CHAPTER 4.2

BUILDING A CYBER SMART COMMUNITY

ZAMA I. DLAMINI
JACKIE PHAHLAMOHLAKA

1. Introduction

In 2018 the Deputy Minister of Higher Education and Training for South Africa, Mr. Buti Manamela, visited the United Nations for the opening of the 2018 Justice Initiative Global Hackathon. He remarked on his visit to Silicon Valley or what he refers to as "the place of inventions" (Department of Higher Education and Training 2018) and how it related to developing economies like South Africa. These are places that are enjoying the benefits of the internet while they contribute extensively to illegal drugs, human trafficking, cyber fraud, and other related crimes. South Africa has one of the highest rates of cyber crimes on the continent (Department of Higher Education and Training, 2018).

He acknowledged that global skills competitions, seminars, skills transfer, and knowledge sharing are significant and could assist in raising awareness, help toward developing solutions, and provide assistance to solving or mitigating some of these problems. Within a smart community, various systems, users, and other devices interact with each other over ubiquitous networks, delivering services over cyberspace and social networks. As a technology, they possess qualities which make them significant in developing economies. While the concept of smart communities has been around within cyberspace for a while now, technological advances have made their development and usage even easier through social networking services, due to their inherent ubiquitousness.

A smart community is viewed as an integral part of our future society and a promising solution to many socioeconomic problems, problems in

which developing economies typically experience additional unique and varied challenges (Caperna et al., 2017).

Developing nations, like South Africa, are essentially those with low, lower middle, or upper middle incomes (Al-Kuwari, 2018). These countries are often exemplified by a low human development index (HDI) relative to other countries, an underdeveloped industrial base, and lower levels of sophisticated urbanization. A nation's gross domestic product (GDP) per capita compared with other nations is also often used as a reference point for comparison (Correa et al., 2017). There is however no universal, agreed-upon criterion for what makes a country developing versus developed and which countries fit these two categories. Similar features of developing countries are low standards of living; these are results of, among other causes, low income, inequality, poor health, and inadequate education. South Africa is considered to be a developing economy.

This chapter shares some methods that could be employed in order to construct and deploy a local cyber smart community in a developing economy, where the notion of smart communities seems to be fitting and significant compared to that of smart cities. Researchers have conducted many studies and communal initiatives in such environments, and the lessons learned and insight gained from these endeavors are provided as examples and inspiration for this chapter. Some of the expected benefits of cyber smart communities include confidence in trading and systems used, resilient and sustainable local businesses and entrepreneurships, and cost savings from optimizing use of resources; improved private, public, and government services and interaction for citizens; better streams of data to improve decision-making; and the opportunity to attract technology-savvy members and businesses within a smart community (Kehoe et al., 2011; Silva et al., 2018; Allen et al., 2020).

The rest of this chapter presents cyber smart communities and their significance, then the cyber smart community role players, which is followed by the cyber smart community building approaches. The cyber smart community challenges are discussed before the conclusion of this chapter.

2. Cyber smart community

A smart community should have the ability to integrate multiple technological solutions, in a secure fashion, to manage a community's

assets. This includes local government information systems, schools, libraries, transportation systems, hospitals, power plants, law enforcement, and other community services for it to be considered cyber smart.

It is a challenge to talk about smart communities without mentioning smart cities. One distinct difference between the two is their focus. Smart cities include the collective community processes that empower communities' institutions, while smart communities focus on interventions than enrich individuals (Caragliu, Del Bo, and Nijkamp 2009; Kummitha and Crutzen 2017; Albino, Berardi, and Dangelico 2015). Smart communities intend to produce a more free social distribution of benefits rather than leaving it to the market to decide (Correa, Pavez, and Contreras 2017; Xia and Ma, 2011). That is empowering citizens rather than market economics. With that being said, the concept of smart cities in developing countries like South Africa is mainly ways of turning urban environments into gold mines for consultants, and hardware and software companies, and re-engineering cities to the image that benefits the most prosperous and well-serviced inhabitants while transferring additional resources and benefits from the poor to the rich (Kummitha and Crutzen, 2017; Kiganda, 2016).

Any discussion involving technological advances in the cyber domain today cannot be complete without discussing safety. There is always a criminal element looking to exploit any vulnerability that accompanies rapid development to their own advantage and in this domain the criminals evolve as quickly as the technology (Grobler et al., 2011). Safety refers to the state of being safe, the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational failure, error, accidents, harm, or any other event which could be considered undesirable. It is the control of recognized hazards to achieve an acceptable level of risk.

It is imperative that the smart community is also a secure one, since technology pervades the daily lives of its members. Mobile crowd-sensing (MCS) applications, for example, could potentially collect sensitive sensor data pertaining to individuals. GPS sensor readings can be used to estimate traffic congestion levels in a given community but at the same time these GPS sensor readings can be used to determine private information about the individual, such as the routes they take during their daily commutes, and home and work locations (Gurstein, 2013). This could be done without the user's knowledge, especially if they are not cyber-savvy. The security and privacy policies should unavoidably affect the management of, access to,

and provenance of, information to record ownership and process history of data across and within services (Xia and Ma, 2011).

Members of the smart community should work together with the private sector, government, academia, and citizens in assisting cybersecurity providers to produce proof-of-concept solutions. This could potentially be developed into complete systems of defense and even commercial products. Ideally, these cyber security solutions would have been tailored for that particular community's needs for them to become a cyber smart community.

