmail.com, amaniabdul39@gmail.com, rawanawd08@gmail.com, AbeerSalawi87@gmail.com, 443040568@stu.bu.edu.sa, mialmushilah@bu.edu.sa

**Abstract**

Cyber security practices mainly involve the prevention of external threats to software, hardware, server data, and other assets which are connected to the internet. Organizations follow a lot of cyber security practices to protect their systems and databases from malicious cyber actors. Cybercriminals use different techniques like spear-phishing, phishing, password attack, denial of service, ransomware, etc. to cause harm to people, organizations, and governments and steal important information from them. We analyzed the use of deep learning algorithms to deal with cyber-attacks. Deep neural networks or deep learning consist of machine learning procedures to support the network to fix complex issues and learn from unmanaged data. In addition, we also analyzed some of the cyber security laws and practices implemented in the US and Saudi Arabia to work collaboratively against cyber threats. It is observed that both countries are doing well against cyberthreats, but they need to work even more to provide training and support to professionals in the public sector who handle sensitive data about cyber security.

**Keywords:** Saudi Arabia, US, Cyber Security, Cyberthreats.

## 1. Introduction

Cyberspace is viewed as an important part of all aspects of life in the US, including their defense and economy (The White House, 2018). Being the superpower and cradle of the cyber domain, the US is probably the first country to find lethal threats intertwined on the internet. The country has always raised its voice for legal regulations on virtually "unregulated" cyberspace. Due to constant deliberations, the US has a strong cyber law infrastructure. The US deals with cyber security issues at the federal level with sector-specific regulations and statutes.

Some of the major cyber security laws in the USA are the "Gramm-Leach-Bliley Act (1999)", the "Health Insurance Portability and Accountability Act (HIPAA)" passed in 1996, and the "Federal Information Security Management Act (FISMA)". As the name suggests, HIPAA is focused on the healthcare sector and FISMA handles cyber security matters for federal agencies. Some other statutes are dealing with specific matters, including 2006's "Veterans Affairs Information Security Enhancement Act" (Craig, 2006) and they serve only one government agency, i.e., the Department of Veterans Affairs (VA). There are also other cyber laws for populous states like New York, Massachusetts, and California.

However, some cyber laws have raised criticism for being too invasive and regulative. For example, Congress had enacted the "Computer Fraud and Abuse Act (CFAA)" in 1986 which criminalizes the access and constant sharing of protected data. It has been criticized a lot for disincentivizing legal security research and being too restrictive (Charles Koch Institute, 2016). Since

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

1986, the US government has been able to access digital communications like social media messages, emails, etc. with a court order (Subpoena) under the "Electronic Communications Privacy Act.

Considering the increasing and more complex challenges in cyberspace which are getting multi-sectoral day by day, a uniform cyber security framework is the need of the hour. The cyber regulations have affected compliance at several sectors and levels as companies have to deal with various state and federal laws. Hence, the "Cyber Security and Infrastructure Security Agency Act" was signed in 2018 by Donald Trump, former US President (McCaul, 2018). On the other hand, the UAE is a rapidly growing economy, but it has been widely on the radar of cybercriminals over the years (Mansoor, 2020) due to its booming oil industry, rapid technological growth, and heavy growth of the economy. Hackers unleashed their sinister cyber-attacks during the COVID-19 pandemic on the servers of UAE-based companies which caused financial insecurities and fear (Sanderson, 2020). The UAE has the most robust cyber laws in the Middle East region, considering the changing scenario.

The "Cyber Crimes Law 2012" or the "UAE-Law No. 5, 2012" is aimed at "Combating of Information Technology Crimes" replacing the previous "Cyber Crimes Law, 2006". The Telecom Regulatory Authority of UAE has supervised and established the Computer Emergency Response Teams (UAE CERT) for sharing cyber security information with the government and improving cyber security in India. They work with various law enforcement agencies to enforce frameworks and policies to deal with cyber-attacks. UAE CERT shares data and collaborates with the CERTs of other countries worldwide so that researchers can improve the path to information security. The "National Electronic Security Authority (NESA)" is the federal body in the UAE to monitor cyberspace of the country. The UAE's "National Cyber Security Strategy 2019" is aimed to create robust and safe cyberspace in the UAE for citizens to meet their needs and encourage businesses to raise and thrive. The legal framework consists of artificial intelligence, data security and privacy, cloud services, blockchain, and digital signatures.

### 1.1 Background

With the emergence of the IoT and AI-driven world and the revolution of the information age, there has been a sporadic growth of virtual space for the global internet community. The cyber-world is the first and last resort for today's generation, from education to business to entertainment and recreation. However, extreme dependence for daily activities on the web of the users without knowing and worrying about the potential risks has been the major issue. Though there have been endless possibilities unleashed by the web for improving human efficiency, there are a lot of concerns about security in cyberspace on the enormity of the internet.

