The OIC-CERT 5G Security Framework
Bracing for What's Coming

Ts Mohd Shamir bin Hashim
Cybersecurity Malaysia, Permanent Secretariat of the OIC-CERT
Co-chair, OIC-CERT 5G Security Working Group

The fifth generation (**5G**) wireless technology represents a complete transformation of the telecommunication networks that will be able to cater for the demand from the emerging and disruptive technologies such as Artificial Intelligence (**AI**), Internet of Things (**IoT**), and Cloud computing, to name a few. These technologies will be craving for bandwidth to enable new applications usage where 5G will transform the digital landscape and serve as a catalyst for innovation, new markets, and economic growth. In fact, 5G will be critical towards the realisation of the Fourth Industrial Revolution (**4IR**) where billions of devices will be connected to the Internet through this technology It is predicted that 5G networks will have more than 1.7 billion subscribers worldwide by 2025 [1].

The society today does not have a choice with these emerging technologies but to embrace and adopt them or risk being left behind by the rest of the world. Countries that are slow in adopting will move to the bottom of the food chain and left at the mercy of others. In the world that is moving towards interconnectivity, the security risk lies at the weakest link in which it would be the interest of all parties to ensure every link has taken the minimum security endeavour to protect, in this case, digital data transmission and management.

The 5G digital transformation will continue to introduce new dimensions of attack vectors, surfaces, and vulnerabilities through the connected digital systems. The IoT, for example, will bring a new set of issues, such as the security, safety, and robustness of the cyber and physical systems. Novel types of attack will bring new challenges to the industry by surprise. As such, more and more targets will be attractive and easy to be approached by the cyber criminals thus the need to enhance the cybersecurity to commensurate the threats that existed due to the development in digital technologies.

Since the dawn of cybersecurity, inter border collaboration has always been a pillar in mitigating cyber threats. One of this collaboration is the Organization of the Islamic Cooperation- Computer Emergency Response Team (**OIC-CERT**), which is a platform for information sharing and development of cybersecurity capabilities for the members [2]. The OIC-CERT is an affiliate institution of the Organization of the Islamic Cooperation (**OIC**) and more information on this collaboration can be found at *www.oic-cert.org/en/*.

The OIC is said to be the second largest organization after the United Nations with 57 member countries. This many countries under one umbrella would be a good opportunity for digital interconnectivity but lacking in cybersecurity is a great concern and might hamper the roll out of technologies such as 5G to accommodate future development. Base on the International Telecommunication Union Global Cybersecurity Index (**ITU GCI**) 2020 [3] which measure the cybersecurity commitment of 194 countries, only 4 OIC Member Country (**OMC**) are ranked in the global top 20 while 27 falls under the 100 and below position. Therefore, it seems that almost half of the OMC is at the bottom in cybersecurity commitment.

This raises the question on how to elevate the capability and capacity of cybersecurity and digital technology among the OMC. How are these members going to keep up in embracing the emerging technologies such as the 5G?

The OIC-CERT was formed in 2009 to offer cybersecurity assistance to the OMC. Presently 28 of the OMC are members of the OIC-CERT. From the ITU GCI 2020 report, the 4 OMC ranked in the global top 20 are also members of the OIC-CERT. Focusing just to the OIC community, 18 OMC in the top 20 of OIC members are OIC-CERT members. Thus, the OIC-CERT can be an avenue for the OIC to elevate the cybersecurity capability and capacity of OMC to prepare them for the 5G and other disruptive digital technologies.

The OIC-CERT recognize that 5G marks the beginning of a new era and at the same time bringing in cybersecurity challenges to a successful 5G transformation. Thus, to face some of these challenges, the OIC-CERT has established the OIC-CERT 5G Security Working Group (**WG**), led by CyberSecurity Malaysia and Huawei UAE who are the OIC-CERT Secretariat and a Commercial Member respectively, to look at formulation a 5G cybersecurity framework that is systematic and effective as a foundation under the situation of rapid ICT development. This framework is mainly intended for the regulatory authorities of the OMC, with the purpose of assisting them in making policies on regulating 5G equipment vendors, mobile network operators (**MNO**s), and the relevant service providers.