The benefits of cyber smart communities include being proactively aware of the vulnerabilities that exist in the cyberspace. Other benefits include cost savings from optimizing use of resources; improved private, public, and government services and interaction for citizens; better streaming of data to improve decision-making; and the opportunity to attract technology-savvy workers, businesses within smart communities, and secure use of technology in improving the actual physical and virtual safety of the smart community members.

Approach example: cybersecurity awareness training initiative

In an effort to prevent innocent smart users from becoming victims of cyber attacks, an intensive cyber security awareness program can be tailored specifically. This can educate the targeted smart community, from novice internet and technology users with regard to basic cyber security, to expert users. For example, as part of the e-entrepreneurship training initiative, the entrepreneurs could be educated and given training on safe and secure online behavior to ensure their safety and the sustainability of their businesses against cyber attacks (Kiganda, 2016).

The lifecycle of cyber smart communities could vary; a community could possibly function over an indefinite length of time in some cases, or it could be relatively short in others (a couple of years) (Phahlamohlaka et al., 2015). This can depend on any number of factors including the technology used or the goal of its members. Building these communities is a continuous process.

The significance of cyber smart communities

The balance between those living in urban areas and those living in rural areas is continuously inclining. This is one of many important reasons for

considering building smart communities with cyber aspects. South Africa, as one of the developing countries, is made up of rather many communities than cities (Caperna et al., 2019). These are spread out throughout the country such that South African society is facing many challenges that remain to be addressed. In healthcare, for example, there are many adults who have chronic disease while staying alone or with young grandchildren while grandchildren's parents are in big cities trying to make ends meet. Another example is transportation; the traffic of many modern cities is getting saturated and there is a lot of congestion.

The design and deployment of cyber smart communities could facilitate constituting the infrastructure needed to create a set of new services for daily life. On healthcare challenges, cyber smart communities could make it possible to continuously monitor people's health remotely, respond to emergencies in real time, and offer remote emergency care (Nam and Pardo, 2011). These services could support impaired people to live more healthy lives, minimizing time in hospital, at local doctors, or in care homes. All people within the community could benefit, as long as they wish to improve their quality of life.

Recent technological advances in sensing, networking, and computing are leading to the wireless integration of sensor or actuator networks and social networks (CSIR Meraka, 2009). By exploring this integration, the smart community goes beyond either of the currently isolated two areas. Based on the latest progress in underlying technologies for both areas, the smart community can enable many novel functionalities, which otherwise are very difficult, if not impossible, to be realized by social networking services alone. Smart communities allow for collaborating and sharing among social contacts, which can increase real-time awareness of different community members about each other and provide a better understanding of the aggregate behaviors of the community (Partridge, 2004).

3. Cyber smart community role players

Although an infrastructure that is functioning properly, with broadband and the internet as necessary, it could still be insufficient in the successful establishment of a smart community. Our definition of a smart community explicitly mentions collaboration and consensus-building between individuals and institutions at various levels. In other words, we envision policies and digital services to be multiply sourced: bottom-up—that is,

starting from initiatives of small, self-organized groups of individuals, and top-down—that is, coming from national and local government levels.

Connection rates are only a limited measure of success. The role of social capital, defined as the construction of social relations and networks of trust and reciprocity is vital in order to engage all stakeholders to participate and engage with a smart city. It is thus recognized that technology has to be utilizable and understandable by the communities that it is supposed to serve and that ordinary people and communities need to have the skills necessary to utilize ICTs. Additionally, it is necessary to concentrate on ICT applications such as e-voting, e-learning, or e-commerce for all the important aspects of the community's activities. ICT and its applications are developed to facilitate involvement of all role players—see Figure 4.2.1—in the development of the smart community. ICT infrastructure and applications are prerequisites but without real engagement and willingness to collaborate and cooperate between governments, industry, other voluntary organizations, academia, and community there is no smart community.

Figure 4.2.1: Cyber smart community role players

Community

This is the most significant role player of the entire smart initiative. It is comprised of its local cultural or traditional leaders, local businesses, and the consumers. It is sometimes difficult to understand the local model outside of context. Cultural influence dominates; any solution meant for the local citizens must be introduced to the leaders first, following specific protocol (Kesswani and Kumar, 2018). Not heeding these considerations could lead to a 90% chance of failing, as the solution will not get any buy-in from the local entrepreneurs.

Community stakeholders

Community stakeholders are defined as those who have direct power over, or are directly impacted by, smart community initiatives but whose interest spans one or more communities, or those whose influence extends to or is impacted by a particular smart community initiative in defined geographic areas (International Telecommunication Union (ITU) 2017). These stakeholders may include mayors, local council officials, local staff, local committees comprised of elected officials and citizens, local departments, chambers of commerce, local leaders, management districts, media, local influencers, other utility providers, and customers.

Local entrepreneurs

Much city planning has historically been conducted by city planners, architects, and bureaucrats among others, often ignoring the choices or needs of the people at ground level. If smart cities do not consider the citizens' views or stakeholder perception in their construction, then it may be overambitious to expect any contribution from them to reduce social disparities. In reality, smart city planning has so far proven not to be too different from any other administrative-based planning. Thus, there are serious gaps identified in the way the entire concept of smart cities has evolved.