Sovereign countries across the world have made modest attempts to make frameworks from their part of making borderless cyberspace to protect the sovereignty and citizens' rights and national security like in the physical world. Several Cyber laws have been formed over the recent decades which enumerate the protections and limits and regulatory guidelines in the virtual world. These laws consist of the protection of freedom of speech, intellectual property rights, and access to data by the public. There are several differences and similarities among the existing policies and cyber laws worldwide.

The United States already has the most robust cyber security frameworks and oldest cyber laws in the world, while Saudi Arabia is emerging in cyber security. Frauds and cybercrimes lead to huge security threats and financial losses to the web and economic ecosystems because current laws are insufficient, despite being useful. Each country has defined its legal frameworks, but it is important to pay attention to the need for universally recognized and comprehensive cyber security law. With a comparative study between the US and Saudi Arabia, this paper attempts to analyses cyber security practices for dealing with and prevention of cyber-attacks in both countries.

### 1.2 Literature Reviews

Rapid globalization, ever-rising dependence on IoT, and technological advancements have led to seamless ways for people to publish, interact, and share content through high-speed networks despite the distance and location. But internet and communication technology (ICT) has also become a breeding ground for all kinds of cyber-crimes like deception, extortion, online scams, financial frauds, cyberbullying, etc., especially in Saudi Arabia. **Nuaimi (2021)** examines several Cyberbullying prevention strategies implemented in Saudi Arabia and determines the risky use of internet tools and their association with cyber-bullying. The author also determines how effective these strategies are in Saudi Arabia. The findings suggest the best possible recommendations for cybercrime regulators and policymakers.

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

Considering the above cyber threats, it is very vital to improve awareness about cyber security. Hence, **Alzubaidi (2021)** measures the existing cyber security awareness levels in Saudi Arabia in terms of incident reporting and security practices through an online questionnaire. The findings also suggest some recommendations as per the data analysis to promote awareness level. **Alrubaiq & Alharbi (2021)** provide a detailed analysis of cyber security by examining some of the most important parts of cyber security in e-government initiatives in the Kingdom of Saudi Arabia. They proposed a holistic framework to implement several scientific guidelines.

To make computers think and work like humans, Artificial Intelligence (AI) is a great aspect of ICT that can recognize speeches and touch for doing common activities without human intervention. Most of the systems are designed to serve the purposes as per the nature of the environment and the natural reactions of humans. Its intelligence is based on machine learning. **Soni (2020)** evaluates the existing challenges and solutions for AI in cyber security in the US and proposes innovative solutions for AI in cyber security in the United States.

Cyber security is very vital to protect the information in mobile devices, servers, computers, computer networks, systems, and electronic devices from malicious actors. There are different forms of malicious attacks emerging over the years, especially in the United States where the government is constantly putting efforts to deter cyber-crimes. The US government has recently reported a range of cyber-attacks on the Department of Defence against pharmaceutical companies, healthcare providers, and human services to hamper their efforts to fight against the COVID-19 pandemic and this attack was reported to be conducted by the Chinese government. This way, cyber security has been increasingly important to protect the national interest and **Nadikattu (2020)** provides notable insights and tools implemented for cyber security in the US.

### 1.1 1.3 Research Gap

Cyberattacks can happen anytime and cybercriminals can target anyone despite their financial and occupational backgrounds. To protect organizations and individuals, collective efforts are needed, and both the USA and Saudi Arabia have witnessed tremendous growth in a short period, especially in terms of technological advances, and that grabbed the attention of cybercriminals. This study attempts to analyses the existing cyber security practices in both countries and finds out the best algorithms to ensure cyber security.

### 1.2 1.4 Research Question

- What are the best algorithms used for cyber security?
- What are the cyber security practices in the US and Saudi Arabia?

### 1.3 1.5 Importance of the Study

There are so many issues due to which it became important to investigate the matters of cyber security in Saudi Arabia and the United States of America. It is very important to implement technology to deliver various services but protecting these technological solutions and citizens' data is equally important. A robust framework is very much needed for citizens to provide a lot of services and it should be protected for social welfare. This research is conducted to find out the best security practices and algorithms that organizations can use to prevent cyber-attacks in the future.

### 1.4 1.6 Research Objectives

- To recommend the best algorithms for cyber security
- To find out the cyber security practices and laws to prevent cyber-attacks in Saudi Arabia and the US
- To find out the cyber security practices and laws to prevent cyber-attacks in Saudi Arabia and the US

## 2. Research Methodology

### 2.1 Research Method & Design

To fulfill the above research objectives, we have conducted secondary research to find out the best security practices for the US and Saudi Arabia governments and policymakers. There are several algorithms widely used for ensuring cyber security by several organizations. There is a need to find out the best cyber security approach to prevent and deal with different kinds of cyber-attacks.

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

### 2.2 Research Approach

To answer the above research questions, we have found different research materials from various sources and explored earlier studies in the field of cyber security. There are so many studies in this field in various countries. The key here is to find relevant solutions for both countries so that they can work together to prevent cyber-attacks and ensure proper socio-economic growth.

