Olatunji Osunji,

Doctoral Student, Marymount University

Arlington.

O0o34411@marymount.edu, olatunjiosunji@yahoo.com

2023849152

School of Business & Technology

Marymount University

1000 N Glebe Rd, Arlington, VA 22201

5G-Using Standards to Mitigate ICT Risks in Sustainable Development.

Abstract:

Digitalization and access to the internet has proven to be a catalyst for achieving the Sustainable Development Goals and since 5G comes with higher speed, capacity, in-built security features and other offerings, it can ensure that several of these goals are achieved in a much easier, efficient and secure manner. However, most of these standard security features of 5G are turned off by default, resulting in similar vulnerabilities that earlier generations of broadband technologies has. The visibility of the impact of digitalization of processes, infrastructure and services has been clouded by the continual increase in the number and sophistication of cyber-attacks. This cloud has created a trust issue on the use of services offered over the internet which development activities rely on. Since the developmental goals will not be sustainable without managing the risk inherent in the use of Information and Communication Technologies, securing 5G system has become an important component of this ecosystem. This report reviews how standards can be adopted to help mitigate risks of using 5G in the process of achieving the Sustainable Development Goals. It is hoped that this will be a good addition to the existing knowledge base for achieving the Sustainable Development Goals and mitigating risk associated with 5G.

Keywords.

5G, Compliance, Cyber Security, Security Standards, Sustainable Development Goals, Trust.

1. Introduction:

During the World Summit on Information Society (***WSIS + 10 summit***) in 2015, stakeholders within government, academic, private and international organizations were charged to integrate Information and Communication technologies (ICT) in their implementation approaches to the Sustainable Development Goals (SDGs).[1] This declaration positioned digitalization as a perquisite for sustainable development and ICT became the bedrock for development efforts as digitalization of services and processes continue to increase. One common denominator of the digitalization is access to the internet and SDG 9.c is aimed at increasing access to internet and ICT in least developed countries.[2] Bandwidth, speed and capacity of the telecommunication system have an impact on how well access to internet will aid in achieving these goals. Since high cost of internet service is an issue in developing countries,[3] individuals often settle for low bandwidth or data rate. With higher speed, people in rural area will be able to participate in real-time online training, E-health learning while more Internet of Things (IoT) devices can connect and send data faster to the cloud for processing[4].

5G is an emerging technology that can make this happen. It comes with improved bandwidth, capacity, and reliability of wireless broadband services. It is set to meet the demand of increasing data and communication requirements – from the billions of connected IoT, autonomous vehicle, enhanced health care and e-learning. With 5G, some of the hurdles against SDGs will be crossed. It is an improvement on what the present day 4G has to offer-100 times faster.[5] Being an emerging technology 5G is plagued with a challenge: the existence of a lag between its adoption and development of the regulations that will guide its use, especially as it relate to the risk associated with its use. Because of 5G's importance to economic development, critical infrastructure and its nature of crossing continental boundaries, standards are been developed to guide its implementation and use. 3GPP is the main global body for developing standards of mobile communications and these standards include ensuring good cyber security posture for 5G network. However, an EU risk assessment report on 5G stated that some of these security standards will be turned off in the network equipment, while network operators will choose to whether to implement them or not.[6] Since the developmental goals will not be sustainable without managing the security risk inherent in the use of ICT, the security of 5G network has become an important component of this eco system. This report reviews how standards can be adopted to help mitigate risk of using 5G in the process of achieving the SDGs'. This report is divided into four sections: the first is this introduction which continues with

---

[1] Niels Schia, "The Cyber Frontier and Digital Pitfalls in the Global South," Third World Quarterly, 39, no. 5, (2018): 821–837, https://doi.org/10.1080/01436597.2017.1408403.

[2] United Nations. "Target 9.c: Access to ICT," accessed June 5, 2020, https://stats.unctad.org/Dgff2016/prosperity/goal9/target_9_c.html

[3] A4AI, "Mobile Broadband Pricing Data for Q2 2019," accessed June 18, 2020, https://a4ai.org/extra/mobile_broadband_pricing_usd-2019Q2

[4] George Lwanda, "How 5G can Advance The SDGs ," accessed July 1, 2020, https://www.weforum.org/agenda/2019/04/how-5g-can-advance-the-sdgs

[5] GSMA, "The 5G Guide A reference for Operator", April, 2019, 29, https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf

[6] NIS Cooperation Group, "EU Coordinated Risk Assessment of the Cyber Security of 5G Networks," October 9, 2019, 7, https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

how ICT has impacted the development efforts and the risk associated with it. This is followed by why we need 5G and how it can help achieve the SDGs'. The third section looks at how standards have help to mitigate ICT risks, which is then followed by recommendation and conclusion. It is hoped that this will be a good addition to the existing knowledge base for achieving the SDGs and mitigating risk associated with 5G.