The OIC-CERT 5G Framework clarify the different 5G cybersecurity areas, roles, and responsibilities. The WG, with the contribution from Huawei UAE, has developed an OIC-CERT 5G cybersecurity risk repository identifying the exact cybersecurity requirements to address 5G cybersecurity concerns. Considering the difference level of cybersecurity capabilities among the OMC, the framework and security requirements are designed to provide a baseline foundation, which can be individually customised to provide guidance to each OMC in regulating their 5G cybersecurity requirements.

It is unrealistic to build and maintain secure and resilient 5G networks, application services, and ensuring trustworthy network equipment through an all-in-one solution. In addition, it cannot be achieved by one person, one organization, or one nation. All parties involved need to work together in addressing the challenges that arises. With the aim to establish the cybersecurity requirements for the OIC community to securely adopt new technologies, the OIC-CERT intend to announce the formation of the 5G Security WG at the GISEC Global 2022 Dubai, UAE in May 2022. To date, the WG has completed the technical development of the framework with the following major components:

1. The OIC-CERT 5G Risk Repository
   The repository provides a risk based approach towards 5G security in the framework. The repository will be used for risk assessment and management of the 5G security risks in information security works where it will include industry consensual threat landscape, attack methodologies, mitigation strategies, and measures for different stakeholders such as the MNOs, network equipment vendors, application providers, and regulators

2. The Baseline Security Technical Specifications and Reference Standards
   A tiered 5G security framework is defined to address the 5G security that also defined a

layered security model to explicitly distinguish roles and responsibilities in securing the 5G equipment, networks, and various applications to build a new digital era respectively. For each layer, corresponding baseline security requirements are given such as for the equipment level, the Network Equipment Security Assurance Scheme (**NESAS**) is jointly developed by GSMA and 3GPP, is recognized as unified cybersecurity standard.

3. A common certification scheme across the OMC
   Provided compliance validation scheme for the OMC. Defined Accreditation Body (**AB**), Certification Body (**CB**), and Evaluation Body (**EB**), detailed the requirements and duties in the certification scheme, evaluation process and criteria, and other necessary components that are critical in establishing an open, transparent, and collaborative cybersecurity ecosystem. This ecosystem is to serve the OMC in addressing pertinent concerns arising from the adoption of the 5G and corresponding applications, and cases that build on top of the 5G such as cloud computing, IoT, and AI. This are the keys that will unlock the value of 5G and define the applications for embracing 5G and beyond.

The OIC-CERT 5G Security Framework is now on the website at *https://www.oic-cert.org* available to members only. It will undergo continuous updating as the technologies evolve. The WG will also start addressing other key elements, such as establishing an information sharing and analysis centre for 5G security and continuing work on enriching the framework developed in 2021 to address the different demands in safeguarding the OMC's digital transformation journey. The cloud security, for example, will further augment the "unlimited bandwidth" provided by 5G with "unlimited storage and unlimited computing power" that is the key to unlock the value of 5G and accelerate the dawn of a new digital era.

References

[1] Forest Interactive, "Positive 5G Outlook Post Covid-19: What Does It Mean for Avid Gamers?," Forest Interactive, 29 June 2020. [Online]. Available: https://www.forest-interactive.com/newsroom/positive-5g-outlook-post-covid-19-what-does-it-mean-for-avid-gamers/. [Accessed 11 November 2021].

[2] Organization of the Islamic Cooperation- Computer Emergency Response Team, "OIC-CERT," CyberSecurity Malaysia, [Online]. Available: https://www.oic-cert.org/en/missionstatement.html#.YbWa1b1BxmU. [Accessed 12 December 2021].

[3] International Telecommunication Union Development Sector, "Global Cybersecurity Index 2020," ITU Publication, Geneva, 2021.