MULTI-STAKEHOLDER ENGAGEMENT IN DEVELOPING NATIONAL CYBER SECURITY TO ENHANCE NATIONAL DEVELOPMENT: THE QUEST FOR MULTI AGENCY COLLABORATION

by:

Jacqueline Chepkoech and Mugah Michael Sitawa

Email: chepruto80@gmail.com

Abstract

The research sought to examine the effectiveness of multi-stakeholder engagement in developing national cyber security capacity to enhance national development with a focus on KDF. Specific objectives were to determine the contributions of KDF and academic institutions in national cyber defence capacity enhancement and determine the effectiveness of the multi-stakeholder framework spearheaded by KDF in national cyber defence capacity enhancement to bolster national development. The theories informing the study were Risk Theory of Safety and Security, and Integrated System Theory of Information Security Management using both diagnostic and descriptive research design methods. The study used a sample size of 100 participants drawn from Kenya security agencies (50) (KDF, NIS, and NPS), Kenyan universities and research institutions (25), and another (25) from the corporate and civil societies comprising the Communication Authority Kenya, and Kenya Information Communication Network (KICTANET). The data was collected using open-ended questionnaires sent to the participants via email. Purposive and snowballing sampling techniques were used, while thematic analysis was used for the qualitative data analysis, expressed in narrative and percentages as per themes therein. Some of the study findings are that, while KDF has been integrated into Kenya's multi-agency teams on cyber security, their contribution has been minimal thus far. However, KDF continues to play an advisory role to the government on digital threats. Further, academic institutions have remained theoretical on cybersecurity matters, with just a few universities offering such training. In addition, while a multi-stakeholder approach is most appropriate to handle cybersecurity threats, there lacks a

proactive multi-agency framework to quell such threats, create awareness, and a response team in the event of cyber-attacks. This study recommends the creation of a multi-stakeholder team to develop home-grown solutions and increase the role of KDF in cybersecurity multi-agency collaboration and advisory roles as well as research. Further, the study recommends, a proactive center for cybersecurity response team to be established in Kenya, spearheaded by the KDF.

Keywords: *Multi-stakeholder, Cybersecurity, KDF, National Development*

Introduction

Cybersecurity relates to the protection of individuals and organizations using internet-connected devices and systems like software and hardware among other electronic devices from potential cyber threats or attacks (Craigen, Diakun-Thibault & Purse, 2014). The increased reliance on information systems pervading all aspects of human life coupled with globalization has introduced the fifth dimension of warfare in the cyber domain (Robinson, Jones & Janicke, 2015). Implementation of information systems is a force multiplier in economic development (Breda, Barbosa & Morais, 2017). However, the introduction of information systems has resulted in an unprecedented increase in cyber threats on a global scale threatening economic and national security with a lack of a coordinated approach at the national level to deal with the threats. Cybersecurity threats relate to malicious acts designed to damage or loss of data and disrupt digital life. Common cyber threats are virus attacks, denial of services, data breaches, and Advanced Persistent Threats (APT) conducted by either State or non-state actors (Humayun et al., 2020). Threat actors range from corporate spies, hostile nation states, criminal organizations like terror groups, and lone hackers, among others (Rollins, 2009). These threats have the capability of delivering devastating strategic effects on critical infrastructure with the potential of crippling effects on the national economy. The cyberspace therefore presents a global-sized threat with potential for high-level collateral damage that does not conform to international legal requirements nor the principles of distinction and proportionality and which introduces a high number of non-combatants to the battle space.

Some of the most severe attacks are state-sponsored attacks targeting critical infrastructure and conducted as a precursor for war on the other dimensions of warfare (Akoto, 2021). The cyber-attacks are meant to cripple a nation's ability to sustain its war or defense efforts by targeting its industrial base. A case in point was the attacks on the Estonian critical infrastructure in 2007 and the Russian State-Sponsored cyber-attacks on the Ukrainian power supply and transport system before the onset and during the conduct of the current military offensive (Czosseck, Ottis & Talihärm, 2011). Cyberspace, however, unlike other dimensions of warfare, presents a challenge in the regulation and application of national and international legal requirements and is devoid of any national boundaries. It is unimpeded by geographical distances, and capabilities are unrestricted by the economic capacities of states or perpetrators (Geers, 2010). Cyber threats harm economic development while the cost of cyber security solutions remains prohibitive. There is thus, the need for the development of capacity for securing cyberspace for economic security (Geers, 2010). Information technology, software development, and cybersecurity skills are some of the soft skills that are cheap to train with high returns in comparison to the prohibitive cost of cyber solutions.