1.1 Link between SDGs and ICT

The Sustainable Development Goals are the world's shared plan to end extreme poverty, reduce inequality, and protect the planet by end of 2030.[7] This report views the success of SDG as dependent on three things: People, Process and Technology. While the aim of the SDGs' is to improve the quality of life, health and wealth of all individuals (people), its success will be determined by the involvement and cooperation of the same **people** whose quality of lives are to be improved; necessary **processes** set in motion by people in authority; and **ICT** that continue to underpin the SDGs'. When there is synergy between these three, all developmental effort will easily be reflected in SDG1 "No poverty", since the main goal of the SDGs are to eradicate poverty globally by 2030.[8]

The continuous effort of the Global e-Sustainability Initiative (GeSI) to quantify the sustainability benefits of ICT underpinning the SDGs revealed that out of the 17 SDGs, 11 have a positive correlation with digital access.[9] This implies that the goals may be achieved faster if more people and devices are connected to the internet. As an example, the report mentioned that for least developed countries there is a causation link between a 5% increase in internet access and 2 saved babies per 1,000 life birth. Also 5% increase in digital access will result into two additional weeks of schooling for women.[10]

With the knowledge that connection to the internet will enhance SDGs, several efforts have been initiated to improve the internet connection experience of people from developing countries. The Digital Infrastructure Moonshot for Africa - Connecting Africa through Broadband[11]and Facebook's 2Africa project - Building a transformative subsea cable to better connect Africa[12] are examples of some of these initiatives. Individuals from developing nations mainly access the internet through mobile devices and as at the end of May, 2020, Africa has an internet penetration of about 39% of its population and Asia has 55%. Over a period of 20years (2000 -2020) the developing world of Africa, Asia, Latin America and Middle East each has internet growth of about 2000%.[13] In addition to this increasing number of mobile access, IoT sensors have been deployed in several nations for data collection in areas like agriculture, climate monitoring and smart cities development. With the continued increase in number of mobile devices and IoTs sensors connected to the internet, achieving the SDG will definitely benefit from a more robust broadband technology that can accommodate more capacity, speed

[7] United Nations Foundation, "Sustainable Development Goals."

[8] United Nations University, "Can we End Poverty by 2030."

[9] GeSI, "Enabling the Global Goals. Evidence of digital solutions' impact on achieving the Sustainable Development Goals (SDGs)," accessed June 30, 2020, 9, https://etno.eu/datas/press_corner/press-releases/2018/GeSI_AS_2018_Digital_Enabling_the_Global-Goals.pdf

[10] Ibid., 5

[11] World Bank, "Connecting Africa Through Broadband" October, 2019, https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf

[12] Facebook, "Building a transformative subsea cable to better connect Africa," May 13,2020, https://engineering.fb.com/connectivity/2africa/

[13] Internet World Stats, "Usage and Population Statistics," accessed July 1, 2020 https://www.internetworldstats.com/stats.htm

and has security inbuilt in it. With more than two-thirds of the global population now connected to a mobile network Ericsson, a telecommunication giant in the 5G space estimates that by 2025, about 50% of internet data traffic will run on 5G networks p.14.[14]

1.2 Concerns about ICT Risks

The continued reliance of development efforts on ICT and hence internet connection has introduced new challenges: increase in the number and rate of cybercrime resulting in lack of trust on the ICT infrastructure that's underpinning the SDGs[15] and presence of new cyber security novice in cyberspace that is already plagued with viruses and worm - cyber pandemic.

The visibility of the impact of digitalization of processes, infrastructure and services is being clouded by continual increase in number and sophistication of cyber attack. This cloud has created a trust issue for the use of services offered over the internet. As suggested by Morgus,[16] this is a sign that more attention should be placed into mitigating the risk of digitalization. It is therefore essential to gain and maintain trust in services offered through digitalization in a sustainable manner. When we view the SDGs' through a cyber-security or risk management lens, we either see a concentrated and concerted effort (*fig 3*) or a dispersed effort (*fig 4*).