### 2.3 Research Limitation

Governments like Saudi Arabia and the USA have understood the need of having complex frameworks for preventing cyber security risks and promoting socio-economic development. It is important to implement advanced systems to boost service delivery to citizens with a strong cyber security framework. Global governments should also invest in cyber security systems and infrastructure to ensure the steady growth of technological advances. Cyber threats lead to significant risks in e-government solutions.

To eliminate threats, associations are needed along with investments in cyber security practices. This research opens further research paths for exploring various options to implement those frameworks. The USA and UAE are working together to boost their cybersecurity practices but there is a lack of studies in their existing e-government practices. Hence, further studies are needed to find and fill the gap so that both countries can work together and secure cyber networks.

## 3. Analysis of Data

Malware, zero-day attack, denial of service (DoS), probe, sinkhole, phishing, adversarial, user root, evasive, poisoning, causative, and integrative attacks have been responsible to affect cyber security systems across the world over the past few decades. A lot of researchers have used the concepts of deep learning to detect such attacks. Before We discuss deep learning algorithms that can be used for cyber security, we analyzed various studies on cyber security attacks that have happened in the past and algorithms used for detection (Table 1).

**Table 1 – Cyber-attacks and algorithms used**

| Cyber Attack | Motive | Threat | Algorithms used | Source |
|---|---|---|---|---|
| Causative | To manipulate the algorithm's decision | Attack and Computational Complexity | Decision-Making | Sihag & Tajer (2020) |
| Spot Evasion | To create infected images replicating original ones | License Plate Identification System | Convolution Neural Network | Qian et al. (2020) |
| Integrity | To input fake intel to actuators | - | Cyber-physical | Wu & Sun. (2017) |
| Poisoning | To increase the risk of errors | not suitable for p-budget attacks | any algorithm which is ideal | Mahloujifar et al. (2020) |
| Poison and Evasion | Injecting virus to affect precise | Significantly decrease the accuracy | PSO, Deep Neural Network | Jiang et al. (2020) |

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

| | | | | |
|---|---|---|---|---|
| | classificati on | | | |
| Adversari al | To manipulate deep learning model to make errors | Safety-vulnerable applications | Deep Neural Network | Xu et al. (2020) |

[1]

**Source** – Dixit & Silakari (2021)

### 3.1. What are the best algorithms used for cyber security?

Deep learning is the most important aspect of machine learning and is classified as per the cyber security attacks mentioned above.

**Figure 1 classifies deep learning algorithms and their subcategories -**

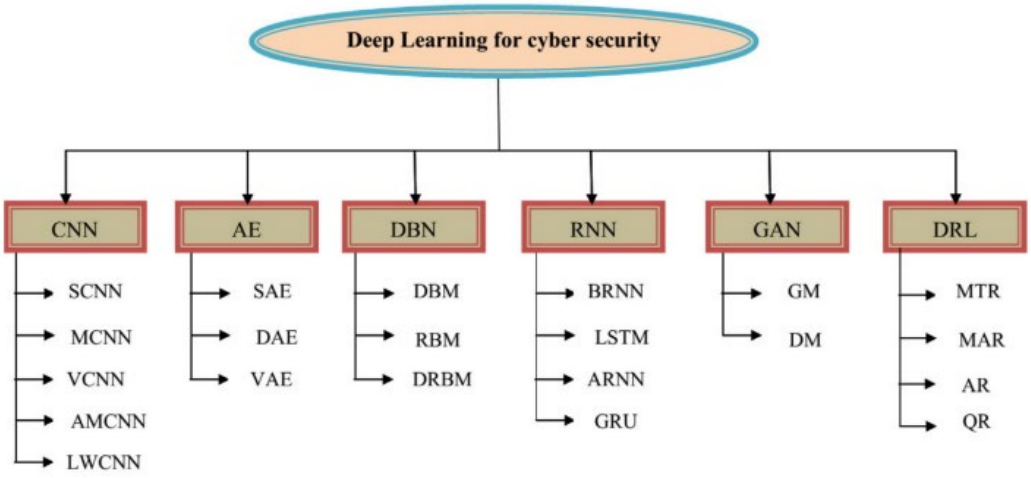


**Figure 1** – Deep Learning Algorithms and their classifications (Dixit & Silakari, 2021).

**3.1.1. Convolutional Neural Network (CNN)** –
This feed-forward algorithm consists of several hidden layers which are fully connected. The neurons are used for the elements and all the inputs are stored in an array. There are 2D and 3D arrays and the convolutional layer is the basic aspect of CNN (Li et al, 2019). The convolutional kernel is the original input which represents weight along with the receptive field (Li et al, 2015). The input is calculated to achieve the feature map. Figure 2 illustrates the overall structure of CNN. There are different subcategories of the CNN algorithm used for detecting cyber security attacks, i.e., single CNN (SCNN), variants of CNN (VCNN), Multi-CNN (MCNN), sharing Limited Weight of CNN (LWCNN), and Acoustic Model CNN (AMCNN).

