Security Policy Papers
Volume 1, Issue (1), 2021, https://nauss.edu.sa

أوراق السياسات الأمنية
http://spp.nauss.edu.sa/spp

جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
Est. 1978

رؤى أمنيـة

سياسة الأمن والخصوصية في العالم العربي

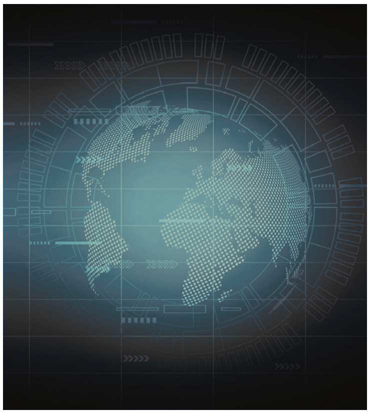
Security and Privacy Liability Policy in the Arab World

Kyounggon Kim
Department of Forensic Sciences, College of Criminal Justice, Naif Arab University for Security Sciences

كيونغون كيم
قسم الأدلة الجنائية، كلية العدالة الجنائية
جامعة نايف العربية للعلوم الأمنية

key massages:

- Focusing on Cooperation, Capability, and Assessment (ACC) approach performed in top-down, bottom-up, short-term, and long-term (TBSL).
- Cooperation between countries is essential to proactively respond to various cyber threats such as cyber criminals and cyber terrorists and to show rapid recovery resilience.
- Develop a cybersecurity evaluation model and a gap analysis model, and spread them to the remaining Arab countries.



1. The Digital Arab World: Inevitable trends and new opportunities

Many Arab countries are implementing digital transformation strategies at the national level to quickly adapt to the changes of the times. According to the Salem, Fadi [(1)], 41% of Internet users in the Arab region answered that the proportion of using government services through the Internet is gradually increasing. Monthly online spending rose from 2.7 billion dollars in 2015 to 7.3 billion dollars in 2017. More than 92% of respondents said they engage in online social activities every month. Smartphone users in the Arab region, which account for 98% of respondents, said they were constantly using at least one social media app, and 91% were using Internet messenger apps. Regardless of gender and age group, Arab users' use of social network services is far higher than that of other regional countries.

Many countries in the Arab world have open data and digital governments. The transition to digital government in the Arab region is huge and complex. Most of the traditional face-to-face services are provided through online channels. From public contracts to complex decision making, we are providing more advanced government services by using big data. 82% of respondents said that the availability of data provided by the government is very important. With the Open Government, users of Arab countries are making interactions with their governments easier and more convenient.

Saudi Arabia is undergoing a transformation into a digital nation as part of its national strategy, Saudi Vision 2030 program. With the catchphrase Digital Saudi, “National Digital Transformation” is in progress (2). Recently, in relation to COVID-19, it is building digital transformation that is much more advanced than other countries, such as testing through mobile apps and applying for vaccines.

As part of this effort, Saudi Arabia ranked 1st in Business environment reforms evaluated by The World Bank, ranked 11 in Legal framework’s adaptability to digital business models evaluated by WEF, and Ranked 13 in the Digital Capacity Index conducted by WEF. According to the Global Competitiveness Report 2019, UAE ranks 25th, Saudi Arabia ranks 36th, Qatar ranks 29th, Bahrain ranks 45th, Kuwait ranks 46th, 53rd in Oman, Jordan 70, Morocco 75, Tunisia 87th, Lebanon 88th, Algeria 89th, 93rd in Egypt, and Yemen 140th. On the other hand, many countries in Europe and Asia show a fairly high level, with Singapore at first, 2nd place is the United States, 3rd place Hong Kong, 4th place Netherlands, 5th place Switzerland, 6th place Japan, 7th place Germany, 8th place Sweden, 9th place United Kingdom, and 10th place Denmark (3).