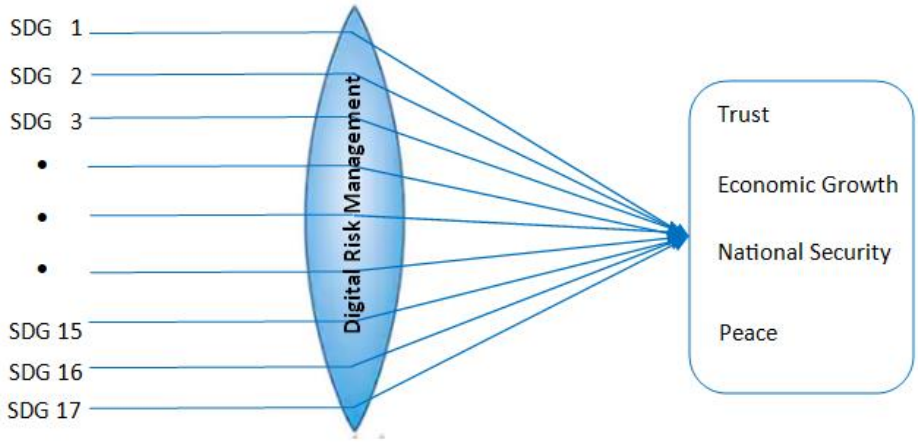

Figure 3: Implementing SDG with digital risk management

Morgus recommends implementing digital risk impact assessments for development projects and programs.[17]

---

[14] Ericson, "Ericsson Mobility Report," November, 2019, 14, https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf

[15] TrendMicro, "Africa A New Safe Harbor for Cybercriminals?"; Serianu, "Africa cyber security report 2017. Demystifying Africa's cyber Security Poverty line."

[16] Robert Morgus, "Securing The Digital Dividends: Mainstreaming Cyber Security in International Development," April, 2018, 17, https://www.newamerica.org/cybersecurity-initiative/reports/securing-digital-dividends/

[17] ibid., 55

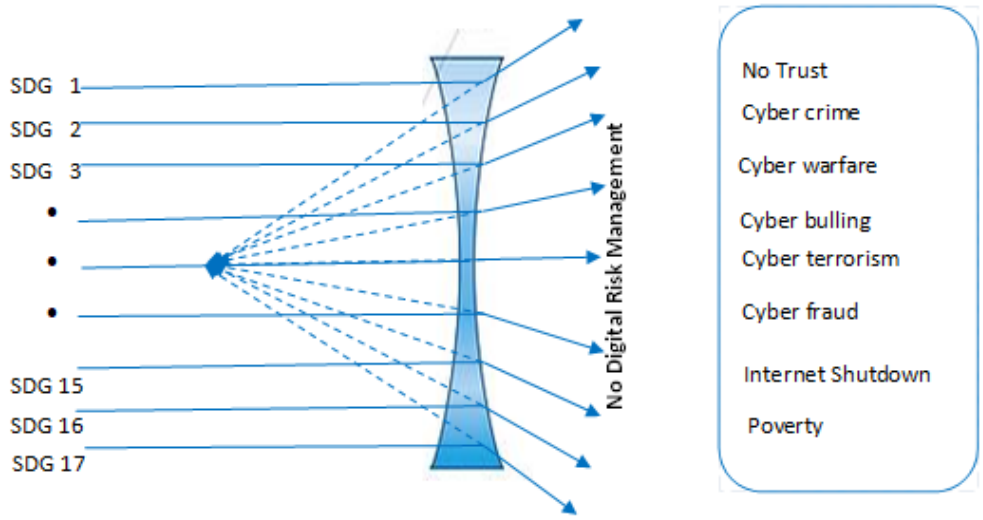

Figure 4: Implementation of SDG without digital risk management

2. 5G SDG Nexus

This section aims to look at why we need 5G and what it has to offer the SDGs'. Several demands have necessitated the need for a more robust, efficient and secure means of telecommunication. Some of these as highlighted on the website of ETSI, The European Standards Organization body dealing with telecommunications, broadcasting and other electronic communications networks and services are:[18]

1. Increasing number of Internet of Things (IoT), video streaming, growing number of connections from users, industrial automation has resulted in networks that need the capacity to manage billions of devices.
2. There is need for better energy performance for mobile devices due to this growing number of connections and data from mobile devices.
3. New industrial automation that requires ultra-low latency or high reliability wireless connectivity.