Cybersecurity solutions have currently emerged as a cornerstone for export sales in the international security market currently topped by the US, China, Japan, and France which account for a third of the global security market (Sales, 2018). The development of the national cyber security skill capacity enhances the national posture for cyber defence and economic security. In this regard, software and cyber skills development will not only be exported as a foreign exchange earner in the regional and global security market but also facilitate the protection of the national cyberspace (Sony & Aithal, 2020). Cyber skills will also serve as a source of employment, improving livelihoods and therefore contributing to national development and security through reduction in predisposition to crime and radicalization caused by poverty hence an effective tool towards achieving total human security. In addition, with cyberspace as the new frontier of warfare, mechanisms have been put in place by regional and international organizations and security blocks for collective defense and response to cyber threats (Wolter, 2013). The UN cybersecurity mandate is to enhance the capacities of member states to deal with the exploitation of cyberspace in aspects threatening international peace and security, e.g. terrorism and state-sponsored attacks.

The U.S embraced a multi-stakeholder approach to cybersecurity in 2016 endorsing a national initiative for cybersecurity education, spearheaded by the National Institute of Standards and Technology (NIST) (Thierer, 2021). The multi-stakeholder initiative in the U.S for improved awareness and preparedness for cybersecurity-related threats was funded by the Department of Commerce for regional alliances and multi-stakeholder partnerships (Ciglic & Hering, 2021). The core goal was to promote cybersecurity education in the U.S, and workforce development to fight cybersecurity threats. The most notable aspect of the milestone made by the U.S is the level of multidisciplinary cooperation for common goals.

The Massachusetts Institute of Technology (MIT) has played a fundamental role in cybersecurity training, and cybersecurity research initiatives to inform pertinent policies (MIT, 2022). MIT has successfully performed internet policy research, with a significant impact in boosting U.S cyberspace security. MIT has significantly impacted cybersecurity research and policy development in the U.S, as well as enhanced cybersecurity awareness through personnel training. Similarly, China has made a milestone breakthrough in cyberspace security by embracing policy responses in developing effective and efficient cyberspace security (Austin, 2018). China sought diplomatic relations with the EU to cooperate in cybersecurity prospects for policy and infrastructure development, prompting the need for interdisciplinary collaboration within and outside the country. Cybersecurity enhancement in South Africa, unlike anywhere else in the African context, has been implemented through schools. South Africa, akin to the U.K has adopted schools as critical institutions in promoting cybersecurity awareness in the digital age (Kritzinger, Bada & Nurse, 2017). Notably, in South Africa and the U.K, education and skills prioritization for cybersecurity are informed by the stakeholders in the economy. The schools, government, and academia play an active role in cybersecurity initiatives in South Africa, with recommendable outcomes (Ciglic & Hering, 2021: Kritzinger, Bada & Nurse, 2017). On the other hand, Egypt has also sought to integrate cybersecurity training in schools to boost awareness and professional development (Alsmadi & Zarour, 2018). The New Education Cybersecurity Program has evolved over the years in personnel training and innovation to improve cyberspace prospects. In the Rwandan ICT sector, numerous stakeholders have contributed to the development of ICT policy for the improvement of the cybersecurity policy in the country (Bowman, 2015). The National Information and Communication Infrastructure (NICI) is the epitome of the cybersecurity policy in Rwanda, developed in 2005 through multi-stakeholder collaboration in the ICT sector.

Kenya has experienced a surge in cyber-attacks in the recent past, with a record count of about 860 million incidences in the past year (Kenya National Computer and Cybercrime Coordination Committee, 2022). Frequent cyber-attacks in Kenya are denial of services, spyware, distributed denial of service, malware/virus, social engineering, and phishing (Joshua and Doreen, 2023). The target of the majority of cyber-attacks is critical communication and information infrastructures, especially with the increased social media usage. In 2017, Kenya faced 7.7 million cyber-attacks. In July 2023, cyber-attacks in Kenya disrupted access to 5,000 Kenyan government services offered online including Visa, driving license application portal, passport, online train booking portal, and mobile money transactions (Africa News, 2023). About 79% of the cyber-attacks in Kenya have been executed by criminals infiltrating the computer systems of numerous organizations across the country (Africa News, 2023). Further, 14% of the attacks involved malicious software overloading traffic, while the rest targeted web-based applications. Besides, Kenya is ranked third after Nigeria and South Africa as the most targeted by cybercriminals in Africa. Overall, there is cause for alarm for the security institutions like the Kenya Defence Forces (KDF), to take up an active role in defending the digital infrastructure, to foster socioeconomic prosperity.

This study examines the role of Kenya Defence Forces (KDF) multi-stakeholder engagement in developing national cybersecurity capacity, to bolster national development. The study-specific objectives were to assess KDF, and academic institutions' contribution to National Cyber defence capacity enhancement, and the effectiveness of a multi-stakeholder framework spearheaded by KDF in National cyber defence enhancement to foster national development.