In this way, countries in the Arab world are undergoing digital transformation in many areas, including government services, to communicate more effectively with their citizens. However, the world on which digital transformation is based is the cyber world. If reliability and stability in the cyber world are not guaranteed, the digital society is bound to become an unstable society.

2. Cyber threats in the Arab World

As Internet users increase and change to a digital society, crimes that disturb the existing social order are naturally occurring on the Internet and digital society. According to Salem Fadi (3), the top five most concerned Internet users in the Arab region. Over 40% of users cited these threats as “very concerned”. Cyberterrorism is one of the biggest concerns in the Arab region. 81% of Internet users in the Arab region are concerned about cyberterrorism.

75% of Internet users in the Arab region express online cybercrimes as their second major concern. About 75% of users reported experiencing at least one cyber threat in the past two years (2015-2017).

With the Fourth Industrial Revolution discussed at the World Economic Forum, digital transformation is going more powerfully around the world. The UN 2030 Agenda of Sustainable Development, for example, states that these digital technologies are quite essential to

Technology cluster	Crucial emerging technology for the SDGs until 2030	Opportunities in all SDG areas, including:	Potential threats, including
Digital – tech	Big Data technologies; Internet of Things; 5G mobile phones; 3-D printing and manufacturing; Cloud computing platforms; open data technology; free and opensource; Massive open online courses; micro-simulation; E-distribution; systems combining radio, mobile phone, satellite, GIS, and remote sensing data; data sharing technologies, including citizen science- enabling technologies; social media technologies; mobile Apps to promote public engagement and behavioural change; prepaid system of electricity use and automatic meter reading; digital monitoring technologies; digital monitoring technologies; digital security technology.	Development, employment, manufacturing agriculture, health, cities, finance, absolute “decoupling” governance, participation, education, citizen science, environmental monitoring, resource efficiency, global data sharing, social networking and collaboration,	Unequal benefits, job losses, skills gaps, social impacts, poor people priced out; global value chain disruption; concerns about privacy, freedom and development, cyber- attacks

Figure 1. *Crucial emerging technology for the SDGs until 2030 and Potential threats.*

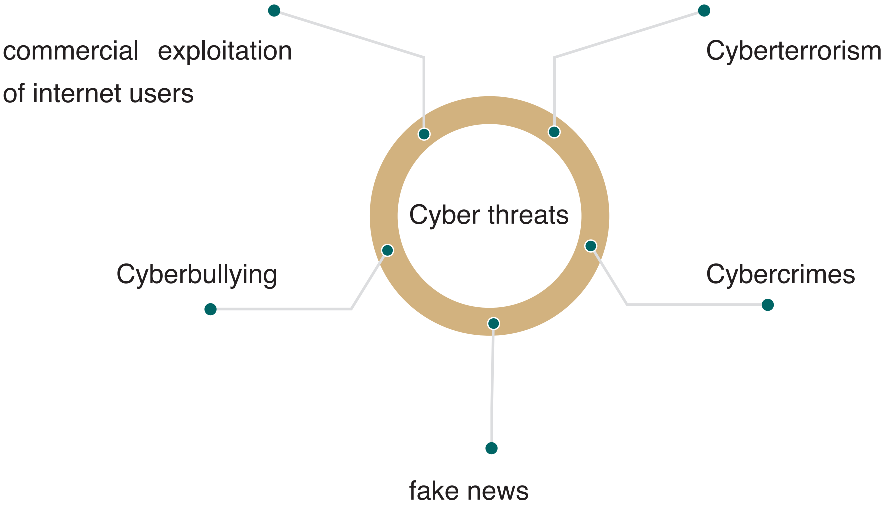
achieving SDG goals [4]. However, the UN also highlights some of the threats and risks arising from digital transformation. According to Figure 1, threats to go to Digital Tech include concerns about privacy, data fraud, theft, and cyber-attacks.

top five most concerned Internet users in the Arab region

There are many actors who disturb the security of the digital society. To keep cyberspace safe, it needs to know about cyber attackers. Cyber attackers have a variety of actors, from curious script kids to cyber terrorists, cyber criminals, and state-sponsored hackers. Cyber threat actors are threatening cyberspace in a wide range from financial gains to the destruction of national digital infrastructure networks.