3.1.2. **Autoencoder (AE)** –

It connects multiple hidden layers with output and input layers. It has the same amount of output and input along with carrying out data transmission with a smaller path. A neural network is used to resolve unsupervised learning and transfer problems.

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

Autoencoders are used for task analysis and discovery as per their characteristics (Baldi, 2012).

3.1.3. **Deep Belief Network (DBN)** –

The hidden and stochastic layer is a simple aspect of DBN. It can be implemented with stochastic variables using an acrylic graph (Mohamed et al, 2011). The discriminative and generative DBN can work as per greedy selection. Some of the major issues are learning and unobserved variables (Zhang et al, 2019). Figure 2 illustrates the structure of DBN.

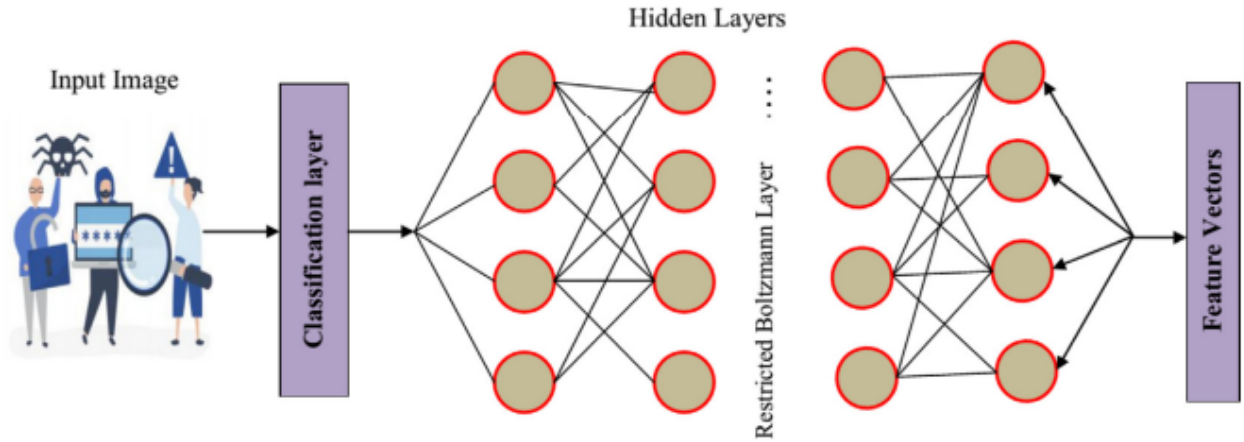


**Figure 2** – Structure of DBN (Dixit & Silakari, 2021)

**3.1.4. Recurrent Neural Network (RNN)** –

It is associated with multiple feedback connections, and it serves as loop activation. The network is enabled for performing temporal procedures and sequence learning (Papernot et al, 2016). The added loop is the fundamental part of RNN with Multilayer Perceptron and it has smaller memory. The stochastic function is activated with neurons and is potentially connected (Pascanu et al, 2015). The gradient function can be used for activation, learning, and architectural functions, and recurrent functions are combined with the annealing concept (Figure 3).

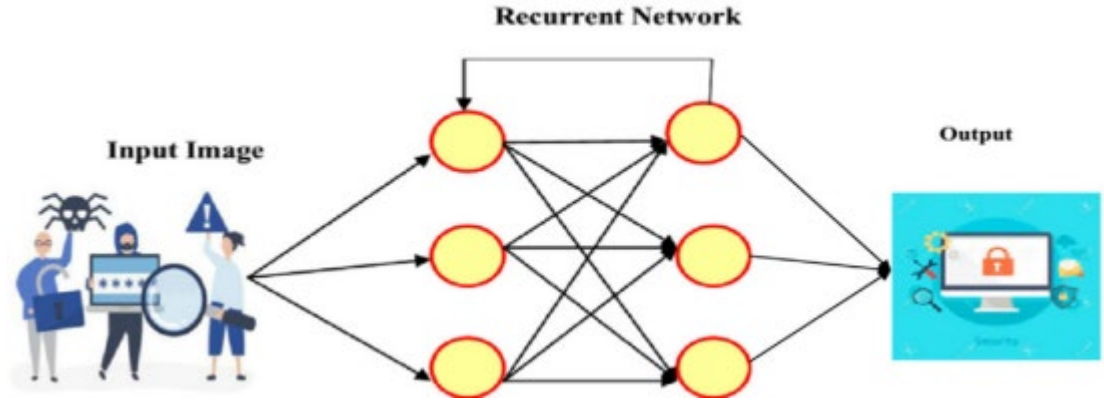


**Figure 3** – RNN Structure (Dixit & Silakari, 2021)

**3.1.5. Generative Adversal Network (GAN)** –

The discriminator and generator are key models, and it determines the tasks with the discriminator model along with producing the right output with the discriminator (Yang

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

et al, 2018). The artificial and real outputs and inputs are understood well with GAN while creating synthetic and quality data (Li et al, 2020). The discrimination process clarifies the fake and real data in the latent network. Hence, the key objective feature of GAN is the minimax theory (Xiao et al, 2018).