THEORETICAL BASIS

The Risk Theory of Safety and Security

The Risk theory is used in scientific disciplines in the threats identification, risk specification, and determination of potential countenance strategies. Risks, according to the risk theory of safety and security, emanate from the objective existence of threats (Lukas, 2016: Ludek, 2016). There exists consciously controlled acting and uncontrolled acting for a given complex part for risks to emerge. The theory underpins, in the course of elements behaviors, interactions occur, and unfortunately, some of the interactions are negative, and could render adversities. A security incident, thus emerges from negative interactions (Lukas, 2016). Through risk identification, an

evaluation of negative acts or threats is done, defining potential impacts (Ludek, 2016). Further, measures to counter pertinent impacts are defined. In addition, risk management strategies are formulated for the fulfillment of the function of the pertinent reference object(s).

This study applied the risk theory of safety and security in defining the strategy for cybersecurity enhancement. Pertinent concepts from the theory utilized are Cyber threats identification, impacts definition, and cyber threats countenance definition based on the scale of threats impacts. Similarly, the concept of risk management, in this case being the multi-stakeholder engagement, spearheaded by KDF, is largely informed by the risk theory of safety and security.

Integrated System Theory of Information Security Management

The Integrated systems theory of Information security management theory was proposed by Kwo-Shing, which combines security policy theory, risk management theory, management systems theory, and control and auditing theory as well as contingency theory, to establish the information security management theory (Hong et al., 2003). The theory denotes integrated systems theory is fundamental in delving understanding of information security management, by defining pertinent strategies and predicting managerial outcomes (Hong1 et al., 2003). The theory acknowledges the increased threats to data security with internet usage, amidst the presence of unauthorized users. As such, the theory proposes the adoption of effective information security management ideals to secure data for organizations and individuals.

This theory was useful in this study, in demystifying contemporary data security risks, and the need for adoption of effective internet data security management strategies to protect individuals and organizations. Further, the theory helps in denoting the essence of integrating multi-agency efforts in defining cybersecurity prospects, through improved information security management.

METHODOLOGY

This study sought to examine the contribution of KDF and academic institutions in national cyber defence capacity enhancement, and the effectiveness of KDF-spearheaded multi-stakeholder engagement to bolster national cyber defence capacity for national development. In this regard a qualitative study design was applied, using both primary and secondary data. Primary data was collected by means of an unstructured questionnaire to enable comprehensive data collection from the respondents by utilizing open-ended questions (Kazi, & Khalid, 2012). Questionnaires were

piloted among the KDF personnel, and approved by the NDU-K study supervisor for dissemination. The study participants were contacted via the phone for briefing about the study, and sought consent for their participation. The questionnaires were then administered via email, for the participants to fill them and send back within seven days. Purposive or judgmental and snowball sampling techniques were used to identify the study participants. In this regard, Security agencies, specific information technology (IT) oriented Kenyan Universities, and corporate and civil society were chosen. Potential bias in this sampling was overcome by ensuring questionnaires were filled independently by the participants.

The target population was the key stakeholders in Kenya's national security agencies and academia mainly Kenyan Universities. Specific institutions of the target population in Kenya comprised Kenya Defence Forces (KDF), the National Police Service (NPS), officials from National Intelligence Service (NIS), Kenyan public/private universities with orientation to computer science and technology courses, the officials from Kenya Communication Authority (CA), and Kenya information communication and technology network officials.

A total of 100 participants were reached, comprising 50 from national Security Agencies (25 from KDF, 15 from NPS, and 10 from NIS). Another 25 were from academia and research institutions (20 from universities and 5 from research institutions). Further, 25 were from corporate and civil society, mainly the KICTANET. Thematic qualitative data analysis method was used in which themes were identified from the questionnaires, and compiled into percentages for discussion.

For the secondary data, the annual reports and publications by the respective institutions on the study topic were utilized. These included government agencies such as the Communication Authority of Kenya (CAK) amongst others, and non-governmental organizations on Cybersecurity like Kenya ICT Action Network (KICTANET), and diverse publications by Kenyan universities and KDF.

FINDINGS AND DISCUSSION

Analysis of the Questionnaire

Out of the 100 questionnaires distributed, seventy were returned dully filled and were used to compute the results. Five (5) of the questionnaires were subtracted from the total sample due to missing data. The data collected from the questionnaires was subjected to frequency counts, and

ultimately the percentages based on the emerging themes from the responses. The biographic information of the participants comprised 45% female and 55% male. Further, 20% fell in the bracket 25-30 years, 30% were in the age bracket 30-40 years, 15% were aged 40-50 years, and the rest (35%) were above 50 years of age. Further, 20% were diploma level, 50% were degree holders, while 10% were post-graduate diploma/masters' level. Further 10% had doctorate qualification.