In Sameh Aboul-Enein's paper (5), the importance of cyberwarfare and doctrines is recognized from the perspective of global military power, and many countries are reinforcing these capabilities (6). Non-state actors are also becoming very familiar with exploiting cyber vulnerabilities. Advances in cyberwarfare and offensive cyber technologies are further fueling this competitive environment. The relevance of existing international humanitarian laws on the use of force in cyberspace, and the obligations of states and international institutions to do so, are becoming ever greater. Sameh Aboul-Enein describes it mentions the different economic levels of countries in the Middle East, and thus the limitations of resources to counter cybercrime and cyber terrorism. It also emphasized the importance of internet gender gap and education. He emphasized the need for ICT education and the enactment of cyber-related laws to better respond to cyber terrorism and cybercrime. He noted that Arab stakeholders should strengthen the cybersecurity culture for individual, national, and international security.

According to data (5), the losses to the national economy and corporations due to cybercrime are increasing very significantly. In December 2020, FireEye was attacked, causing corporate stock prices to plummet, and critical information related to national security was leaked. The countries in the MENA region are at the top of the international financial crime statistics (7). These statistics indicate that about 63% of business enterprises in the region are exposed to economic cybercrime. A more serious problem is that, according to a 2016 survey by PricewaterhouseCoopers (PwC), about 21% of respondents did not even know that their organization was harmed by Cybercrime. 42% of respondents said that these cyberattacks have caused high- or medium-level damage to their business reputation. According to a survey by PwC, financial losses incurred by cyberattacks and cybercrime in the MENA region amounted to US$5 millon-100 million dollars (7).



According to a report published by the UN Broadband Commission, 75 per cent of women experienced cyber violence online (8). Online abuses for women include hate speech, hacking, identity theft, and online stalking, and human trafficking.

Terrorist organizations and non-states actors are using cyber technology as propaganda tools for their goals. Because cyberspace is highly anonymous, it is difficult to trace the origin of the attacker. Cyber terrorist organizations heavily use cyber tools to recruit young people by exploiting anti-establishment sentiments. State-sponsored attacks are consistent with political, social, and military gains [9]. Gauss, a complex cyber-espionage toolkit, conducted cyber-attacks against financial institutions in Lebanon, and Flame was used to cyber-espionage against private institutions and universities in Syria, Lebanon, and Saudi Arabia [10]. These tools could turn on the camera on the victim›s device, intercept conversations or keyboard input.

we propose focusing on Cooperation, Capability, and Assessment (ACC) approach as shown in Figure 2.

As such, many serious damages have occurred in individuals, companies, and countries from various and organized cyber-attacks such as cyber criminals and cyber terrorists. Sometimes simple but high-impact cyber threats also arise. Although many efforts are being made to cope with such cybercrimes and cyber threats such as cyber terrorists, there is still a lack of systematic strategies and policies to prevent and respond to them. Therefore, in the Arab world, cyber diagnosis at the national level is necessary to protect the cybersecurity and important information of citizens, companies, and countries from various cyber threat actors. In addition, cooperation from Arab countries and systematic cyber security talent training are needed.

