NATIONAL DEFENCE UNIVERSITY-KENYA

NATIONAL SECURITY SYMPOSIUM

REPORT

October 2023

"Enhancing **Cyber Security** for National Development"

NATIONAL DEFENCE UNIVERSITY-KENYA

VISION

A centre of excellence in training, education and research in national security and strategy.

MISSION

To empower defence and security professionals through world-class education and training in order to enhance capacity in safeguarding national interest.

CORE VALUES

- ACADEMIC FREEDOM
- HONESTY
- DIVERSITY
- DISCIPLINE
- INTEGRITY
- RESPONSIBILITY

CHIEF GUEST

Mr. Eliud Owalo
Cabinet Secretary
Ministry of Information
Communications & Digital Economy.

Hon Aden Bare Duale, EGH
Cabinet Secretary
Ministry of Defence

General Francis Omondi Ogolla
EGH EBS HSC 'ndc' (K) 'psc' (FRA)
Chief of the Defence Forces and
NDU-K Council Chairperson

UNIVERSITY LEADERSHIP

Vice Chancellor
Maj Gen S M Farah,
CBS 'rcds' (UK) 'psc' (UG)

Deputy Vice-Chancellor, Research, Innovation and Security Studies
Maj Gen W K K Shume
CBS 'ndc' 'psc'(K) 'acsc'(UK)

Deputy Vice-Chancellor, Academic and Student Affairs
Prof Anne Muigai
(BEd, MSc and PhD)

Deputy Vice-Chancellor, Administration and Finance
Maj Gen (Rtd) P A Amogola
CBS 'ndc' 'psc' (K)

NATIONAL DEFENCE UNIVERSITY-KENYA

Established under Section 24 of the Universities Education Act, 2012 on 27 May 2021. NDU-K offers specialized certificates, diplomas and degrees in areas related to Defence and security, as well as other dimensions of security.

FOREWORD

As the National Defence University of Kenya, an institution of strategic national importance mandated to provide education and training in Defence, security, and strategy, we are proud to introduce this report. It emanates from the esteemed discussions and insights shared at our national security symposium themed "Enhancing cybersecurity for national development", where leaders, experts, scholars, and practitioners convened to address the critical challenges facing our Republic of Kenya.

In the contemporary landscape of global security, few threats rival the complexity and pervasiveness of cybersecurity. Recognizing its significance as a threat to national security, this report delves deeply into the discussions on intricate dimensions of cybersecurity and its profound implications for our nation-state. Through meticulous research and critical analysis, it not only sheds light on the challenges posed by cyber threats but also provides policy guidance on how best to confront and mitigate them.

As we continue to deepen our understanding of national defense and security, may this report serve as a beacon of knowledge, guiding our collective efforts to fortify our defenses and safeguard the sovereignty of our nation against the ever-evolving cyber threat landscape.

Major General S M FARAH CBS 'rcds' (UK) 'psc' (UG)
Vice-Chancellor

PAGE INTENTIONALLY
LEFT BLANK

EXECUTIVE SUMMARY

The National Defence University-Kenya (NDU-K) held a national cybersecurity symposium on 26 October 2023. The theme of the symposium was: "Enhancing Cybersecurity for National Security and Development."

Recognizing cyberspace's pivotal role in economic growth, the symposium was aimed at discussing contemporary cyber threats, exploring research findings, and proposing practical strategies to enhance national security and development.

In attendance were high-profile speakers, including Mr. Eliud Owalo (Cabinet Secretary for Information, Communication, and Digital Economy), Hon. Aden Bare Duale (Cabinet Secretary of the Ministry of Defence), General Francis Omondi Ogolla (Chief of The Defence Forces and Chairperson of NDU-K Council), the Kenya Defence Forces Service Commanders, Major General Mohammed Said Farah (Vice Chancellor NDU-K), policy, senior leaders and practitioners from both government and industry.

Led by expert panels, discussions delved into current and emerging cyber threats, strategies for enhancing national cybersecurity capabilities, and a robust policy and legal framework. Lessons included the interconnected nature of ICTs, security, and development, the increasing challenge of cyber threats, the importance of cyber defense capabilities, and the need for adaptive cybersecurity policies.

Key recommendations encompass developing a national cybersecurity policy, allocating funds for research and development, enhancing detection and response capabilities, fostering collaboration, creating an ICT talent pipeline, emphasizing cybersecurity training, promoting secure system implementation, addressing legal framework challenges, recognizing the human element, and integrating cybersecurity into organizational priorities.