The participants were also asked if they had encountered any form of cyber-attack, which revealed that, 75% of the participants had such encounters. Some of the common attacks included hacked social media accounts, denial of service, social engineering, and phishing instances where one is duped into clicking an insecure link. Phishing had a prevalence of 45% among the participants, denial of service 10%, and hacked social media accounts had a prevalence of 60%. The organizations listed by the participants that should be charged with cybersecurity concerns include the KDF with a prevalence of 25%, the Directorate of Public Prosecutions (DPP) with a 5% prevalence, the Communications Authority of Kenya (CAK) with a prevalence of 65%, and the National Computer and Cyber Crimes Co-ordination Committee (NC4) with a prevalence of 45% of the study participants. The 90% of the study participants agreed with the view that a multi-agency strategy would enhance cyber threat management through the creation of synergy enhancing security leading to economic development. On the other hand, 10% demonstrated the need for individual awareness about cyber threats to avert pertinent frequent attacks. Overall, the participants believed that a multi-stakeholder engagement could improve national development through enhanced cybersecurity capacity development.

KDF Contributions in National Cyber Defense Capacity Enhancement

A total of 35% of the KDF study participants stated the institution has embraced a multi-stakeholder approach to address cyber security issues in the recent past. Some of the cited efforts included the incorporation of military personnel in the National Computer and Cyber Crimes Coordination Committee (NC4) and the Kenya Computer Incident Response Team (KE - CIRT) Bundi, Mbaya & Muriuki, (2018), reiterated similar integration efforts exists in the KDF institution, where the pertinent teams work in collaboration with the other stakeholders in the cybersecurity docket. The NC4 is a multiagency institution that provides strategic guidance, coordination, and advisory services to both the public and private sector strengthening the security

resilience and cyber security capacity of the stakeholders. Kenya Computer Incident Response Team (KE-CIRT) is also a multi-agency government organization that facilitates collaboration and multi-stakeholder engagement. The Kenya Information and Communications Act, of 1998, mandates the Communications Authority of Kenya (CAK) to develop a national cyber security management framework through the establishment of a national Computer Incident Response Team (CIRT) (Wanjiku, 2009). However, it emerged that, while such teams exist, their impacts have not been felt fully in the economy, especially with the notable upsurge in cyber-attacks at both individual and organizational levels.

The KDF has a role to advise the government about potential threats to the critical information infrastructure as denoted by 20% of study participants. On the other hand, the Kenya National Computer Cybercrimes Coordination Committee/NC4, (2023) recounts, KDF play advisory role to the government on cyber-related threats for mitigation. However, 45% of study participants felt that the KDF has not made a significant contribution to the digital infrastructure in Kenya. The ultimate goal is to facilitate national capacity development by mitigating cyber-attacks and monitoring as well as mobilizing a collective cyber response to enhance national cyber security. With a prevalence of 70% of study participants, the study established the KDF needs to do more to boost a secure cyberspace in Kenya. The terrorists, among other militia groups, also target Kenya's digital space with the ultimate goal of causing harm to such as the banking sector which has been attacked frequently (Fred, 2016). Some of the study participants (25%) associated some cyber-attacks especially on the government digital platforms with the Al-Shabaab. The implications are that the KDF's role in fighting terror attacks is not limited to physical battles but also in the digital space. Kenyans have increasingly become vulnerable to cyber-attacks because there are insufficient safeguards in cyberspace amid increased reliance on the internet.

The Roles of Academic Institutions in Enhancing National Cyber Defense Capacity

The contribution of academia is critical to the defense of national cyberspace, however, the academic potential remains highly unexploited, and its role in cyber defense is minimal with a highly theoretical approach (Kallberg & Thuraisingham, 2012). Similar findings were established in this study where 65% of the participants delved that, the academic institutions have remained quite theoretical in Kenya as regards cyberspace infrastructure development. The academic knowledge development role ensures maximum utilization of national resources including the academic infrastructure and human resources including students at their highest level of cognitive

capacity (Catota, Morgan & Sicker, 2019). Such advances from academic institutions facilitate national cyber defense and the development of homegrown solutions reducing vulnerabilities posed by outsourced cyber solutions.