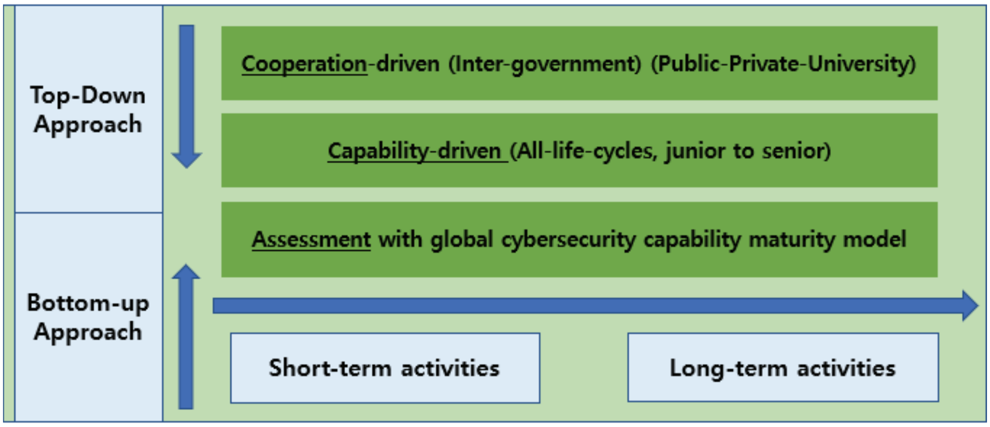

Top-Down Approach
Bottom-up Approach
Cooperation-driven (Inter-government) (Public-Private-University)
Capability-driven (All-life-cycles, junior to senior)
Assessment with global cybersecurity capability maturity model
Short-term activities
Long-term activities

Figure 2. *Proposed approach (CCA + TBSL).*

3 Recommendations for secure in the Arab World

People in the Arab world are now getting used to the Internet and digital society, and the government is becoming a country and region that grows one step further with the change to a digital society. In addition to this, cyber threats are also increasing, so to keep the Arab world safe and peaceful from various cyber threats, we propose focusing on Cooperation, Capability, and Assessment (ACC) approach as shown in Figure 2. Additionally, this method can be performed in top-down, bottom-up, short-term, and long-term (TBSL)

3.1 Cooperation-driven (Top-Down approach)

Cyber threat actors have no national boundaries. Cyber-attacks do not occur only in one country, but often occur simultaneously in multiple countries. Cooperation between countries is essential to proactively respond to various cyber threats such as cyber criminals and cyber terrorists and to show rapid recovery resilience.

The United States and Europe established the North Atlantic Treaty Organization (NATO) in 1949 and are engaged in joint military response activities. In 2007, in Tallinn, Capital of Estonia, as the national infrastructure collapsed due to a cyber-attack, it became clear that cyberattacks were a serious threat to the country. Later, in 2008, the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE) was created to form a joint cybersecurity cooperative organization against cyberattacks [11]. NATO CCDCOE continuously conducts exchanges and joint research with experts through CyCon in Tallinn, Estonia every year.

There are five areas of Maturity Models. D1. Cybersecurity Policy and Strategy, D2. Cyber Culture and Society, D3. Cybersecurity Educations, Training and Skills, D4. Legal and Regulatory Framework, and D5. Standards Organizations and Technology (13).

The European Union issued a joint statement in 2017 entitled “Resilience, Defense and Defense: Building strong cybersecurity for the EU.” Through a joint statement, EU countries are promoting activities such as strengthening the European Union’s level of resilience against cyber-attacks, strengthening detection capabilities against cyber-attacks, and strengthening international cooperation on cyber security [12]. For these activities, the European Union has secured its position as the European Union Agency for Cybersecurity (ENISA), a specialized cybersecurity agency, and has forced ENISA to carry out various cybersecurity activities in the European Union.

. Since the creation of the Arab League in 1945, exchanges between Arab countries have been continuing. Through the Arab League of 22 Arab countries, organizations such as the EU’s ENISA and NATO’s CCDCOE should strengthen organizations that lead research and practice on cybersecurity.

3.2 Assessment with global cybersecurity capability maturity model (Bottom-up approach)

The cybersecurity of the Arab world requires a meticulous assessment of the current situation above all else. It is difficult to effectively allocate time and financial support without specific details on which cyber threat actors and which assets should be protected. Therefore, it is necessary to proceed with accurate assessment with a bottom-up strategy. We must find what is missing and fill the gap. This requires a full National and Regional Cybersecurity Assessment. Areas such as policy, people, process, and technology should be assessment. It should be systematically assessment through a joint cybersecurity research and cooperation between the Arab countries mentioned above. There are two approaches for National and

Regional Cybersecurity Assessment.