It is not enough for governments to provide jobs, and space for local entrepreneurs and SMMEs in order to be attractive and sustainable for its communities. A smart community must have an understanding of all players involved in the efforts to achieve the best results. The smart community concept emphasizes the significance of collaboration, cooperation, and

partnership between all players involved including governments, industry, other voluntary organizations, academia, and community. The most significant role players in the smart community are citizens or the community. They are the key players as the users of the technologies and ICT solutions. This leads to the cooperation between government, industry, academia, and citizens.

Government

It is important to note that technology by itself will not make a city or community smarter; building a smart environment requires a political understanding of technology, a process approach to manage the emerging smart area, and a focus on both economic gains and other public values (Chourabi et al., 2012).

One of the more important roles of the national government is to address the shortage of cybersecurity skills in the workforce and among its citizens. This could be achieved through targeted programs throughout the national education system, starting with research institutions and universities. These programs should be tailored in a manner that facilitates local engagement solving specific locational problems not generally encountered by developed countries. The government should engage with industry and cooperate with local leaders to raise awareness of the importance of cybersecurity across the nation. These skills are both increasingly essential and sought after, and are in short supply.

Many citizens and organizations are also simply unaware of the risks they face in cyberspace. Most of us lock our front doors and take care of our belongings, but we do not take the same degree of care with our devices and online information. The government should be committed to arming citizens with the appropriate knowledge and cybersecurity skills to protect themselves and raise levels of cyber security awareness, so that in turn we can all benefit from the opportunities provided by a more secure cyberspace (Chourabi et al., 2012). The current shortfall in the workforce and the research and development base can only be fixed through investment in sound policy and a long-term education plan that targets high schools and universities to promote careers in the cyber security profession.

Industry

On a global level, Navigant Research in 2011 estimated that about $100 billion over the next ten years would be invested in technologies to support smart cities. This offers vast scope for private players to become actively involved in the sector. Technology vendors and consultancies consider it a prosperous field for their growth. In the light of global commitments to achieving sustainable development goals, we have to see how the corporate interest to enhance economic prosperity is in conflict with environmental and social equity. It should be understood that while big corporations are busy installing ICTs and other technology, in large metropolitan areas, SMMEs in general work in smaller areas with a defined aim of offering goods or services to a small proportion of the population and social enterprises address the most pressing social problems.

At the local level, smart communities potentially open up new business opportunities in addition to providing a foundation for change in traditional industry sectors, and for the growth of new industries. This means that local suppliers to smart communities have two distinct features:

- The local organizations deliver services and solutions in contact with other companies and the community.
- One of the requirements for suppliers to participate in the smart community is to make sure that their products and services use digitalization technologies as a key component.

Most of the local organizations that enable smart communities deliver products that are technical, but do not contain a digital component. This leaves us with a gray area of organizations which, based on the digital limitation, do not belong to the population.

Academia

The national research institutions, universities together with other parties that are involved in national research, play a significant role when it comes to building local cyber smart communities. In South Africa there are a number of ICT initiatives that are taking place at the Seidet Community Center. Some of these initiatives involve the South African government, Mpumalanga province municipalities, public and private sectors, academic and research institutions (such as University of Pretoria and CSIR) who currently are solely working with Seidet on research and community development. These isolated collaborations could be better managed using the existing ICT resources and infrastructure, such as the Seidet Community

Center, which hosts a centralized system that manages both the service providers and consumers. Having such system in place could also reduce redundancy of service delivery. The current ICT initiatives at the Seidet Community Center, working together with the University of Pretoria (UP) and CSIR include the e-entrepreneurial training, and e-Skills program, cybersecurity awareness training and CSIR Broadband for All (BB4All), and the village operators initiative (Kummitha and Crutzen, 2017; Salemink et al., 2017). All these initiatives will be further discussed.

4. The cyber smart community building approaches

Various factors play a role in the development and success of a cyber smart community. Environment, infrastructure, funding, the level of technology adoption, and continuous personal development for and within smart communities and what they stand for, are significant. These factors are just as influential at the individual level of members within smart communities. This section presents some of the approaches employed in successful growth efforts, as well as practical, insightful methods for improving communities to becoming cyber smart.

The proactive planning approach

This approach is the same as project planning and can incorporate a number of the steps involved in such processes, in the following manner:

- identifies a smart community problem that stands in the way of becoming cyber smart
- creates a work plan for addressing problems and attaining the goals
- describes measurable beneficial impacts to the community that result from its implementation
- determines the level of resources or funding necessary to implement the plan

Identifying smart community requirements

Local decision-making in achieving community self-sufficiency is fundamental to the success and positive growth in every smart community. The community involvement is central to the strategic planning, and

comprehensive and strategic planning is a time-consuming process. It requires the development of a community-wide needs assessment that collects community input and analyzes this in order to prioritize problems and the basic needs of the community.

- **Comprehensive planning:** This process involves completing a community-wide needs assessment to engage the community in identifying and prioritizing all goals and the community problems preventing the achievement of those goals. Next, the community is involved in the process of developing a method to accomplish long-range goals, also discussing initial ways to overcome the problems. This method should include a process to measure the progress toward achieving those goals. Comprehensive plans usually require at least a year to complete and cover a five- to ten-year time span (Rios, 2012).
- **Strategic planning:** This is a process used when a community already has a comprehensive plan and wants to move forward to achieve its long-range goals. Strategic planning involves the participation of the community in identifying problems that stand between the community and its goal of becoming cyber smart. This results in a strategic plan; a strategic plan generally takes at least a year to complete (Rios, 2012).