On the other hand, 20% of the study participants denoted, that there are just a few universities in Kenya that offer cybersecurity degrees and courses. Lack of homegrown cyber solutions creates dependence on outsourced solutions presenting an exploitable national security vulnerability (Forrester, Lopez & Valentina, 2022). The insufficiency of the required expertise can be addressed through academia by analyzing problems in cyberspace. Fortunately, security agencies like the military (KDF) may spearhead a multi-stakeholder framework to facilitate problem identification and define potential remedies for implementation. The academic institutions helps formulate course and curriculum development and software development for homegrown solutions.

Kaibiru et al, (2023) indicates a dire national skill deficit and the need to address the gap through curriculum interventions. According to the study, 13.2% of national universities offer cybersecurity degree programs. Further improvements in the courses can be implemented through a military-spearheaded multi-pronged approach comprising the Integration of cybersecurity in schools and other academic institutions. Similar findings were established in this study where 20% stated there are very few institutions training cyber security-related courses in Kenya. The learning institutions ought to integrate cybersecurity courses in every discipline as a common course and the introduction of the skills at lower educational levels through the CBC was spearheaded as denoted by 45% of the study participants. In this endeavor, the Ministry of Education in conjunction with the military through National Defence University-Kenya NDU-K could offer oversight for effective program implementation across the country. However, such an approach would require a parliamentary Act.

The launch of cybersecurity courses as common courses in universities and the Competence curriculum (CBC), will facilitate the utilization of Universities and research institutions as national resources for the development of cyber capacity as denoted by 20% of study participants. Lehto, (2015) underpinned, that the learning institutions of higher learning can conduct national cyber threats analysis in conjunction with security agencies through an integrated academic data analysis program to develop cyber solutions for existing threats. The focus of such a development in the learning institutions is to facilitate maximum utilization of existing academic infrastructure like the data analytics center that exists in JKUAT (Kariuki, 2017). The use of local tools and facilities

would help in the development of homegrown solutions in response to cyber threats to address vulnerabilities as denoted by 55% of study participants. Besides, 90% of the study participants denoted the need for the development of homegrown solutions to cybersecurity threats. The direct involvement of ministries of education, commerce and industry, the State Department of Youth Affairs, and the Ministry of Information, Communication and Technology (ICT) would be crucial, as cited by 35% of the study participants. Overall, the effective multi-stakeholder approach to cybersecurity in Kenya is essential with the rising cases of cyber-attacks.

Information communication technology (ICT), software development, and cybersecurity skills are soft skills, cheap to train with high returns in comparison to the prohibitive cost of cyber solutions as identified by 95% of participants from academic backgrounds. Cybersecurity solutions have currently emerged as a cornerstone for export sales (Westerlund & Rajala, 2014). In this respect, the development of the national cyber security skill capacity enhances the national posture for cyber defense and economic security. Software development and cyber skills will not only facilitate protection of the national cyberspace but can also be exported as a foreign exchange earner in the regional and global security market as denoted by 25% of the study participants. It will also serve as a source of employment improving livelihood and therefore contributing to national development hence an effective tool towards achieving total human security.

Multi-Stakeholder Framework Effectiveness in National Cyber Defense Capacity Enhancement

Cyberspace is the 5th dimension of warfare and just as it diffuses national boundaries it also presents a common space to all stakeholders, from the micro individual to national-level systems (Wells, 2016). A Multi-stakeholder engagement in cyber security is complex and requires military spearheaded multi-agency approach and an aggressive development of capacity. This requires a graduated approach capitalizing on academic institutions, the Ministry of Defense, education, commerce and industry, communication and digital economy, and the State Department for Youth Affairs. Similarly, 95% of study participants denoted the increased need for multi-stakeholder cooperation in Kenya to quell the cyber threats and frequent attacks. Jone, (2021) reported the viability of a multi-agency strategy is pegged on the fact that outsourced cyber solutions have a prohibitive cost and expose cyberspace to exploitable vulnerabilities in the age of IT dependence. The collaborative framework therefore provides for synergy facilitating maximum utilization of

scarce resources while enhancing the national cyberspace defense posture and contributing towards national economic development.

Munyua (2016) revealed that multi-stakeholder engagement will improve the national cyberdefence capacity by revolutionizing collaboration on cybersecurity. Multi-stakeholder engagement will improve national cyber defense capacity as it does not just enhance collaboration but also offers solutions to most cybersecurity-related issues. Similarly, this study established, that lack of multi-agency collaboration contribute to heightening cyber security attacks in Kenya with a 56% response rate from the participants. The study participants in this regard, delved into, how a multi-stakeholder framework allows for resource mobilization for synergy. Such an approach provides a framework for information sharing, capacity development, threat analysis, and response to facilitate national development.