The first is to assess with a well-known model. The second method is to develop a customized Cyber Security Capability Maturity Model based on the characteristics of the Arab world, distribute it to Arab countries, receive opinions, and develop continuously.

Develop a cybersecurity evaluation model and a gap analysis model, and spread them to the remaining Arab countries, and a joint peace and cybersecurity system should be built. Through this, it is possible to reduce the risk of cyber terrorism and cybercrime, and to prevent and respond more rapidly

Through this, it is possible to assess the current cybersecurity status of Arab countries, to suggest ways to go further, and to continuously monitor and manage.

Among the known models, there is the Cybersecurity Capability Maturity Model for Nations made by the United Nations.

There are five areas of Maturity Models. D1. Cybersecurity Policy and Strategy, D2. Cyber Culture and Society, D3. Cybersecurity Educations, Training and Skills, D4. Legal and Regulatory Framework, and D5. Standards Organizations and Technology (13).

Based on this, each country should establish a cybersecurity national strategy, and the national strategy should be aligned with the common values of Arab countries.

There is also an evaluation and analysis method according to the Global Cybersecurity Index developed by ITU-T (14). The UK also created the Global Cyber Security Capacity Center (GCSCC) to develop, evaluate and manage indicators (15).

Organizations are needed to measure, evaluate, and continuously manage this way. In addition, it is necessary to make efforts to grow one step further through the evaluation between Arab countries, and through workshops and exchanges of various experts in areas that are mutually insufficient. As the GCSCC evaluation model was also developed by a group of 50 experts, it is necessary to gather experts from Arab countries to create a national cybersecurity maturity evaluation model that fits the characteristics of Arab countries. In the U.S., President-elect Joe Biden has invested $9 billion to strengthen U.S. cybersecurity capabilities, strengthening the work of the U.S. Cybersecurity and Information Security Administration (CISA) and expanding security upgrades across the federation.

Since the Arab world has a large difference in economic level between countries, leading countries in the Arab world are led by sharing Digital Transformation, Cyber Security policy, strategy, evaluation, and diagnosis with Arab countries and helping them grow and develop together. For joint cybersecurity and peace in 22 Arab countries, more advanced Arab countries first preemptively.

In cybersecurity, the balance of hard power and soft power is essential

3.3 Assessment with global cybersecurity capability maturity model (Bottom-up approach)

In cybersecurity, the balance of hard power and soft power is essential. Human Capital skills are crucial in Soft Power. Cybersecurity problems cannot be resolved in a short period of time and will continue to arise in the future. Therefore, it is necessary to train cyber security experts to strengthen cyber security capabilities. It is not a short-term approach to nurturing talent, but a mid- to long-term and continuous approach. From infancy to undergraduates, masters, doctors, and specialized companies, education and training must be conducted to cultivate manpower and to continuously strengthen competence. And such training should be developed and carried out in accordance with the cybersecurity strategy of not only individual Arab countries, but also the Arab world.

To cultivate cyber experts, it is necessary to train men and women together for the entire life cycle. In addition to nurturing the currently required experts, investments should be made nationally to nurture the next generation of cybersecurity experts. Many countries are creating programs to train the next generation of cybersecurity leaders at the national level. Representatively, there is Korea's Best of the Best (BoB) program. Students who have completed the BoB program have won the World Hacking Competition DEFCON twice. And for such a program, it is necessary to make cybersecurity experts into a mentor pool and share the experiences and knowledge of seniors in an apprenticeship through a mentoring system.