Setting cyber smart community priorities

Setting cyber smart community priorities begins by describing the conditions that would exist in a "perfect cyber smart community." The resulting list of statements could be regarded as the community's goals in such areas as employment, education, cultural preservation, housing, and family income (Al-Kuwari 2018; Siebeling and Romijn, 2004). The point is to envision an overall cyber smart community or a subset of the community, living in an ideal situation.

- **Problem and resource analysis:** This could be regarded as the first part of a requirements analysis. A successful cyber smart community is one that is designed based on a good understanding of the community conditions and identifies the problems preventing the community from becoming a cyber smart community. Community conditions include aspects of

the community such as its geographic location, demographics, ecosystem, and history. A community assessment can be conducted to identify problems and determine which adverse current community condition will be addressed (Siebeling and Romijn, 2004).

Identifying the specific problems plaguing a community is critical in designing a sustainable cyber smart community. Problems or negative current conditions, both internal and external, are aspects that would have to change or be overcome in order to become a cyber smart community.

The last task under this activity is to refine the list of available resources by using the list of assets, funding, and people identified in the community assessment to build an inventory of internal and external resources that could be available for a cyber smart community and that would address the problems identified in the assessment.

- **Cyber smart community goals, objectives and challenges:** The cyber smart community goal is a basic description of the purpose of the cyber smart community—a reduction, or resolution of the problem or problems identified. The goal statement represents the result of the success achieved by the cyber smart community. The statement should be brief, to the point, and realistic (Rios, 2012).

  The objectives are specific, measurable accomplishments designed to address the stated problems and attain defined goals.

  Every cyber smart community has the potential to run into challenges that can impede progress and prevent or delay successful completion. There should be contingency planning in place which involves identification and preparation for potential challenges that may cause a delay in achieving a cyber smart community, to fall behind schedule, or to go over budget. A contingency plan is fallback position that allows better preparation to handle urgent circumstances.

  Cyber smart community evaluation measures should also be defined, in order to measure the effectiveness and efficiency of a cyber smart community and further determine the level of achievement of the cyber smart community objectives. Findings from an evaluation will also help a

community to plan for the future, as it can identify additional or persistent problems that need to be solved. This is why building a cyber smart community is a continuous process.

Research, development and innovation (RDI)

This approach focuses on undertaking cyber security-related research and development initiatives aimed at cultivating innovation within the smart community. These initiatives should be about, and for, the smart community, with the additional directive of potentially developing a cyber smart community that will benefit the smart community at large. Some of the strategic objectives of the RDI should focus on the following:

- Investigating the development of a new safe and secure application and technologies that will address the smart community's need for it to be resilient.
- Examining models to test and validate robustness of solutions developed for the smart community in an effort to make it a cyber smart one.
- Conducting RDI that will assist in securing local entrepreneurs and other community members in conducting business and studying online, and remaining the cyber-savvy users.
- Designing, developing, facilitating and nurturing synergies between the smart community structure and new technology in order to effectively provide and maintain proper governance of the smart community through cyber security policies and other related regulations.
- Creating employment opportunities through socioeconomic development programs.

This approach's implementation should go iteratively through the phases such as conceptualization, preparation, and development; implementation and commercialization; and the review of growth and sustainability. The RDI approach should be a continuous process within the smart community. Some of the benefits of this approach include:

- the development of new products and services (such as an education portal for students, apps for local businesses)

- reduced time to market for new products and services
- greater efficiency in the allocation of scarce resources
- greater participation by all sectors of the community and leading to more widespread use
- diminished digital inequality through the increased appropriation of ICT
- increased innovation

Approach example: BB4All and village operators initiatives

One of the Council for Scientific and Industrial Research (CSIR) community development projects is called Broadband for All (BB4All). It was aimed at diminishing the widening gap in digital inequality to bring the social and economic benefits offered by broadband connectivity to rural communities in South Africa and other developing countries. The objective of the initiative was to provide broadband access to rural communities in an affordable and sustainable fashion. This was accomplished by the enabling of low-cost building and sharing of connectivity, utilizing mesh networking principles and equipment (Meraka, 2009) to expand coverage within a smart communities.

To ensure sustainability of the initiative, the local community facilitated and ensured that adequately skilled and trained local entrepreneurs (also known as the village operators (VO)) were responsible for operating, promoting, and expanding the BB4All offering within a community (Roux, 2009). Seidet facilitated the VO recruitment via schools and the Mpumalanga Department of Education. Seidet is regarded as a significant stakeholder and key contributor to the BB4All initiative. They are local entrepreneurs; young people with the right attitude and approach to become VOs. The VOs underwent entrepreneurial and business mentoring, personal development, and training on the BB4All network infrastructure maintenance, operation, and support (CSIR Meraka, 2009).

The function of the VO is to service an exclusive area with a limited number of clients, key clients being clusters of schools. The clients are connected through a peer-to-peer community mesh network. The community mesh networks are linked through a backhaul network called a backhaul mesh. In addition to connecting the mesh communities, this mesh network contains a link to an IP backbone for IP services and the internet.