The SDGs' also contributed to these demands through the continuous increase in number of mobile device in developing country, increasing number of IoT sensors used for data collection in areas like agricultures and other requirements for high speed and low latency telecommunication to reach and serve the rural area's needs.

In response to these needs, the Radiocommunication sector of International Telecommunication Union (ITU-R) came up with recommendation - IMT 2020 to satisfy the demands:[19]

[18] ETSI, "Why do we need 5G?" accessed June 30, 2020, https://www.etsi.org/technologies/5g
[19] International Telecommunication Union, "Workshop on 5G"

1. Enhanced Mobile Broadband (eMBB) – This is aimed at addressing the constantly increasing traffic caused by growing number of connected devices and high user density.
2. Massive Machine-type Communications (mMTC) – Addresses the needs for devices and IoT that requires low data rates and energy efficiency
3. Ultra-reliable and Low Latency Communications (URLLC) - This take care of mission critical applications in industrial automation, and intelligent transportation systems.

According to GSMA, a body representing mobile communications industry worldwide, 5G era will create an environment that will deliver sustainable network, economics and innovation by driving growth in new use cases for large and critical IoT. In addition, it becomes the platforms to accelerate the digitalization and automation of industrial processes – which include the goals of industry 4.0.[20]

2.1 Areas where 5G helps SDG

The generation of mobile broadband before 5G already made positive impact on several of the sustainable development efforts. For example, people in developing nations already leveraged 3G and 4G technology to have access to e-commerce, e-government, e-health, e-learning and e-everything (through digitalization), but the increasing demand in bandwidth and speed will require taking advantage of 5G technology offerings. An article on the World Economic Forum's website by George Lwanda, of UNDP, stated that none or insufficient education has been identified as a hindrance to an upward social-economic progress, and while physically reaching the high number of uneducated living in rural areas of the developing world may be both difficult and costly, e-learning is being used through 4-G.[21] However, 5G offers more advantages that will allow for near real time e-learning, without much energy consumption, instead of watching pre-recorded videos.[22] Also there will be no need to clear land, cut down trees and erect school structures, thereby helping achieve SDG 12 & 15 and funds for this can be reallocated to other areas of the economy.

Nokia, another telecommunication company and major player in the 5G eco system also identifies the following areas where 5G can make impact on SDGs:[23]

1. SDG [2,14] - In the area of agriculture, supporting conservation and sustainability more data can be collected from IoT sensors using 5G and then processed using Machine Learning for up-to-date status information on the environment - weather, air, land or sea.
2. SDG 9 - 5G will help to connect people to more information and opportunities through e-services and which will assist in building a resilient infrastructure and foster innovation,
3. SDG 11 - 5G, with cloud computing and data science will help achieve smart cities that are resilient, safe, and sustainable.
4. SDG 13 - A reduction of up to 15% in greenhouse and gas emissions by 2030 can be achieved with 5G aided digitalization services and industries.

[20] GSMA, "The 5G Guide A reference for operator," 25.
[21] George Lwanda, "How 5G can advance the SDGs ."
[22] Ibid.
[23] Nokia, "Nokia and the United Nations Sustainable Development Goals," accessed June 13, 2020, https://www.nokia.com/about-us/sustainability/our-approach/nokia-and-the-united-nations-sustainable-development-goals/

2.2 Risk of 5G network

Despite the promises and enhancement of 5G, there are risks inherent in its use. The United States Cybersecurity and Infrastructure Security Agency (CISA) stated that some legacy vulnerabilities from 4G may be carried over into 5G.[24] Compared to 4G, 5G network uses more virtualization technology and this introduces new surface of attack. These vulnerabilities also lead to privacy concerns on the network, for example the possibility to knowing the location of a user was demonstrated by a team of researchers led by Syed Rafiul Hussain during the November 2019 Association for Computing Machinery's Conference on Computer and Communications Security held in London.[25] These researchers identified 11 new vulnerabilities in 5G. Hence, 5G networks may be vulnerable to attack or manipulation if not properly designed, implemented or managed.[26]

A severe disruption to 5G network will not only have significant effect on the underlining services that are dependent on it and meant to achieve one or more of the SDGs, but also functionality of other National Critical Infrastructures. Least to say, mitigating 5G risk has become a national security issues (U.S now has a 5G cyber security strategy, EU performed a region wide risk assessment of 5G, China wants to maintain dominance among 5G players). If this is not mitigated, the journey towards providing peace, equality and eradicating poverty through sustainable development will take a longer time to achieve.