In conclusion, the symposium highlighted cyberspace's vital role in national development, emphasizing the collaborative integration of effective cybersecurity policies and strategies.

PAGE INTENTIONALLY
LEFT BLANK

TABLE OF CONTENT

PAGE INTENTIONALLY
LEFT BLANK

INTRODUCTION

National Defence University-Kenya (NDU-K) is mandated to proffer solutions on contemporary and future security challenges. The University pursues this mandate by, among other ways, linking diverse stakeholders in government, industry and private sector to contribute to development of policies and strategies to address national, regional and global security issues with a bearing on Kenya's national interest. In this regard, the University identified cyber security as a key aspect of national security which requires special attention in order to facilitate the Government of Kenya to achieve its national development agenda through leveraging opportunities and mitigating the challenges in the cyberspace.

The cyberspace provides enormous opportunities which include global connectivity, information access, E-commerce, financial services, education and E-learning, innovation and technology advancement through online collaboration, data analytics, smart technology, health and telemedicine, environmental monitoring, communication and social networking as well as entertainment and media among others. The cyberspace, therefore, plays a vital role in increasing capital and labour productivity while at the same time enabling citizens to obtain goods and services at lower costs which in turn makes it one of the main drivers of economic growth and national development. Cognizant of these opportunities, the Government of Kenya has identified digital and creative economy as one of the focus areas of the Bottom-Up Economic Transformation Agenda (BeTA).

In spite of the overwhelming opportunities, the cyberspace faces significant challenges and risks such as cyber security threats, privacy concerns, misinformation and digital divide. Some of the cyber security threats include Distributed Denial of Services (DDoS) attacks, social engineering, cyber espionage, identity theft, ransomware, supply chain attacks among others. Some public and private institutions in Kenya have experienced one or more of the cyber security threats in varying levels. The most recent incident is the attempted attack on the Government's E-citizen platform by hackers who identified themselves as Anonymous Sudan. These threats, if not mitigated, impact on national security and development.

It is against the above background, that NDU-K organized the national cybersecurity symposium themed, "Enhancing cybersecurity for national security and development." The symposium provided a platform for key stakeholders; policy makers, practitioners, legal experts and scholars to engage on the subject matter with a view to identifying the challenges and proffer mitigation strategies.

AIM

This report highlights objectives of the symposium, the theme and sub-themes, key addresses, approach and symposium discussions as well as outcomes based on the objectives.

OBJECTIVES OF THE SYMPOSIUM

01

To Discuss **CYBER THREATS** as a contemporary challenge to national security and development.

02

To Discuss **RESEARCH FINDINGS** and developments on cybersecurity and their implication on national Security and development.

03

To Propose **PRACTICAL STRATEGIES** to mitigate cyber threats for the enhancement of national security and development.

THEME AND SUB-THEMES

The Symposium achieved its objectives through discussions premised on the theme, ***"Enhancing cybersecurity for national development,"*** with the following sub-themes:

a. Current and emerging cyber threats to national security and development;
b. Developing capabilities and strategies for enhancing national cyber security; and
c. National cyber security policy and legal framework for national security and development

METHODOLOGY

The symposium methodology comprised of key note addresses, topical speeches and discussions. The discussions under each sub-theme were led by a selected team of Six (6); chairperson, key presenter and discussants. The chairpersons of the respective panels introduced the topic for discussions as well as panel members and welcomed the key presenters on the respective sub-theme. Thereafter, they moderated inputs, questions and comments from the panel and audience participants.

PARTICIPATION

The symposium attracted a total of Five hundred and seventeen (517) participants; out of whom two hundred and twenty-three (223) attended in-person, while two hundred and ninety-four (294) attended virtually (online).

The participants that attended in-person were: Cabinet Secretary Ministry Information, Communication and Digital Economy, Mr. Eliud Owalo (Chief Guest); Cabinet Secretary Ministry of Defence Hon. Aden Bare Duale; Chief of The Defence Forces and Chairperson of the NDU-K Council, General Francis Omondi Ogolla, Kenya Defence Forces' Service Commanders, NDU-K Vice Chancellor Maj Gen S M Farah; Deputy Governor, Nakuru County; General Officers, Director Generals of State corporations and agencies; Chief Executive Officers; NDU-K Deputy Vice-chancellors, Senior officers and officers from KDF and other national security agencies; cybersecurity practitioners, experts and delegates from seventy-six (76) public and private institutions.