For redundant routing, this type of network ensures that a VO device can link to two or more other VOs from other communities.

Similar concepts of RDI together with its application within the local communities should be increased, with an inclusive notion of cybersecurity coupled with developments that are advanced to improve communities' lives.

Community empowerment from a socioeconomic perspective

This approach encourages smart communities to resist being controlled without their own opinions on where they would like to see their communities, and what they would like to contribute in improving their lives through local business. It recommends that smart community people should act in a democratic way and demand from their leaders that their different opinions are heard and that their leader talk with them instead of talking to them, in an effort to contribute to local community empowerment in socioeconomics (Damiani et al., 2017).

Socioeconomic development in smart communities leverages technology to increase efficiency while reducing costs. The success of this requires a government's dedication, incentives, vision, and leadership. For example, free Wi-Fi can be used as a significant tool in connecting entrepreneurial businesses and local communities by supporting business transactions; additionally, private investments and entrepreneurship play crucial roles in ensuring a strong, smart community economy. It is in no doubt that the economy is the main element of smart city initiatives (Popescu, 2015), but information technology, as a backbone and core of smart communities, should thereby remain safe and secure from cyber threats and attacks (Kramer et al., n.d.). This means that information technology has been a facilitator in addressing economic challenges for communities and nowadays is regarded as the basis of every sector of every economy (Graham, 2001).

Role players involved in this approach include:

- leaders of community-based organizations and community structures who work with community processes to cultivate participation, foster collaborative relationships, and enable meaningful dialog
- community activists whose role is to create awareness about social challenges and to spark collective action for transformation

- community development facilitators whose work is to mobilize, organize, and accompany people toward a common goal
- coordinators of community development initiatives whose work is to cultivate participation and foster a sense of common purpose among community groups

An example of this approach at work is presented below.

Approach example: E-entrepreneurship training and e-Skills program

The first entrepreneurship training of sixteen members from the Seidet community was done in 2011 by the Department of Economics at the University of Pretoria (UP). This was followed by further training of fourteen members from the broader Siyabuswa Community in 2013 at the Seidet Community Center in Siyabuswa (Grobler et al., 2011). Linked to this entrepreneurship training was also the e-Skills training component, facilitated once again by academics from the Department of Informatics, UP. The second training at the Seidet Community Center in Siyabuswa was the collaboration between Seidet, the University of Pretoria, and the CSIR, with the CSIR focusing on cybersecurity awareness training (Kummitha and Crutzen, 2017; Grobler and Dlamini, 2012). The e-Skills component was conducted as part of the broader e-Skills program of the national Department of Communications. The combination of the entrepreneurship and the e-Skills training was dubbed e-entrepreneurship training.

The enhancement of the e-entrepreneurship training with cyber security awareness is one of a kind that is necessary for any smart community for it to be cyber smart. There are many areas that the smart community requires training on, and when this training is conducted, it is recommended to couple it with cyber security topics that are related to that specific domain. As mentioned above, in all sectors IT is regarded as a foundation and IT without a security aspect, is a plan for failure (Grobler et al., 2011).

It is also worth noting that the success of such training requires the cooperation of various key stakeholders, such as academia, community leaders, and community, and the government in the case of the above example.

Approach example: Fostering application development initiative

This is a fairly recent initiative that was sparked in 2018 during a meeting with the Municipal Manager of Dr. JS Moroka Municipality, Benny Mahlangu. He challenged Unisa academics to participate in alleviating the problem of youth unemployment in the Siyabuswa area, located in Mpumalanga, South Africa. Some members, from both Seidet and Unisa had been working behind the scenes to put together an initiative that would prepare ten unemployed youths to participate in an upcoming mobile application development, the hackathon challenge. There were five males and five females, showing remarkable potential; youth from the Siyabuswa community itself, who were selected to participate in the mobile application development hackathon. This initiative required that the tools provided to the community's youth could further enable them to promote reciprocal facilitation of skill enhancement. The program is designed to promote a much larger initiative with the goal of seeing all ten participants past training, in order for them to evolve into trainers for the envisioned smart community in Siyabuswa.

Again, it is through such initiatives where local government not only led or talked to its community, but further understood the day-and-age of what could solve the needs of the community better (Benevolo et al., 2016). Understanding that, since the future depends on IT, its benefits could be easily be transferred and used now.

The education and continuous development approach

The government should work in partnership with industry and academic institutions to improve cyber security education at all levels of the smart communities. This will not only allow them to become cyber smart, but to also develop a community with the right skills and expertise that can help all take full advantage of the opportunities in cyberspace (Rios, 2012). Cyber security education should be through a consistent curriculum and superior teaching from pre-school age to grandparents; all users in cyberspace should receive such cybersecurity training and education. Cyber security threat reality and headlines should be made available to all online and device users to enhance their daily decisions they make online and in the applications they choose to use. This could assist users for smaller actions that they need to take, such as understanding the significance of continuously updating the firmware of their devices so as to minimize the risk of cybersecurity threats.