In order to mitigate these risks, the European Union recommended some technical and strategic measures.[27] Some of these measures are centered on adopting and supporting the use of standards. The next section looks at standardization in 5G network and how it can be used to minimize risk of 5G with a view to building user's trust in the services that will run on such network.

[24] Cybersecurity and Infrastructure Security Agency, "Overview of Risk introduced by 5G adoption in the United States," 9.

[25] Liliy Newman, "As 5G Rolls Out, Troubling New Security Flaws Emerge."

[26] ENISA, "ENISA Threat Landscape for 5G Networks. Threat assessment for the fifth Generation of Mobile Telecommunications networks (5G)" November 21, 2019, 56.

[27] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk Mitigating Measures." January, 2020.

3. Standardization in 5G

In the world of technology, standards help to achieve interconnection and interoperability among products and services from different manufactures. As an example, all the promises of e-services, telemedicine and agricultural advancements using 5G depends on effective use of spectrum, which is been standardized by ITU among other things. ITU-R releases the requirements for a standard and evaluates the technologies that are submitted to it based on those requirements.

In other to coordinate 5G standardization process, telecommunication related organizations, national and regional bodies come together to form standardization bodies. The main 5G standards body is the 3rd Generation Partnership Project (3GPP). 3GPP is a global standards organization uniting seven regional and national standards organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC) across the globe.[28] They all work together to produce 5G standard.

3GPP is divided into three technical specification groups where each focuses on a specific area. These are, Radio Access Networks (RAN); Services & Systems Aspects (SA); and Core Network & Terminals (CT).[29] The Service and System Aspects have a working group, (SA WG3) which is responsible for security and privacy in 5G standards. The group addresses 5G standardization through improved subscriber un-traceability, protection of subscriber privacy, flexible identity management and lawful interception requirements in 5G systems.[30]

3.1 Challenges with 5G standardization

One of the vulnerabilities associated with network operators and suppliers is the "*lack of compliance with 3GPP standards or incorrect implementation of standards*".[31] Some of these security standards of 5G are optional during the implementation stage for manufactures, integrators, suppliers and telecommunication operators. The network equipment are developed and supplied with security turned off by default. Bruce Schneier, in one of his articles attested to the fact that 4G standard faced similar issues - "*operators even ignored security features defined as mandatory in the standard because implementing them was expensive.*"[32] In essence, even though standardization has been put in place to improve security, there is no compliance to it at most levels of 5G system development life cycle. While achieving a secure 5G network is dependent on how well the operators and integrators deploy and manage these security standards in their networks, there is need for an oversight of their implementations.

For the purpose of this review, a system development life cycle (SDLC) will be defined as "*a formal way of ensuring that adequate security controls and requirements are implemented in a new system or application*".[33] There are several phases defined, but the five commonly used ones are Requirements Analysis/Initiation Phase; Development/Acquisition Phase; Implementation Phase; Operations Maintenance Phase and Disposal Phase.[34] When applied to

---

[28] 3GPP, "About 3GPP."

[29] Ibid.

[30] 3GPP, "3GPP 5G Security."

[31] NIS Cooperation Group, "EU Coordinated Risk Assessment of the Cybersecurity of 5G Networks," 21.

[32] Bruce Schneier, "5G Security," January, 14 2020, accessed https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html

[33] Brian Evans, "The System Development Life Cycle: A Phased Approach to Application Security." January 7, 2019, accessed https://securityintelligence.com/the-system-development-life-cycle-a-phased-approach-to-application-security/

[34] Rebecca Bernstein, "5 System Development Life Cycle Phases."

a 5G network, efforts of 3GPP fall within the first two stages. "*In order to minimize exposure to risks, standardization has to drive the specification of new networks in such a way that security is built in from the design phases rather that as an afterthought*".[35] Security should be top priority at every phase of any 5G related project. In terms of prioritization during a government acquisition process, security of an entity within a critical supply chain should be given more priority than cost, schedule or performance.[36] 5G Standards provided by 3GPP and other 5G standardization bodies need to be enforced at all phase of 5G SDLC.