A multi-agency framework, like the National Cyber Security Secretariat and the National Computer and Cyber Crimes Coordination Committee (NC4) in this case, can be enhanced to facilitate a military-spearheaded multi-stakeholder/multi agency framework to facilitate collective response through the full operationalization of existing multi-agency institutions like KE-CIRT and NC4 ((BundiMbaya & Muriuki, 2015). With a prevalence of 45% of study participants, this study established that the KDF has the potential to lead a proactive cyber defense team/multi agency team to bolster safety in Kenya's cyberspace. However, 20% of participants stated, that CA should lead the multi-agency team in such endeavors. However, overall, there was consensus that KDF plays an influential role in the security prospects of Kenya, and so it should be in cyberspace. An effective multi-agency framework would address the Lack of a common information-sharing platform and collective response and preparedness like US PPP (Public Private Partnership) for information sharing (Maude, 2013). The Public and private sectors in U.S, work in collaboration on matters cybersecurity. The creation of a platform for risk analysis and mitigation utilizing all national resources including academia allows all data traffic to be channeled through a common platform to facilitate the analysis of threats and development of cyber solutions.

On the other hand, corporate institutions are critical stakeholders in cyberspace and have leveraged information technology to advance economic development (Reveron & Savage, 2020). The sector, especially the banking industry in Kenya has been the hardest hit by cyberattacks resulting in huge losses with a direct effect on the economy (Tariq, 2018). The same hackers can access different

banks with isolated as opposed to integrated approaches to cyber defense. Cyber security threats to the financial institutions can be mitigated through an information-sharing platform and the implementation of a collective cyber response framework, as established in this study. Multi-stakeholder collaboration allows for an integrated approach to address the existing cybersecurity skill gap in cybersecurity (Tagarev & Sharkov, 2016). In this regard, collaborative efforts of forensics and Cyber Law developed by the government, and the input of security agency institutions such as NDU-K would certainly bear the most fruit as denoted by 70% of the study participants. While there have been some attempts to enhance multi-stakeholder efforts, minimal progress have been achieved in defining a proactive team in this respect.

Multi-stakeholder framework would provide the best strategy for exploiting the threats presented by reliance on information systems as stipulated by 75% of the study participants. Besides, 90% of study participants denoted confidence in the KDF-led multi-agency cyber defense team, citing previous interventions of KDF in other public sectors like the Kenya Meat Commission. However, the multi-stakeholder cybersecurity framework in Kenya is not comprehensive and lacks effective implementation, owing to collaboration between the public and private sectors in cybersecurity remaining substantially low. The defence efforts in cyberspace are weakened by the absence of a proactive multi-stakeholder in Kenya. As such, Kenya suffers from an uncoordinated cybersecurity framework development (Sang, 2022). A military-spearheaded multiagency framework for the mobilization of national resources for capacity development to facilitate the exploitation of cyberspace for economic development through sustainable cyber defence is thus fundamental in Kenya.

Due to the complex landscape of the cyber domain, a multi-stakeholder engagement best presents the strategy for the mobilization of national resources for capacity development, which would therefore incorporate the development of a framework for multi-stakeholder engagement (Ciglic & Hering, 2021). The multi-stakeholder engagement strategies have been implemented in countries like the US, Egypt, and South Africa among others. Locally, a multi-stakeholder engagement for resource mobilization and synergy would allow for efficient collective cybersecurity threat analysis, capacity building, information sharing, and collective response as denoted by 85% of study participants.

Conclusion

Cybersecurity is a collective multi-stakeholder responsibility that requires collaborative action to achieve national cybersecurity capacity development. Numerous efforts to multi-agency approach for cybersecurity have been made in Kenya, comprising NC4, and Kenya Computer Incident Response Team integration with the KDF, however the inputs from the KDF into the team have seemingly been low. The most remarkable role of KDF on cybersecurity roles in Kenya is the government advisory on such threats. Through improved channels and strategies to manage the Cyber threats in Kenya, a secure cyber space shall be realized for full exploitation of the pertinent opportunities to achieve socioeconomic development.

The academic institutions have made minimal efforts to boost the Cyber security resilience in Kenya. There are very few universities offering comprehensive courses on Cyber security. More efforts are of the essence to boost awareness, through training of personnel at both CBC levels and the institutions of higher learning on cyber security matters. It is important for the learning institutions to not only develop appropriate curriculum on cyber security, but also work in collaboration with other agencies like the KDF. Overall, there are skills deficits in cybersecurity in Kenya, which partially informs the prevalence of the cyber-attacks in Kenya in the recent past.