Approach example: Cybersecurity awareness training initiative

The South African research institution, CSIR, together with one of the local government departments, developed cyber security awareness training to educate novice internet and technology users with regard to basic cyber security. The topics that were covered in the training session included: cybersecurity in an enterprise, physical computer security, mobile security, password protection, malware, pop-ups—adware and spyware, botnets, surfing the web, email security, file sharing and copyright, internet banking, cookies, phishing attack avoidance, social networking, social engineering, identity theft, and cyberbullying (Kiganda, 2016). This program was then tailored for different users, for example it has been as part of the e-entrepreneurship training initiative, where a group of local entrepreneurs were trained on safe and secure online behavior to ensure their safety (Dlamini and Modise, 2013). This training initiative is regarded as a significant part of the smart community in an effort of making it "cyber smart."

5. Cyber smart community challenges

A cyber smart community initiative will find itself in alignment with a community's goal to improve the economy, implement innovative policies, and stimulate economic development in high-growth industry sectors to attract capital investment and citizen services. It is critical for government and industry leaders to define, engage, and communicate the value of a cyber smart community to their constituencies and bases. This requires addressing many challenges related to cyber security threat, such as:

- **Insider attacks:** a malicious threat to an organization that comes from internal people in an organization, such as employees, former employees, contractors, or business associates, who have inside information concerning the organization's security practices, data, and computer systems.
- **Phishing and spear phishing:** a common form of email attack designed to make targeted victims perform a specific action by clicking on a malicious link or attachment. The difference between them is primarily a matter of targeting.
- **Lack of cyber security knowledge:** the insufficient security that can be applied to computing devices such as computers and smart

phones, as well as to both private and public computer networks, including the whole internet.

- **Distributed denial-of-service (DDoS) attacks:** occurs when multiple systems flood the bandwidth or resources of a targeted system, usually one or more web servers. Such an attack is often the result of multiple compromised systems flooding the targeted system with traffic.
- **Malware:** any program or file that is harmful to a computer user for example computer viruses, worms, Trojan horses, and spyware.
- **SQL injection:** a code injection technique, used to attack data-driven applications, in which diabolical SQL statements are inserted into an entry field for execution.
- **Bring your own device (BYOD):** refers to the policy of permitting employees to bring personally owned devices (laptops, tablets and smartphones) to their workplace and to use those devices to access privileged company information and applications.

Other challenges include the following:

- prioritizing cybersecurity and transparency
- developing data and privacy standards
- creating a body of knowledge around the constituent experience

Addressing the challenges

In order to confer the benefits that could be presented by the cyber smart community, the challenges identified above should be addressed. Below are some of the strategic measures that can be taken into consideration to achieve a cyber smart community and thus enjoy the benefits it presents.

Emphasize cybersecurity and privacy

Smart technologies introduce new attack surfaces, which consequently pose new threats and attack vectors. Emphasizing cybersecurity is fundamental to creating a smart community that is secure, reliable, and resilient as well as protecting privacy. Privacy and cybersecurity are equally important as fundamental values and as an area requiring separate consideration and implementation approaches. Compliance with a

legislative privacy policy could serve as a pre-condition for private company use of public data assets in a smart community framework. Further emphasis should be focused on the following:

- Proactively testing smart community entities, such as user, infrastructure, applications, processes, and procedures to prevent phishing attacks, ransomware, social engineering schemes, and other cyber threats; equipping smart community entities with best practices for user names and passwords.
- Training and testing smart community entities on compliance with national cybersecurity regulations, such as the National Cybersecurity Policy Framework, the Cybercrime Bill, and the Protection of Personal Information Act.
- Training smart community entities to successfully report and respond to cyber security incidents.
- Dealing with the shortage of cyber security professionals within a smart community.
- Prioritizing replicability, interoperability, scalability, and sustainability.

To ensure rapid and successful deployment of smart solutions in its cities and communities, a model for this prioritization provides emphasis on establishing and demonstrating replicable, scalable, and sustainable models for incubation. This involves the deployment of interoperable, standards-based solutions using advanced technologies such as IoT and cyber-physical systems (CPS), and demonstrating their measurable benefits in cities and communities.

Leverage higher education research and associated workforce investments

Leverage higher education to develop a research agenda and capitalize on cybersecurity research, innovation, and industry investments of its universities, community colleges, technical institutes, and entrepreneurial communities. Industry investments in developing cyber security curriculums, course materials, instructional approaches, and pathways to commercialization are critical to effectively train the next generation of cyber smart communities in both technical and non-technical skills on cyber security defense.

6. Summary remarks

The main goal is to promote quality of life through the use of technology in ways that improve the efficiency of services and meet residents' needs. Government plays a critical role in smart communities at both national and local levels, at national level through the provision of funding, national policies and regulations, procurement services, and the development of best practices. Industry is also likely to play a key role here in developing countries.

Local governments are the place where citizens often have the most direct touchpoints with these new capabilities, including street maintenance and lighting, citizen engagement, transit, and other forms of service delivery. Most importantly, underlying all of these efforts should be an emphasis on access and equity across both cities and rural communities. It should allow all citizens to benefit from the advent of smart technologies, and demonstrate and articulate returns on investment so that both investors and citizens can fully understand the impact of smart community efforts.

The smart community model features a community targeted focus and implementations of this model are better suited to developing economies, where they can adapt, and be implemented in a manner tailored to the community itself. Every smart community is unique, because its components are based on the community itself.

A key factor to the successful development of a cyber smart community is full engagement and cooperation of all the role players that are involved in the endeavor, such as industry, education, government, and community. This united effort is essential and creates synergy, which allows individual initiatives to build upon each other for faster progress, resulting in the involved, informed, and trained critical mass necessary for transformation of how the entire community carries out its work.