OPENING REMARKS

1.1 Mr. Eliud Owalo, Cabinet Secretary Ministry of Information, Communication and Digital Economy

The Chief Guest, Mr. Eliud Owalo, Cabinet Secretary (CS) Ministry for Information, Communication, and Digital Economy (MIC&DE); in his the key note address recognized the undeniable intertwining of Information and Communication Technologies (ICTs) and national economic development by driving economic growth, improving access to essential services and propelling Kenya towards becoming a digitally empowered nation.

CS MIC&DE pointed that the rollout of 100,000 kilometers of terrestrial fiber optic cable infrastructure brings new numerous benefits including improved connectivity especially in remote and underserved areas. Also, the government is connecting 25,000 local markets to WiFi and installing 1,450 digital hubs countrywide that will be accessed freely. These will allow more people to access high speed internet, bridging the digital divide and promoting digital inclusion. Also, the expansion of fiber optic networks facilitates the delivery of government e-citizen services online, making them more accessible and efficient for citizens. Reliable and high-speed internet is essential for businesses, innovation and will attract investments in various sectors such as technology, finance and e-commerce. Furthermore; schools, Technical and Vocational Education and Training (TVETs), Universities and research institutions will leverage online resources, collaborate with peers globally and access research findings.

The CS MIC&DE affirmed the imperative to confront and mitigate challenges posed by cybersecurity threats. Protecting the national terrestrial fiber cable and other critical information infrastructure is crucial for ensuring the security and stability of our communication networks and essential services. The government of Kenya recognizes the importance of safeguarding these assets and continues to implement various initiatives to enhance their protection. The National ICT policy, Cybersecurity Strategy and legislations, he explained, continue to guide efforts on strengthening defenses, enhancing detection and response capabilities, building resilience, and ensuring data and critical

infrastructure protection. To ensure cohesion in cybersecurity efforts, Mr. Owalo informed of the establishment of the ICT Taskforce, comprising experts from government, academia, and the private sector to review and streamline ICT policies and regulations.

As the Cabinet Secretary for IC&DE, he expressed commitment to strengthening the partnerships between ICT, Defence and other stakeholders through joint efforts in implementing the digital transformation agenda and the protection of ICT assets for national economic prosperity.

Protecting the national terrestrial fiber cable and other critical information infrastructure is crucial for ensuring the ***security and stability*** *of our communication networks and essential services. The government of Kenya recognizes the importance of safeguarding these assets and continues to implement various initiatives to enhance their protection.*

Mr. Eliud Owalo
Cabinet Secretary Ministry of Information, Communication and Digital Economy

1.2 Hon. Aden Bare Duale, Cabinet Secretary Ministry of Defence

Hon. Aden Duale, Cabinet Secretary of the Ministry of Defence (CS Defence), underscored the critical importance of cybersecurity in safeguarding the nation's security and prosperity. Emphasizing the pervasive nature of digital interconnectedness in modern society, the Cabinet Secretary highlighted the dual nature of technological advancements, which bring both unprecedented opportunities and new threats.

Cyberattacks, ranging from disruptive actions by malicious actors to sophisticated cybercriminal activities targeting critical infrastructure and financial systems, pose significant risks to national defense, economic stability, and citizen privacy. Recognizing the evolving and diverse nature of cyber threats, the Ministry of Defence has embarked on a proactive strategy to strengthen Kenya's cybersecurity posture.

Key initiatives include substantial investments in cutting-edge technology, the enhancement of cybersecurity infrastructure, and the promotion of collaboration among government agencies, private sector entities, and international partners. The Ministry's approach to cybersecurity encompasses risk management, incident response, and information sharing, supported by comprehensive training and capacity-building programs for cybersecurity professionals. Moreover, the government is committed to reinforcing legal and regulatory frameworks to combat cybercrime effectively and uphold the rule of law in cyberspace while protecting citizens' rights and freedoms. Beyond technical measures, the Ministry recognizes the importance of fostering a culture of cybersecurity awareness across all sectors of society, promoting cyber hygiene practices, and encouraging vigilance against cyber threats. The Ministry of Defence, avails its ready forces and capabilities to the government, Ministries, departments and agencies in support of a resilient digital transformation, continuous evaluation of the cybersecurity landscape, reviews and updates to security policies and laws, and in training, research and awareness.