### 3.1.6. Reinforcement Learning (RIL) –

Mnih et al. (2016) were the first to introduce the concept of deep reinforcement learning and enhanced the cumulative rewards along with the basic concept of ML function. Deep neural networks minimize the high data sizes (Javaid et al, 2016). The multilayer perceptron implements A-functional values.

### 3.2. What are the cyber security practices in the US and Saudi Arabia?

Cybersecurity practices are developing constantly considering the increasing security threats. Some countries have prepared more resources to deal with cyber threats in a better way. According to the recent findings by Atlas VPN, the UK, US, and Saudi Arabia are committed to cyber-security, and they lead in first and second positions, while other countries still don't have proper education and training programs for professionals (William, 2021).

The International Telecommunication Unit (2020) has released Global Cybersecurity Index 2020 (GCI) and the commitment of each country is measured and the GCI score is given as per their technical, legal, capacity building, organizational, and corporation indicators.

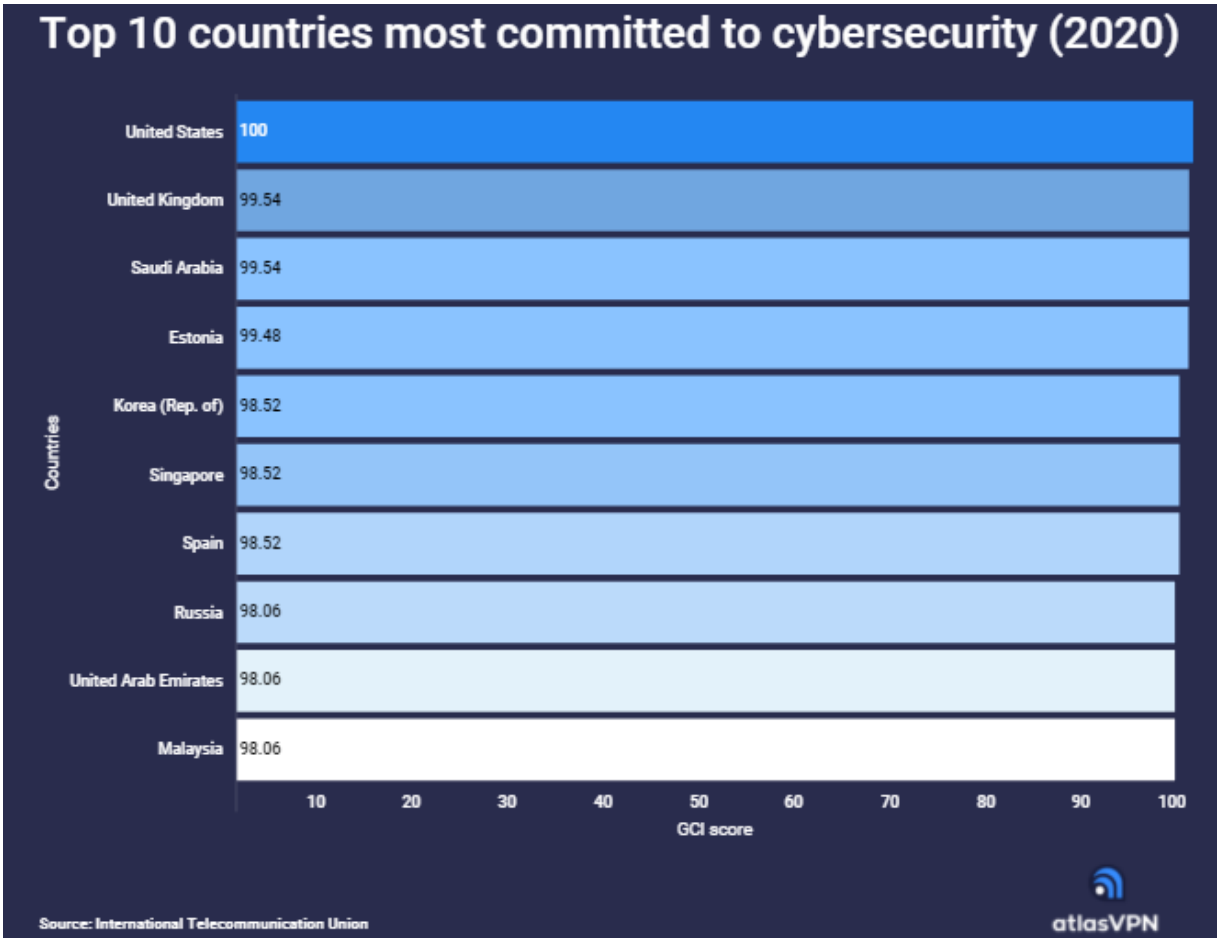


**Figure 4** – GCI Score of Countries Committed to Cybersecurity (Source: AtlasVPN)

The United States has achieved 20 out of 20 points in each indicator and scored a perfect 100. However, there are still more improvements needed considering the recent cyber-attacks on Americans. For

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

example, ransomware attacks initiated by Russian hackers exposed vulnerabilities on the supply chain. On the other side, Saudi Arabia stands just behind the US with 99.54 like the UK. Saudi Arabia is one of the fastest emerging markets which have focused highly on cyber security. They have come up with a national cyber security framework as part of their strategic plan to have a balance between trust, security, and growth.