The benefits that can be realized by individual communities can be achieved at even larger scale by the nation. Increasing the availability and usability of open data, improving services through the optimizations resulting from integrated analytic understanding across agencies and economies of scale in deployment of infrastructure assets all represent opportunities for the nation to become "smarter." At the same time, it is simultaneously setting an example and providing leadership that will enable local communities to realize their own priorities. It is crucial however to

note that the essential value gained by the “smartness” is not in the technology used or deployed, but the manner in which the solution serves the community and meets its most significant needs.

References

Albino, Vito, Umberto Berardi, and Rosa Dangelico. 2015. “Smart Cities: Definitions, Dimensions, Performance, and Initiatives.” *Journal Urban Technology,* 22 (January): 3–21.

Al-Kuwari, Saif. 2018. “South Africa: Remarks by the Deputy Minister of Higher Education and Training, Mr Buti Manamela to United Nations Office on Drugs and Crime – Education for Justice Initiative Global Hackathon Symantec Headquarters, Mountain View, California, USA.” *Database of Press Releases Related to Africa—APO-Source* (blog). July 11, 2018. https://appablog.wordpress.com/2018/07/11/south-africa-remarks-by-the-deputy-minister-of-higher-education-and-training-mr-buti-manamela-to-united-nations-office-on-drugs-and-crime-education-for-justice-initiative-global-hackathon-symantec/.

Allen, Barbara, Louise E. Tamindael, Sarah H. Bickerton, and Wonhyuk Cho. 2020. “Does Citizen Coproduction Lead to Better Urban Services in Smart Cities Projects? An Empirical Study on e-Participation in a Mobile Big Data Platform.” *Government Information Quarterly,* 37 no. 1: 101412. https://doi.org/10.1016/j.giq.2019.101412.

Benevolo, Clara, Renata Paola Dameri, and Beatrice D’Auria. 2016. “Smart Mobility in Smart City.” In *Empowering Organizations*, edited by Teresina Torre, Alessio Maria Braccini, and Riccardo Spinelli, 13–28. Cham: Springer International Publishing. https://www.researchgate.net/publication/284916936_Smart_Mobility_in_Smart_City_Action_taxonomy_ICT_intensity_and_public_benefits, Accessed: June 28, 2018.

Caragliu, Andrea, Chiara Del Bo, and Peter Nijkamp. 2009. “Smart Cities in Europe.” http://ideas.repec.org/p/dgr/vuarem/2009-48.html, Accessed: July 22, 2018.

Caperna, Antonio, Minervino, Guglielmo and Serafini, Stefano. "Smart Cities Local Community and Socioeconomic Development: The Case of Bologna" in Smart Economy in Smart Cities, Elsevier, pp. 601-53, 2017.

Chourabi, Hafedh, Taewoo Nam, Shawn Walker, José Ramón Gil-Garcia, Sehl Mellouli, Karine Nahon, Theresa A Pardo, and Hans Jochen Scholl. 2012. “Understanding Smart Cities: An Integrative Framework.” In *Proceedings of 2012 45th Hawaii International Conference on System Sciences*, 2289–2297. New York, NY: IEEE.

Correa, Teresa, Isabel Pavez, and Javier Contreras. 2017. “Beyond Access: A Relational and Resource-Based Model of Household Internet Adoption in Isolated Communities.” *Telecommunications Policy,* 41 no. 9: 757–68. https://doi.org/10.1016/j.telpol.2017. 03.008, Accessed: June 22, 2018..

CSIR Meraka. 2009. “Broadband 4 All™.” http://www.broadband4all.co.za/, Accessed: July 15, 2018.

Damiani, Ernesto, Ryszard Kowalczyk, and Gerard Parr. 2017. “Extending the Outreach: From Smart Cities to Connected Communities.” *ACM Transactions on Internet Technology* 18 (October): 1–7. https://doi.org/10.1145/3140543.

Department of Higher Education and Training. 2018. “Deputy Minister Buti Manamela: Remarks at United Nations Office on Drugs and Crime” Education for Justice Initiative Global Hackathon. South African Government. https://www.gov.za/speeches/deputy-minister-buti-manamela-remarks-united-nations-office-drugs-and-crime-education.

Dlamini, Zama, and Mapule Modise. 2013. “Cyber Security Awareness Initiatives in South Africa: A Synergy Approach.” *Case Studies in Information Warfare and Security: For Researchers, Teachers and Students*.

Graham, Stephen. 2001. *Splintering Urbanism: Networked Infrastructures, Technological Mobilites and the Urban Condition*. London and New York: Routledge.

Grobler, Marthie, and Zama Dlamini. 2012. “Global Cyber Trends a South African Reality.” In *Proceedings of IST-Africa 2012 Conference* edited by Paul Cunningham and Miriam Cunningham. Dublin: IST-Africa Institute and IIMC.

Grobler, Marthie, Zama Dlamini, Sipho Ngobeni, and Aubrey Labuschagne. 2011. “Toward a Cyber Security Aware Rural Community.” In *Proceedings of the 2011 Information Security for South Africa (ISSA) Conference*, 7. http://researchspace.csir.co.za/dspace/handle/10204/5183.