While Kenya has made good progress in securing the cyberspace, there lacks a proactive multi-agency cybersecurity team to handle the emerging cyber threats. The way KDF ensures physical security of Kenya, it is in the very same spirit they ought to take over the cyber space for a secure digital economy. With the increased online consumers, the risks of digital warfare is inevitable, hence the need for heavy presence of not only the KDF, but also other agencies as well working in collaboration. The key stakeholders in the cybersecurity in Kenya should be Kenya communication authority, security agencies, research institutions and the Universities, all spearheaded by the KDF. Besides, corporate institutions from the private sector, such as the banking sector should not be left out in the cybersecurity mitigation and response team since they are common target by the cyber criminals.

Recommendations

This study recommends the development of home-grown cybersecurity solutions, through effective multi-stakeholder collaboration. Potential stakeholders in this endeavor are the academic institutions, the government of Kenya especially parliament, stakeholders in the security docket, communication authority, corporate sector especially the private sector, and ultimately the KDF offering insights and advisories on pertinent threats.

The study also recommends an increased role of the KDF in cyberspace security enhancement through, not only participation in multi-agency teams like NC4, but also research. This study established that KDF has been integrated into the cybersecurity teams but thus far their inputs and impacts have been minimal.

It is also recommended that academic institutions should initiate cybersecurity-related programs to boost the personnel pool in Kenya and increase awareness through the provision of common courses at both CBC and higher learning levels. This study established few universities are offering cybersecurity-related courses, hence a skills deficit.

The study recommends the creation of a center for cybersecurity response, and information sharing that incorporate agencies from academia, security agencies, corporate institutions, and others, spearheaded by KDF. This study established, that there is no proactive multi-agency cyber-attack response team.

References

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber-attacks. *Journal of Peace Research*, *58*(5), 1083-1097.

AfricaNews. (2023, October 3). *Kenya hit by record 860m cyber-attacks in a year*. Africanews. https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a-year//#

BundiMbaya, K., & Muriuki, P. (2018). ASSESSMENT OF INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA.

BundiMbaya, K., & Muriuki, P. (2017). ASSESSMENT OF INFORMATION COMMUNICATION TECHNOLOGY CRIMES AND OFFENCES IN KENYA.

Czosseck, C., Ottis, R., & Talihärm, A. M. (2011). Estonia after the 2007 cyber-attacks: Legal, strategic and organizational changes in cyber security. *International Journal of Cyber Warfare and Terrorism (IJCWT)*, *1*(1), 24-34.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology innovation management review*, *4*(10).

Catota, F. E., Morgan, M. G., & Sicker, D. C. (2019). Cybersecurity education in a developing nation: The Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), tyz001.

Ciglic, K., & Hering, J. (2021). A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy*, *6*(3), 360-374.

Communications Authority of Kenya. (2018, July 13). *Cyber security overview*. https://www.ca.go.ke/industry/cyber-security/overview/

CA. (2021, August 10). *NATIONAL KE-CIRT/CC CYBERSECURITY REPORT APRIL TO JUNE 2021*. KE-CIRT – Communications Authority of Kenya. https://ke-cirt.go.ke/wp-content/uploads/2021/07/Quarter-4-FY-2020_21-National-KE-CIRT_CC-Cybersecurity-Report-Public-Version.pdf.

Fielder, J. D. (2021). Cyber security in Kenya: Balancing economic security and internet freedom. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 543-552). Routledge.

Fred, M. (2016, August 4). *DEFENCE CS WARNS KENYA AT RISK OF CYBER ATTACKS*. The Computer Society of Kenya. https://www.cskonline.org/about-us/kenya-ict-press/975-defence-cs-warns-kenya-at-risk-of-cyber-attacks

Forrester, J., Lopez, M. L., & Valentina, M. D. (2022). Marketing a cybersecurity Awareness Solution in LPA Contexts. In *Cybersecurity Awareness* (pp. 161-181). Cham: Springer International Publishing.

Geers, K. (2010). The challenge of cyber-attack deterrence. *Computer Law & Security Review*, *26*(3), 298-303.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243-248.

Hong1, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, *11*(5), 243-248.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering*, *45*, 3171-3189.

International Telecommunication Union. (2019). *Towards a Multi-stakeholder initiative to develop and improve national cybersecurity strategies* (2019). https://www.itu.int/en/ITU-T/Workshops-and-Seminars/cybersecurity/Documents/PPT/S1P1_Serge_Zongo.pdf.