Lack of awareness and training about cyber security is the main reason behind the rise of cyber-attacks. People could control the risks by providing more knowledge in this area. Only 46% of countries have successfully managed to provide specialized cyber security training to the government and public sector officials. These employees handle a lot of confidential and sensitive data. So, they must have proper training on creating a cyber-safe environment (Figure 5).

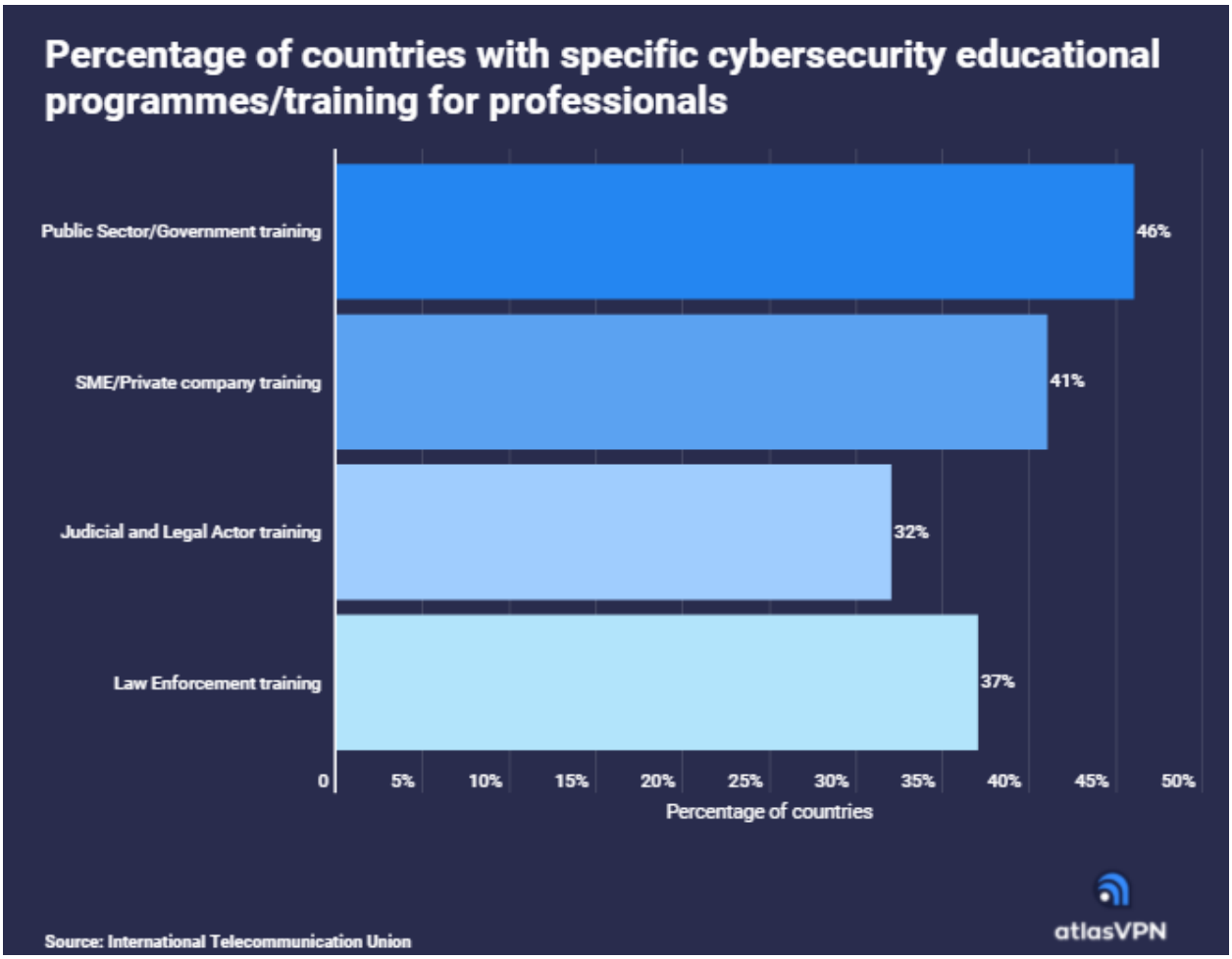


**Figure 5** – Countries managed to provide cybersecurity training (Source – atlas von)

Around 41% of nations provided private or SMEs with cybersecurity training. Hackers usually attack businesses as they can easily make money off ransomware attacks or stolen information. Though MNCs have cyber security experts, several smaller businesses cannot afford those experts. The leaders behind GCI can help address cyber-security issues in developing countries. They can reach more robust and balanced security over cyber threats with proper cyber security strategies.