Gurstein, Michael. 2013. “Review of J. Phahlamohlaka (ed.), Community-driven Projects: Reflections on a Success Story a Case Study of Science Education and Information Technology in South Africa.” *The Journal of Community Informatics,* 9 no. 4.

Spatial and Economic Smart Strategies for the 21st-Century Metropolitan Caperna, Antonio, Tracada, Eleni, Minervino, Guglielmo, Alatalo, Elina, and Maria Cerreta. 2019. Spatial and Economic Smart Strategies for the 21st-Century Metropolitan City of Naples. Advances in 21st Century Human Settlements. Springer, Singapore Available in: https://link.springer.com/chapter/10.1007%2F978-981-10-8588-8_12, Access: August 26, 2019.

International Telecommunication Union (ITU). 2017. “ITU: ICT Facts and Figures 2017.” *ETrade for All*” (blog). August 21, 2017. https://etradeforall.org/itu-ict-facts-figures-2017/.

Kehoe, Mike, Michael, Cosgrove, Steven De Gennaro, Colin Harrison, Wim Harthoorn, John Hogan, John Meegan, Pam Nesbitt, and Christina Peters. 2011. “Smarter Cities Series: A Foundation for Understanding IBM Smarter Cities.” *Redguides for Business Leaders, IBM*.

Kesswani, Nishtha, and Sanjay Kumar. 2018. “The Smart-X Model for Smart Cities.” In *Proceedings of the 2018 IEEE 42nd Annual Computer Software and Applications Conference* 755–60. https://doi.org/10.1109/COMPSAC.2018.00112.

Kiganda, Antony. 2016. “Smart Cities in South Africa Verses Smart Communities.” *Construction Review Online* (blog). 13 April 2016. http://constructionreviewonline.com/2016/04/smart-cities-in-south-africa-verses-smart-communities/.

Kramer, William J, Beth Jenkins, and Robert S. Katz. n.d. “The Role of the Information and Communications Technology Sector in Expanding Economic Opportunity: Eldis.” Accessed July 7, 2020. https://www.eldis.org/document/A36329.

Kummitha, Rama Krishna Reddy, and Nathalie Crutzen. 2017. “How Do We Understand Smart Cities? An Evolutionary Perspective.” *Cities* 67 (July): 43–52. https://doi.org/10.1016/j.cities.2017.04.010.

Meraka. 2009. “Mesh Networks.” 2009. http://www.meshnetworks. com/.

Nam, Taewoo, and Theresa A. Pardo. 2011. “Conceptualizing Smart City with Dimensions of Technology, People, and Institutions.” In *Proceedings of the 12th Annual International Digital Government Research Conference: Digital Government Innovation in Challenging Times* (dg.o ’11), 282–91. New York, NY: ACM.

Navigant Research (2011). Smart cities; intelligent information and communicationstechnology infrastructure in the government, buildings, transport, and utilitydomains (research report). http://www.navigantresearch.com/research/smart-cities, Accessed: 09 July 2018.

Partridge, Helen L. 2004. “Developing a Human Perspective to the Digital Divide in the ‘Smart City’ ”. In *Australian Library and Information Association Biennial Conference*, September 21–24.

Phahlamohlaka, Jackie, Zama I. Dlamini, Linda Malinga, Sipho Ngobeni, and Thami Mnisi. 2015. *A Practise-Based Theory of SEIDET Smart Community Centre Model*. IEEE. https://doi.org/10.1109/ISTAS.2015.7439411.

Popescu, Gheorghe H. 2015. “The Economic Value of Smart City Technology.” *Economics, Management and Financial Markets* 10 no. 4: 76. https://www.questia.com/library/journal/1P3-3915611821/the-economic-value-of-smart-city-technology.

Rios, Patrice. 2012. “Creating ‘The Smart City.’” Available at: https://archive.udmercy.edu/bitstream/handle/10429/393/2008_rios_smart.pdf?sequence=1, Accessed: June 18, 2018.

Roux, Kobus, 2009. “Broadband for All (BB4all)™.” *CSIR Science Scope* 3 no. 3: 16–17.

Salemink, Koen, Dirk Strijker, and Gary Bosworth. 2017. “Rural Development in the Digital Age: A Systematic Literature Review on Unequal ICT Availability, Adoption, and Use in Rural Areas.” *Journal of Rural Studies* 54 (August): 360–71. https://doi.org/10.1016/j.jrurstud.2015.09.001.

Siebeling, Tom, and Henny A. Romijn. 2004. “A Novel Approach to Innovation Processes in Community Driven Projects: How an Extended Learning Selection Model Explains the Success of SEIDET, an Educational Community Development Project in Rural South Africa.” MSc thesis, Faculty of Technology Management, Eindhoven University of Technology, the Netherlands.

Silva, Bhagya Nathali, Murad Khan, and Kijun Han. 2018. “Toward Sustainable Smart Cities: A Review of Trends, Architectures, Components, and Open Challenges in Smart Cities.” *Sustainable Cities and Society* 38 (April): 697–713. https://doi.org/10.1016/j.scs.2018.01.053.

Xia, Feng, and Jianhua Ma. 2011. “Building Smart Communities with Cyber-Physical Systems.” *SCI '11: Proceedings of 1st International Symposium on From Digital Footprints to Social and Community Intelligence*, September 2011, 1–6 https://doi.org/10.1145/2030066.2030068.