3.2 5G Standard needs compliance

As an outcome of its 5G risk assessment, EU recommended some set of technical and strategic measure to help mitigate the risks discovered. Some of the recommendations involve a form of adopting or enforcing standards.[37]

1. *Ensuring and evaluating the implementation of security measures in existing 5G standards.*
2. *Raising the security standards in suppliers' processes through robust procurement conditions.*
3. *Using EU certification for 5G network components, customer equipment and/or suppliers' processes;*
4. *Using EU certification for other non 5G-specific ICT products and services (connected devices, cloud services).*

Adopting these recommendations will be taking the right step as other critical Infrastructure areas have used similar method to mitigate risk.

3.3 Areas where standardization has been used to reduce digital risk

Two critical Infrastructure industries that has employed and enforced standard in mitigating risks are the energy sector and railway. In the North America, the North America Electric Reliability Corporation (NERC) - a non-profit organization, has standards for cyber security of monitoring and control systems within the Bulk Electric System (BES) companies. On the other side of the Atlantic Ocean, UNIFE, the Association of the European Rail Supply Industry operates the IRIS standard for rail operators to comply with.

3.3.1 NERC Reliability Standards

According to NERC website, the Reliability Standards are sets of requirements for planning and operating the North American bulk power system (NABS) with focus on performance, risk management, and entity capabilities. [38] The standards were developed using an ANSI-accredited process which ensures openness to all stake holders affected with the reliability of the NABS and is transparent to the public. The standards are listed as Critical Infrastructure Protection (CIP) Standards and each consist of a set of minimum security requirements for power generation, transmission and distribution enterprises to comply with. As of July 1, 2020, there were 15 active CIP standards of which 11 are subject to enforcement while the enforcement of the remaining 5 are been planned.[39] For example CIP-013-1 – Cyber

[35] 5G-Ensure, "Making 5G Networks and Systems Secure and Trustworthy."

[36] Potomac Institute, "Security Strategies for Global Supply Chains: Addressing Risk, Seizing Opportunity."

[37] NIS Cooperation Group, "Cybersecurity of 5G networks EU Toolbox of risk mitigating measures," 12.

[38] NERC, "Standard," accessed July 1, 2020, https://www.nerc.com/pa/Stand/Pages/default.aspx.

[39] NERC, "CIP Standard," accessed July 1, 2020, https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Security – Supply Chain Risk Management, which is subject to enforcement, addresses the relevant cyber security supply chain risks in the planning, acquisition, and deployment phases of the SDLC for BES Cyber Systems. In order to ensure compliance with NERC Reliability Standards, each organization under NERC is assessed, investigated, evaluated, and audited. Depending on violations, sanctions or fine or both are given to those in violation of mandatory NERC Reliability Standards.[40]

3.3.2 The International Railway Industry Standard (IRIS):

Another way that standard has been adopted to help minimize risk is through ISO/TS 22163:2017 standard, owned by ISO and implemented by the International Railway Industry Standard's (IRIS), an internationally recognized management system standard. The structure is based on ISO 9001 standard with additional business management systems requirements specific to railway industry.[41] It is a transparent System for auditing and issuing certification to railway equipment manufacturers, system integrators, operators or business partners against standard requirements. Its main objective is to improve the quality and safety in the rail sector. Companies can become certified by undergoing a certification audit conducted by third party certifying bodies and a successful audit results in a certificate that is valid for 3 years. IRIS certification is mandatory for sales of rolling stock and railway related equipment and components in Europe (RINA).[42]

4. Recommendations:

People need to be able to trust the e-services they use and if these services have 5G networks as its bed rock, then 5G need to be secure and resilient. A zero trust is needed because:

- The network operators are not trusted to implement security feature, hence there is need for auditing against compliancy to standards.
- The suppliers are not trusted not to have altered any features of the equipment, hence adequate testing should be done before implementation.
- The manufactures are not trusted not to have included a back door or vulnerability in their product, there need to testing, auditing and certification.