Jones, R. (2021, May 26). *Cybersecurity outsourcing: Unnecessary cost or clever investment?* Infosecurity Magazine. https://www.infosecurity-magazine.com/opinions/cybersecurity-outsourcing-cost/

Joshua, K. and Doreen, A. (2023, August 22). *Kenya's digital infrastructure under threat? A look at Anonymous Sudan's thwarted cyberattack attempt and its implications for Kenya's digital systems*. Centre for Intellectual Property and Information Technology law. https://cipit.strathmore.edu/kenyas-digital-infrastructure-under-threat-a-look-at-anonymous-sudans-thwarted-cyberattack-attempt-and-its-implications-for-kenyas-digital-systems/#

Kariuki, K.J. (2017, February 21). New Centre to Drive Data Sciences & Business Analytics in Africa Unveiled at JKUAT. https://www.jkuat.ac.ke/departments/it/?p=4021

Kivuva, M. (2019). *Cybersecurity in Kenya: Priorities for 2019*. Kenya ICT Action Network. https://file:///C:/Users/ictmanager/Downloads/Cybersecurity-in-Kenya-priorities-for-2019.pdf.

Kenya National Computer and Cybercrime Coordination Committee. (2022). *Cyber risks, incidents, and crimes management*. NC4 – Protecting Kenya's Cyberspace. https://nc4.go.ke/research-and-collaboration/

Kaibiru, R. M., Karume, S. M., Kibas, F., & Onga'nyo, M. L. B. (2023). Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education. *Journal of Information Security*, *14*(2), 136-151.

Kallberg, J., & Thuraisingham, B. (2012, June). Towards cyber operations-The new role of academic cyber security research and education. In *2012 IEEE International Conference on Intelligence and Security Informatics* (pp. 132-134). IEEE.

Kazi, A. M., & Khalid, W. (2012). Questionnaire designing and validation. *Journal of the Pakistan Medical Association*, *62*(5), 514.

Kritzinger, E., Bada, M., & Nurse, J. R. (2017, May). A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK. In *IFIP World Conference on Information Security Education* (pp. 110-120). Springer, Cham.

Lehto, M. (2015, July). Cyber security competencies: cyber security education and research in Finnish universities. In *ECCWS2015-Proceedings of the 14th European Conference on Cyber Warfare & Security: ECCWS* (Vol. 2015, pp. 179-88).

Ludek, L. (2016). Theoretical Sources for a Theory of Safety and Security. In *SECURWARE: The Tenth International Conference on Emerging Security Information, Systems and Technologies*.

Lukas, L. (2016). Theoretical sources for a theory of safety and security. In *The Tenth International Conference on Emerging Security Information, Systems and Technologies, SECUREWARE*.

Malcolm, J. (2008). *Multi-stakeholder governance and the Internet Governance Forum*. Terminus Press.

Maude, F. (2013). Cyber security information sharing partnership. *Retrieved from*.

Malan, J., Lale-Demoz, E., & Rampton, J. (2018). Identifying the Role of Further and Higher Education in Cyber Security Skills Development. *Skills: Concepts, Measurement and*

Policy, Approaches. A/68/552 Report of the Secretary-General on "Progress on the implementation of recommendations related to strengthening information and systems security across the Secretariat"

Robinson, M., Jones, K., & Janicke, H. (2015). Cyber warfare: Issues and challenges. *Computers & Security*, *49*, 70-94.

Reveron, D. S., & Savage, J. E. (2020). Cybersecurity convergence: digital human and national security. *Orbis*, *64*(4), 555-570.

Sony, M., & Aithal, P. S. (2020). Developing an industry 4.0 readiness model for Indian engineering industries. *International Journal of Management, Technology, and Social Sciences (IJMTS)*, *5*(2), 141-153.

Sang, M. (2022). An Appraisal of Kenya's National Cybersecurity Strategy 2022: A Comparative Perspective By: Michael Sang.

Sales, N. A. (2018). Privatizing cybersecurity. *UCLA L. Rev.*, *65*, 620.

Theohary, C. A., & Rollins, J. (2009). Cybersecurity: Current legislation, executive branch initiatives, and options for Congress.

Tariq, N. (2018). Impact of cyberattacks on financial institutions. *Journal of Internet Banking and Commerce*, *23*(2), 1-11.

Tagarev, T., & Sharkov, G. (2016). Multi-stakeholder Approach to Cybersecurity and Resilience. *Information and Security: An International Journal*, *34*(1), 59-68.

Thierer, A. (2021). Soft law in US ICT sectors: Four case studies. *Jurimetrics*, *61*(1), 79-119.

Wolter, D. (2013). The UN takes a big step forward on cybersecurity. *Arms Control Today*, *43*(7), 25.

Westerlund, M., & Rajala, R. (2014). Effective digital channel marketing for cybersecurity solutions. *Technology Innovation Management Review*, *4*(10).

Wanjiku, R. (2009). Kenya Communications Amendment Act (2009) Progressive or retrogressive. *Association for Progressive Communications (APC)*, *1*(1), 1-20.

Wells, L. (2016). Cyberspace as the 5th Domain of Warfare. *Center of excellence for national security*, 1-29.