The Cabinet Secretary reiterated the government's unwavering commitment to securing Kenya's digital future, emphasizing that cybersecurity is not solely a technical challenge but a strategic imperative requiring collective action and steadfast resolve. Through collaborative efforts, Kenya aims to defend against cyber threats, uphold sovereignty in cyberspace, and ensure a safer and more prosperous future for all citizens.

1.3 General Francis Omondi Ogolla, Chief of the Defence Forces and Chairperson of NDU-K Council

General Francis Ogolla, Chief of the Defence Forces (CDF) and Chairperson of NDU-K Council, in his remarks, underscored the myriad opportunities presented by cyberspace, including its role in enhancing defense capabilities and driving economic growth. By leveraging digital technologies, the military can improve situational awareness, streamline operations, and respond to emerging threats with agility and precision. Additionally, cyberspace serves as a catalyst for innovation, collaboration, and information sharing, thereby bolstering national security and fostering economic prosperity.

Despite the opportunities afforded by cyberspace, the CDF acknowledged the formidable challenges posed by cyber threats. These threats, ranging from cyber espionage to terrorism, undermine national security, socio-economic stability, and public trust. Moreover, the rapid pace of technological advancement exacerbates vulnerabilities, necessitating proactive measures to mitigate risks and safeguard critical infrastructure.

In response to these challenges, he outlined Kenya Defence Forces' proactive initiatives to ensure a safe and resilient cyberspace. This includes investments in state-of-the-art cybersecurity infrastructure, technology, and human capital development. In addition to the establishment of the Cyber Command Center as a central hub for monitoring, detecting, and responding to cyber threats in real-time, establishing NDU-K a strategic institution for building capacity on contemporary national security issues, and support of national cybersecurity efforts through the National Computer and Cybersecurity Coordination Committee (NC4). Moreover, KDF is actively engaged in collaborative partnerships with government agencies, industry stakeholders, and academic institutions to foster information sharing, capacity building, and joint exercises aimed at strengthening cyber defenses.

Gen Ogolla underscored that enhancing cybersecurity extends beyond defense; it is about developing and leveraging national cyber capabilities. He emphasized the need for the military to extend its expertise into the digital domain, cultivating cyber warriors capable of detecting, deterring, and responding to threats effectively. He emphasized the necessity of fostering public-private partnerships, information sharing, and international cooperation to pool resources, intelligence, and capabilities.

1.4 Major General S M Farah, Vice-Chancellor NDU-K

Major General S M Farah, Vice-Chancellor NDU-K, in his opening speech outlined NDU-K's role as a strategic institution in education, training, and research. He emphasized the institution's comprehensive curriculum, which provides students with the knowledge and skills necessary to navigate the complexities of today's security environment.

The Vice-chancellor highlighted the dual nature of cyberspace, offering both opportunities for innovation and connectivity, as well as threats to national sovereignty and stability. He emphasized the need for proactive measures to mitigate cyber threats, including cyber espionage, sabotage, and ransomware attacks, which pose significant risks to the nation's security and prosperity.

Furthermore, Maj Gen Farah emphasized NDU-K's commitment to collaborative capacity-building initiatives aimed at enhancing cybersecurity awareness and resilience across the broader community. Through training, research, outreach programs, workshops, and seminars, the institution empowers organizations and individuals to recognize and mitigate cyber risks, thereby strengthening the overall cyber defense posture of the nation.

In conclusion, the Vice-chancellor reiterated the strategic imperative of cybersecurity and positioned NDU-K as a strategic institution for higher learning, committed to cooperating and collaborating in research, practical skills, and innovation for economic development.

> *Through training, research, outreach programs, workshops, and seminars, the institution empowers organizations and individuals to recognize and mitigate cyber risks, thereby strengthening the overall* ***cyber defense*** *posture of the nation.*
>
> ***Maj Gen S M Farah***
> *Vice-Chancellor NDU-K*

SYMPOSIUM DISCUSSIONS

The National symposium unfolded as a crucial forum, delving into the intricacies of Kenya's cybersecurity landscape with a focus on the first objective of the symposium which was to discuss cyber threats as a contemporary challenge to national security and development. To achieve this, the symposium discussions revolved around three interlinked sub-themes, each unraveling pivotal challenges and presenting strategic policies to fortify national cybersecurity, aligning it with the imperatives of sustainable development as follows:

Leadership following the proceedings

PANEL DISCUSSANTS

SPEAKER:
Dr Vincent Ngundi
-Ag. Director Cyber Security, CAK

Sub Theme I:
Current and emerging cyber threats to national security & development.