While there are opportunities for improvement, the implementation of standard security features by 3GPP and partnering organizations should be enforced. Certification like that of IRIS, and mandatory standards like NERC CIPs, should be introduced for all stake holders in the 5G network. The energy sector and bulk power system grids have NERC CIP because most other critical infrastructures depend upon electricity. While 5G has found its way to becoming a national cyber security concern, access to e-services, smart city, smart manufacturing, IoT - achieving most of SDGs and other critical infrastructure too are becoming dependent on 5G as well. Applying standards like NERC CIP will ensure that standard are applied across all layer of 5G SDLC and sanctions are given to violators.

The following steps are recommended

[40] NERC, "Sample notice of penalty."
[41] IRIS, "Information on IRIS."
[42] RINA, "International Railway Industry Standard IRIS quality certification."

1. Form a global, transparent, non-profit organization tasked with the improving the cyber security and resiliency of 5G network. This should be a global body because unlike rail or electricity, which is mainly within a region, 5G system cuts across regions and continents.
2. The body must develop and audit mandatory standards for cyber security and resiliency of the 5G systems.
3. Certification mechanism must be introduced for manufacturers, suppliers and Integrators operating in the 5G-eco system.
4. Standards must be made easy to implement and not complicate the already complex 5G network.
5. Process should be in place to audit, issues sanctions, implement fines and ensures mitigation of confirmed violations of mandatory standards.
6. Companies operating within 5G eco-systems must register with the body, be certified and be compliant with the mandatory standards that are applicable.
7. The standards and or certification should cover all areas of 5G SDLC, especially those not covered by 3GPP.

Conclusion:

Standards should be made easy to be complied with, especially when it involves cyber security and resiliency. For projects directed towards achieving the sustainable development goals and relying on one or more component of ICT, especially 5G, nations and sponsoring international organizations should seek to engage suppliers, integrators and operators that are certified and compliant with mandatory standards. This will serve as one of the step toward introducing digital risk management into the life cycle of sustainable development.

Reference:

3GPP. “3GPP 5G Security.” August 6, 2018. Accessed

https://www.3gpp.org/news-events/1975-sec_5g

3GPP. “About 3GPP” Accessed June13, 2020. https://www.3gpp.org/about-3gpp

5G-Ensure. “Making 5G Networks and systems Secure and Trustworthy.” Accessed June 28,

2020. https://5gensure.eu/sites/default/files/5G-ENSURE_brochure%20on%205G%20Standardisation.pdf

A4AI. “Mobile Broadband Pricing Data for Q2 2019”. Accessed June 18, 2020

https://a4ai.org/extra/mobile_broadband_pricing_usd-2019Q2

Bernstein, R. "5 System Development Life Cycle Phases". Concordia University, Texas. Last

modified March 17, 2017, Accessed https://online.concordia.edu/computer-science/system-development-life-cycle-phases

Bruce Schneier blog 5G Security. January 14, 2020. Accessed

https://www.schneier.com/blog/archives/2020/01/china_isnt_the_.html

Cybersecurity and Infrastructure Security Agency. "Overview of Risk introduced by 5G

adoption in the United States." Access June 20, 2020. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf

ENISA. “ENISA threat landscape for 5G Networks. Threat assessment for the fifth generation of

Mobile telecommunications networks (5G)” November 21, 2019. Accessed

https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport

Ericson. “Ericsson Mobility Report”. November, 2019. Accessed

https://www.ericsson.com/4acd7e/assets/local/mobility-report/documents/2019/emr-november-2019.pdf

ETSI. Why do we need 5G?. Accessed June30, 2020.

https://www.etsi.org/technologies/5g

Evans, B. "The System Development Life Cycle: A Phased Approach to Application

Security." January 7, 2019. Accessed https://securityintelligence.com/the-system-development-life-cycle-a-phased-approach-to-application-security/

GeSI. “Enabling the Global Goals. Evidence of digital solutions‘ impact on achieving the

Sustainable Development Goals (SDGs).” Accessed June 30, 2020. https://etno.eu/datas/press_corner/press-releases/2018/GeSI_AS_2018_Digital_Enabling_the_Global-Goals.pdf

GSMA. “The 5G Guide A reference for operator”. April, 2019. Accessed https://www.gsma.com/wp-content/uploads/2019/04/The-5G-Guide_GSMA_2019_04_29_compressed.pdf