In addition to nurturing human resources, the cybersecurity private market should be expanded, and efforts should be made to foster start-ups and large corporations. The private sector should be developed so that human resources can work creatively as well as the government period in which they can work after receiving education and training. And these private sectors and the government should work together to protect cybersecurity and security.

4. Conclusion

The number of people in the Arab world who participates on the Internet is constantly increasing, and Arab countries are gradually moving towards a digital society through digital transformation. In addition, the digital society will further become a smart society. In a smart society, the development of a smart city such as a smart factory, a smart home, and smart mobility is inevitable. Now, The Arab world is rapidly entering the Internet and digital society. Accordingly, many threats are occurring together. To maintain the security and peace of the Arab world from various cyber threat actors such as cyber criminals and cyber terrorists, close cooperation between Arab countries is necessary.

the boundary line between the physical and cyber worlds is blurred, and an era in which the two worlds are united is approaching. In this new world, it is difficult to guarantee the success of the digital society unless the reliability of cybersecurity is guaranteed.

Reference

1. Salem, Fadi. “The Arab World Online 2017: Digital transformations and societal trends in the age of the 4th industrial revolution.” (2017).
2. National Digital Transformation Annual Report 2019, https://ndu.gov.sa/report/ndu-annual-report-en.pdf
3. Klaus Schwab, The Global Competitiveness Report 2019, World Economic Forum,http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf
4. Transforming our world: the 2030 Agenda for Sustainable Development, https://sdgs.un-.org/2030agenda
5. Sameh Aboul-Enein, Cybersecurity Challenges in the Middle East, GenevaPapers, 2017.
6. Ji-Young, Kong, Lim Jong In, and Kim Kyoung Gon. “The All-Purpose Sword: North Korea’s Cyber Operations and Strategies.” In 2019 11th International Conference on Cyber Conflict (CyCon), vol. 900, pp. 1-20. IEEE, 2019.
7. J. Tebbs, Adjusting the Lens on the Economic Crime in the Arab World, PwC, 2016, http://www.pwc.com/m1/en/publications/documents/economic-crime-in-the-arabworld-2016.pdf
8. UN Broadband Commission for Digital Development, Cyber Violence against Women and Girls: A World-wide Wake-up Call, 2015, http://www2.unwomen.org/~/media/headquar-

ters/attachments/sections/library/publications/2015/cyber_violence_genderreport.pdf?v=1&d=20150924T154259

9. Kim, Kyoung-gon. “” State-Sponsored Hacker and Changes in hacking techniques.” (2017).

10. T. Hamid, “Cyber Warfare in the Middle East Is No Game”, The National, 2012, http://www.thenational.ae/business/industry-insights/technology/cyber-warfare-in-the-middleeast-is-no-game

11. Healey, Jason, and Leendert Van Bochoven. Nato’s Cyber Capabilities: Yesterday, Today, and Tomorrow. Atlantic Council of the United States, 2012.

12. Resilience, Deterrence. “Defence: Building strong cybersecurity for the EU: adopted by the European Commission on 13 September 2017/European Union.” URL: https://eur-lex.europa.eu/legalcontent/EN/TXT.

13. Barclay, Corlane. “Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2).” In Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards?, pp. 275-282. IEEE, 2014.

14. Index, ITU Global Cybersecurity. “URL: https://www.itu.int/en/ITU-D/Cybersecurity.” Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2. pdf (data obrashcheniya: 12.04. 2019) (2018).

15. Bada, Maria, Ivan Arreguin-Toft, Ian Brown, Paul Cornish, Sadie Creese, William H. Dutton, Michael Goldsmith et al. “Cybersecurity Capacity Review of the United Kingdom.” Global Cyber Security Capacity Centre, University of Oxford (2016).

Received 1 Jan. 2021; Accepted 15 Feb. 2021; Available Online 31 Mar. 2021.

Production and hosting by NAUSS

* Corresponding Author: Kyounggon Kim
Email: kkim@nauss.edu.sa

doi: 10.26735/OUTI8333