PANEL DISCUSSIONS

CHAIR	**Prof Fred Jonyo**	**UoN**
PANELLISTS	Lt Col Wilson Kigotho	KDF
	Fredrick Musili	CBK
	Mr Ben Roberts	Liquid
	Mr Nicholas Mulira	Safaricom PLC
	Mr Fidel Muia	KBA

PANEL DISCUSSIONS

CHAIR	**Prof Agnes Wausi**	**UoN**
PANELLISTS	William Makatiani	Serianu
	Mr Adam Lane	Huawei
	Ms Shain Rahim	CISCO
	Mr John Wali	Junior Achievement Kenya
	Dr Joe Sevilla	Strathmore

SPEAKER:
Prof. Moeli Kashorda,
CEO KeNET

Sub Theme II:
Developing capabilities and strategies for enhancing national cyber security

SPEAKER:
Dr .Humphrey Njogu
Principal Policy Analyst, KIPPRA

Sub Theme III:
National cybersecurity policy & legal framework for national security and development.

PANEL DISCUSSIONS

CHAIR	**Brig Yvonne Kerubo**	**KDF**
PANELLISTS	Col Dr James Kimuyu	NC4
	Jennifer Nganga	State Law Office
	Mr Timothy Were	MIC&DE
	Mr John Sergon	Consultant
	Mr Keniz Agira	KCSFA

1.1 Current and emerging cyber threats to national security and development

The discussions on the sub-theme, "Current and emerging cyber threats to national security and development," provided a comprehensive overview of the alarming growth of cyber threats, driven by motivations such as geopolitics, money, ideology, compromise, and ego, posing significant challenges to Kenya's security and development.

The following are the discussions highlights:

- The sub-theme discussions underlined that Kenya's cyberspace environment presents several factors that allow cyber threats to pose significant challenges. Some of the factors include:

    (1) Kenya's rapid adoption of digital technologies across various sectors including finance, healthcare, and government, outpace the implementation of adequate cybersecurity measures, creating opportunities for cyber-attacks.

    (2) Kenya's cybersecurity infrastructure is relatively underdeveloped compared to more advanced economies, resulting in gaps in network security, incident response capabilities, and regulatory frameworks.

    (3) Many individuals and organizations in Kenya lack awareness about cybersecurity best practices, making them more susceptible to cyber-attacks such as phishing, malware, and social engineering.

    (4) Kenya's strategic location and geopolitical significance may attract the attention of state-sponsored groups seeking to gather intelligence or disrupt operations for political or economic reasons.

    (5) Kenya's reliance on external technologies and software, which may not always be properly secured or regularly updated, can create vulnerabilities that actors can exploit.

- Some of the current and emerging cybersecurity threats and challenges to the security and development of a nation state discussed include:

    (1) Panel experts underscored the significant challenge posed by Advanced Persistent Threats (APTs). APTs are sophisticated and targeted cyber-attacks, often sponsored by nation-states or well-funded criminal organizations. They aim to infiltrate networks, steal sensitive data, disrupt critical infrastructure, and undermine national security. APTs target various sectors, including government agencies, financial institutions, and critical infrastructure, compromising data integrity, confidentiality, and availability, thereby posing serious risks to national security, economic stability, and public trust.

(2) Ransomware attacks encrypt a victim's data and demand payment for decryption, causing widespread disruption to businesses, government agencies, and critical infrastructure. These attacks have become increasingly prevalent and sophisticated, posing significant financial and operational risks. Research on ransomware attacks, such as the Colonial Pipeline incident in the United States, underscores the importance of strengthening cybersecurity defenses and resilience measures for critical infrastructure in Kenya. Instances like the ransomware attack on Kenya's health sector in 2019 highlight the vulnerability of essential services to cyber threats. Research-informed strategies for investing in threat intelligence, incident response capabilities, and cybersecurity training are crucial for mitigating the impact of ransomware attacks and ensuring continuity of operations for critical infrastructure in Kenya.