Facebook. “Building a transformative subsea cable to better connect Africa”. May 13,2020. Accessed from https://engineering.fb.com/connectivity/2africa/

Internet World Stats. "Usage and Population Statistics." Accessed July 1, 2020. https://www.internetworldstats.com/stats.htm

International Telecommunication Union. Workshop on 5G. Accessed (June 15, 2020). https://www.itu.int/en/ITU-T/Workshops-and-Seminars/standardization/20170402/Documents/S2_4.%20Presentation_IMT%202020%20Requirements-how%20developing%20countries%20can%20cope.pdf

IRIS. "Information on IRIS." Accessed July 2, 2020.https://www.iris-rail.org/index.php?page=global&content=global_information&desc=info_teaser

Lwanda, George. “How 5G can advance the SDGs .” Accessed July 1, 2020. https://www.weforum.org/agenda/2019/04/how-5g-can-advance-the-sdgs

NIS Cooperation Group, “EU coordinated risk assessment of the cybersecurity of 5G networks.” October 9, 2019. Accessed https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

NERC. "Sample notice of penalty." Accessed July 1, 2020. "https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2605_Part%201.pdf"

Nokia. “Nokia and the United Nations Sustainable Development Goals.” Accessed June 13, 2020. https://www.nokia.com/about-us/sustainability/our-approach/nokia-and-the-united-nations-sustainable-development-goals/

NIS Cooperation Group, “Cybersecurity of 5G networks EU Toolbox of risk mitigating measures.” January, 2020. Accessed https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132

Newman, H. Liliy. “As 5G Rolls Out, Troubling New Security Flaws Emerge.” November 12,

2019. Accessed https://www.wired.com/story/5g-vulnerabilities-downgrade-attacks/?mbid=social_twitter&utm_brand=wired&utm_campaign=wired&utm_medium=social&utm_social-type=owned&utm_source=twitter

NERC. "Standard." Accessed July 1, 2020.

"https://www.nerc.com/pa/Stand/Pages/default.aspx.

NERC. "CIP Standard." Accessed July 1, 2020.

https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx.

Morgus, Robert. “Securing The Digital Dividends: Mainstreaming Cybersecurity in International Development.” April,2018. Accessed https://www.newamerica.org/cybersecurity- initiative/reports/securing-digital-dividends/

Potomac Institute. “Security Strategies for Global Supply Chains: Addressing Risk, Seizing Opportunity”. October, 2018. Accessed https://www.potomacinstitute.org/images/VITAL/Security_Strategies.pdf

RINA. "International Railway Industry Standard IRIS quality certification." Accessed June14, 2020. https://www.rina.org/en/qms-in-the-railway-sector

Serianu. “Africa cyber security report 2017. Demystifying Africa's cyber Security Poverty line.” 2017. Accessed https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf

Schia, N. Niels. “The cyber frontier and digital pitfalls in the Global South.” Third World Quarterly, 39, no. 5, (2018): 821–837. Accessed https://doi.org/10.1080/01436597.2017.1408403.

TrendMicro. “Africa A New Safe Harbor for Cybercriminals?” 2013. Accessed https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf

United Nations. "Target 9.c: Access to ICT." Accessed June 5, 2020. https://stats.unctad.org/Dgff2016/prosperity/goal9/target_9_c.html

United Nations Foundation. “Sustainable Development Goals.” Accessed June 2, 2020 https://unfoundation.org/what-we-do/issues/sustainable-development-goals/#:~:text=The%20Sustainable%20Development%20Goals%20(SDGs,protect%20the%20planet%20by%202030.

United Nations University. "Can we End Poverty by 2030." September 09, 2015.

Accessed https://unu.edu/publications/articles/can-we-end-poverty-by-2030.html#:~:text=The%20primary%20objective%2C%20or%20Goal,its%20forms%20everywhere%E2%80%9D%20by%202030.&text=To%20end%20extreme%20poverty%20by,Saharan%20Africa%2C%20in%20particular).

Wen, H. Joseph. “Internet computer virus protection policy.” Information Management & Computer Security, 6 no. 2 (May 1, 1998): 66-71. doi:http://dx.doi.org.proxymu.wrlc.org/10.1108/09685229810209388

World Bank. “Connecting Africa Through Broadband” October, 2019. Accessed https://www.broadbandcommission.org/Documents/working-groups/DigitalMoonshotforAfrica_Report.pdf