## 4 - Results & Findings

Deep learning algorithms are widely used to detect various attacks and to handle them in a cybersecurity system. Cyber attackers can target anything or institutions like companies, banks, financial organizations, servers, computer networks, emails, vehicles, etc. Here, I discussed some of the most widely used deep learning algorithms to detect cyber threats. Considering the increasing level of cyber threats, US-based cyber security firm Quali and UAE-based Beacon Red have committed to collaborating for providing cyber security testing environments and cyber training to GCC countries. Mauricio De Almeida, Beacon

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

Red CEO has announced that they will provide joint cyber security services to all Gulf Corporation Countries like Kuwait, Qatar, and Saudi Arabia (Jo, 2021).

He further added that they will provide services related to cyber security to military, governments, and major infrastructure projects and each consumer can pick the right environment as per their needs. The companies can build sophisticated environments with physical and virtual features with training, intelligence, and cybersecurity provided by Beacon Red and automation of cloud infrastructure by Quali. Secure environments and scenarios will be developed for businesses to validate projects. However, there are no financial details about the strategic relationship revealed yet but huge stakes have been involved from both organizations. A sensitive environment needs to test new security services and conduct penetration and vulnerability tests and detonate software updates and malware attacks in a realistic and safe environment.

## 5- Conclusion and Future work

In the Middle East, companies have had a different range of challenges for a long time, considering some of the cyber-attacks in the past and recent days, i.e., from Stuxnet attack in Natanz nuclear facility in Iran to destructive attack in Saudi Aramco. Even the United States suffered DoS attacks against eight of the most important financial institutions. It goes without saying that both the United States and Saudi Arabia should work together in policy and operational levels to deal with these threats because the internet is borderless and cybersecurity needs are multi-dimensional. Along with the governments of both countries, companies should also consider some important workforce issues. In future work, we need to hire the right candidates who are responsible for information security. Educational programs must be developed for IT departments and training must be administered on best security practices and cyber threats. The Internet knows no international boundaries and so are the cyber attackers. Hence, this article has suggested some of the best cyber security practices the US and UAE are following and deep learning algorithms that can be used against cyber-attacks. Cyber security is one of the most discussed domains in emerging economies considering the analyses of cyber security practices and laws in the US and UAE. Cyber security requires counties to be strict against emerging online threats with rapid technological advances while correcting the loopholes in cyber laws. Meanwhile, only national laws are not sufficient for cross-border cyber terrorism, conflicts, and frauds as the internet is a borderless platform. A basic international framework is the need of the hour, and it is important to practice a uniform cyber law rather than determining jurisdictions. These two countries have made cognizant efforts in cyber safety as the first step towards international cooperation to fight against cyber threats.

## References

**[1]** The White House (2018). *National Cyber Strategy for the USA*. Retrieved https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

**[2]** Craig, L. (2006). S.3421 – 109th Congress (2005-2006*): Veterans Benefits, Health Care, and Information Technology Act of 2006.* Retrieved from https://www.congress.gov/bill/109th-congress/senate-bill/3421.

**[3]** Is the Computer Fraud and Abuse Act Ripe for Reform? - Charles Koch Institute. (2016). Retrieved 21 September 2021, from https://charleskochinstitute.org/stories/is-the-computer-fraud-and-abuse-act-ripe-for-reform/.

**[4]** McCaul, M. (2018, November 16). H.R.3359 – 115th Congress (2017-2018): Cybersecurity and Infrastructure Security Agency Act of 2018. Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3359.

**[5]** Mansoor, Z. (2020). Four of five organizations in UAE faced at least one 'cyber-attack' in 2019 - study. Retrieved 21 September 2021, from https://gulfbusiness.com/four-of-five-organisations-in-uae-faced-at-least-one-cyber-attack-in-2019-study/.

**[6]** Sanderson, D. (2020). *Coronavirus: Cybercriminals launch Covid-19 attack barrage.* Retrieved from https://www.thenationalnews.com/uae/coronavirus-cyber-criminals-launch-covid-19-attack-barrage-1.1009181

**[7]** Nuaimi, A. A. (2021). Effectiveness of Cyberbullying prevention strategies in the UAE. In *ICT Analysis and Applications* (pp. 731-739). Springer, Singapore.

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

**[8]** Alzubaidi, A. (2021). Measuring the level of cyber-security awareness for cybercrime in Saudi Arabia. *Heliyon*, *7*(1), e06016.

**[9]** Alrubaiq, A., & Alharbi, T. (2021). Developing a Cybersecurity Framework for e-Government Project in the Kingdom of Saudi Arabia. *Journal of Cybersecurity and Privacy*, *1*(2), 302-318.

**[10]** Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *Available at SSRN 3624487*.

**[11]** Nadikattu, R. R. (2020). New Ways of Implementing Cyber Security to Help in Protecting America. *Journal of Xidian University*, *14*(5), 6004-6015.

**[12]** Dixit, P., & Silakari, S. (2021). Deep learning algorithms for cybersecurity applications: A technological and status review. *Computer Science Review*, *39*, 100317.