(3) The discussions touched upon the vulnerabilities introduced by interconnected global supply chains, with adversaries exploiting weaknesses to compromise critical infrastructure. Attackers target the software supply chain to infiltrate trusted vendors and distribute malicious software to unsuspecting customers. Supply chain attacks can compromise the integrity of software, hardware, and firmware, leading to widespread compromise and data breaches. The SolarWinds supply chain attack demonstrates the significance of supply chain security for safeguarding national state security and defense systems. While Kenya may not have experienced a similar high-profile incident, the reliance on international vendors for critical infrastructure components underscores the need for vigilance. Research on supply chain risk management and security assurance mechanisms informs Kenya's efforts to enhance visibility, transparency, and accountability across its supply chains, including vendor vetting, code reviews, and software bill of materials (SBOM) requirements.

(4) The proliferation of Internet of Things (IoT) devices, such as smart home appliances, industrial sensors, and medical devices, introduces new attack vectors and security vulnerabilities. Insecure IoT devices can be exploited to launch large-scale distributed denial-of-service (DDoS) attacks, harvest sensitive data, or disrupt critical services.

(5) The adoption of cloud computing introduces unique security challenges, including data breaches, misconfigurations, insider threats, and unauthorized access. In recent years, Kenyan organizations have increasingly adopted cloud computing services for data storage, collaboration, and application hosting. Securing cloud environments requires robust security controls, encryption, access management, and continuous monitoring.

(6) Nation-states and cybercriminal groups conduct cyber espionage operations to steal sensitive information, intellectual property, trade secrets, and government secrets. Cyber espionage threatens national security, economic competitiveness, and innovation. Instances of cyber espionage and intellectual property theft pose significant threats to Kenya's national security, economic competitiveness, and innovation. While the symposium may not have pointed high-profile cases in Kenya,

the risk is present due to the country's growing digital economy and strategic geopolitical position. Research on cyber threat attribution, forensic analysis, and incident response informs Kenya's efforts to identify and deter malicious actors, protect sensitive information, and strengthen cybersecurity capabilities to defend against cyber espionage and intellectual property theft.

(7) While the adoption of emerging technologies such as AI, quantum computing, and blockchain is still evolving in Kenya, the potential security implications are increasingly recognized. As these technologies mature and become more widely deployed, it's essential to anticipate and address potential security risks and vulnerabilities proactively. Research on emerging technologies, such as artificial intelligence and autonomous systems, has implications for Kenya's national defense capabilities as well as strategic deterrence. While Kenya is still developing its military capabilities in these areas, investment in R&D initiatives and technology partnerships can help leverage emerging technologies for military applications, while addressing ethical, legal, and policy considerations related to their use in national defense and security operations. Participants emphasized the importance of collaborative efforts involving telecommunications companies, government bodies, and cybersecurity experts to address security concerns of new technologies.

- Experts and participants alike stressed the importance of investing in cybersecurity education and training. Kenyan individuals and organizations have been targeted by phishing attacks aimed at stealing credentials, financial information, and sensitive data. In 2020, the Communications Authority of Kenya warned the public about an increase in phishing scams related to COVID-19, urging vigilance and cybersecurity awareness. Suggestions included promoting a cybersecurity-awareness culture, especially among government personnel, and incorporating programs into school curricula to instill a culture of cyber hygiene from an early age.

- The discussions on this sub-theme concluded with a consensus on the complexity of new and emerging cyber threats to Kenya's security and development. There was emphasis on the crucial need for implementing robust cybersecurity controls and comprehensive cybersecurity legislation to empower authorities with a legal framework to combat cyber threats effectively. Audience members highlighted the importance of public awareness campaigns to inform citizens about the significance and implications of cybersecurity.

1.2 Developing capabilities and strategies for enhancing national cyber security

Discussions on the second sub-theme on developing capabilities and strategies for enhancing national cyber security highlighted the comprehensive approach that addresses technical capabilities, policy frameworks and human resources.