**[13]** Sihag, S., & Tajer, A. (2020). Secure estimation under causative attacks. *IEEE Transactions on Information Theory*, *66*(8), 5145-5166.

**[14]** Qian, Y., Ma, D., Wang, B., Pan, J., Wang, J., Gu, Z., ... & Lei, J. (2020). Spot evasion attacks: Adversarial examples for license plate recognition systems with convolutional neural networks. *Computers & Security*, *95*, 101826.

**[15]** Wu, G., & Sun, J. (2017). Optimal switching integrity attacks in cyber-physical systems. In *2017 32nd Youth Academic Annual Conference of Chinese Association of Automation (YAC)* (pp. 709-714). IEEE.

**[16]** Mahloujifar, S., Diochnos, D. I., & Mahmoody, M. (2020). Learning under p-tampering poisoning attacks. *Annals of Mathematics and Artificial Intelligence*, *88*(7), 759-792.

**[17]** Jiang, W., Li, H., Liu, S., Luo, X., & Lu, R. (2020). Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles. *IEEE transactions on vehicular technology*, *69*(4), 4439-4449.

**[18]** Xu, H., Ma, Y., Liu, H. C., Deb, D., Liu, H., Tang, J. L., & Jain, A. K. (2020). Adversarial attacks and defenses in images, graphs, and text: A review. *International Journal of Automation and Computing*, *17*(2), 151-178.

**[19]** Li, D., Deng, L., Gupta, B. B., Wang, H., & Choi, C. (2019). A novel CNN-based security guaranteed image watermarking generation scenario for smart city applications. *Information Sciences*, *479*, 432-447.

**[20]** Li, Y., Ma, R., & Jiao, R. (2015). A hybrid malicious code detection method based on deep learning. *International Journal of Security and Its Applications*, *9*(5), 205-216.

**[21]** Mohamed, A. R., Dahl, G. E., & Hinton, G. (2011). Acoustic modeling using deep belief networks. *IEEE transactions on audio, speech, and language processing*, *20*(1), 14-22.

**[22]** Baldi, P. (2012). Autoencoders, unsupervised learning, and deep architectures. In *Proceedings of ICML Workshop on unsupervised and transfer learning* (pp. 37-49). JMLR Workshop and Conference Proceedings.

**[23]** Zhang, J., Qin, Z., Yin, H., Ou, L., & Zhang, K. (2019). A feature-hybrid malware variants detection using CNN-based opcode embedding and BPNN based API embedding. *Computers & Security*, *84*, 376-392.

**[24]** Papernot, N., McDaniel, P., Swami, A., & Harang, R. (2016). Crafting adversarial input sequences for recurrent neural networks. In *MILCOM 2016-2016 IEEE Military Communications Conference* (pp. 49-54). IEEE.

**[25]** Pascanu, R., Stokes, J. W., Sanossian, H., Marinescu, M., & Thomas, A. (2015). Malware classification with recurrent networks. In *2015 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)* (pp. 1916-1920). IEEE.

**[26]** Yang, J., Liu, K., Kang, X., Wong, E. K., & Shi, Y. Q. (2018). Spatial image steganography based on generative adversarial network. *arXiv preprint arXiv:1804.07939*.

**[27]** Li, S., Ye, D., Jiang, S., Liu, C., Niu, X., & Luo, X. (2020). Anti-steganalysis for an image on convolutional neural networks. *Multimedia Tools and Applications*, *79*(7), 4315-4331.

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30

**[28]** Xiao, D., Huang, Y., Zhang, X., Shi, H., Liu, C., & Li, Y. (2018). Fault diagnosis of asynchronous motors based on LSTM neural network. In *2018 prognostics and system health management conference (PHM-Chongqing)* (pp. 540-545). IEEE.

**[29]** Mnih, V., Badia, A. P., Mirza, M., Graves, A., Lillicrap, T., Harley, T., ... & Kavukcuoglu, K. (2016, June). Asynchronous methods for deep reinforcement learning. In *International conference on machine learning* (pp. 1928-1937). PMLR.

**[30]** Javaid, A., Niyaz, Q., Sun, W., & Alam, M. (2016). A deep learning approach for network intrusion detection system*s. EAI Endorsed Transactions on Security and Safety*, *3*(9), e2.

**[31]** International Telecommunication Union. (2020). *Global Cybersecurity Index 2020*. ITU Publications. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf.

**[32]** William S. (2021). Study: US, UK, and Saudi Arabia lead in commitment to cybersecurity - Atlas VPN. Retrieved 26 September 2021, from https://atlasvpn.com/blog/study-us-uk-and-saudi-arabia-lead-in-commitment-to-cybersecurity.

**[33]** Jo, H. (2021). Can the UAE emerge as a leading global defense supplier? Retrieved 26 September 2021, from https://www.defensenews.com/digital-show-dailies/idex/2021/02/15/can-the-uae-emerge-as-a-leading-global-defense-supplier/

DOI: https://doi.org/10.54216/JISIoT.050202
Received: September 17, 2021 Accepted: November 30