The following were the highlights of the discussions:

a. Kenya should prioritize investment in cybersecurity infrastructure, including advanced security technologies such as intrusion detection systems, firewalls, endpoint protection, and security information and event management (SIEM) solutions. Building a robust cybersecurity infrastructure is essential for detecting, preventing, and mitigating cyber threats effectively.

b. Promoting cybersecurity awareness and providing training to individuals and organizations across various sectors is critical in fostering a cyber-aware culture and reducing the human factor in cyber incidents. Kenya should invest in cybersecurity education programs, workshops, and awareness campaigns to enhance the knowledge and skills of its workforce in identifying and responding to cyber threats.

c. Due to the evolving nature of technology, Kenya must develop, update and enforce comprehensive cybersecurity policies, regulations, and standards to govern cybersecurity practices across government agencies, critical infrastructure sectors, as well as private organizations. Establishing clear guidelines for cybersecurity governance, risk management, incident response, and data protection is essential in enhancing the nation's cyber resilience.

d. Establishing dedicated Cybersecurity Operation Centers (CSOCs) and Incident Response Teams (CIRTs) equipped with the necessary expertise, tools, and resources is vital for effectively responding to cyber incidents and coordinating incident response efforts across government and private sectors. CSOCs and CIRTs play a crucial role in detecting, analyzing, and mitigating cyber threats in a timely manner to minimize the impact on national security and critical infrastructure.

e. Encouraging research and innovation in cybersecurity is essential for developing cutting-edge technologies, strategies, and solutions to address evolving cyber threats. Kenya can support cybersecurity research institutions, startups, and academic programs to foster innovation, entrepreneurship, and talent development in the cybersecurity field.

f. Collaboration between government, industry, academia, and civil society is essential for enhancing cybersecurity capabilities and sharing threat intelligence. Kenya should foster public-private partnerships to facilitate information sharing, joint cybersecurity exercises, capacity-building initiatives, and collaborative research and development efforts to address emerging cyber threats effectively.

g. Given the transnational nature of cyber threats, Kenya can strengthen cooperation and collaboration with international partners, regional organizations, and law enforcement agencies to combat cybercrime, share best practices, and enhance cybersecurity capabilities. Engaging in bilateral and multilateral cybersecurity dialogues and initiatives can facilitate knowledge exchange, capacity building, and joint efforts to address cyber challenges.

1.3 Cybersecurity policy & legal framework for national security and development

Under the third sub-theme, "Cybersecurity policy & legal framework for national security and development," the symposium explored Kenya's cybersecurity policies and regulations. Kenya has good rankings in digital economy and cyber-related indices in cybersecurity policy and legal framework.

The following were the highlights of the discussions:

a. Kenya has made significant strides in developing cybersecurity policies and legal frameworks to address the growing threat landscape. However, there are still gaps and challenges that need to be addressed to enhance the effectiveness of these frameworks.

b. Kenya developed its first National Cybersecurity Strategy in 2014. The second National Cybersecurity Strategy 2022-2027 provides a comprehensive framework for addressing cyber threats and protecting critical infrastructure. The strategy outlines key objectives, priorities, and actions for enhancing cybersecurity capabilities across government, private sector, and civil society. Despite the existence of the National Cybersecurity Strategy, implementation and enforcement have been inconsistent, and some key initiatives have faced challenges due to funding constraints, resource limitations, and coordination issues. Additionally, a notable void observed was the absence of a national cybersecurity policy.

c. Kenya recognizes the importance of protecting critical infrastructure sectors, such as energy, transportation, telecommunications, finance, and healthcare, from cyber threats. Efforts have been made to develop legislations and sector-specific cybersecurity guidelines, standards, and incident response frameworks to enhance resilience and continuity of essential services. For instance, Kenya enacted the Computer Misuse and Cybercrimes Act in 2018 to address various forms of cybercrime, including unauthorized access, hacking, cyber espionage, identity theft, online fraud, as well as child exploitation. The law provides legal mechanisms for investigating, prosecuting, and punishing cyber offenders. Additionally, Kenya enacted the Data Protection Act in 2019 to regulate the processing of personal data and protect the privacy rights of individuals. Despite progress in critical infrastructure protection, the symposium noted, there are gaps in coordination, information sharing, and resource allocation among different sectors and stakeholders. Limited investment in cybersecurity infrastructure and workforce development also poses challenges to maintaining robust cyber defenses for critical infrastructure.

d. The discussions concluded that strengthening implementation, enforcement, capacity building, coordination, and international cooperation are key priorities for advancing Kenya's cybersecurity resilience and protecting its national security and development interests. Drawing on global best practices and lessons learned from other countries can provide valuable insights and guidance towards shaping Kenya's cybersecurity policy and legislative framework.

Plenary in session

Panelists in one of the panel discussions

LESSONS LEARNED

The following are the lessons learned during the national cybersecurity symposium:

a. The fusion of ICTs, security, social and economic development remains a key consideration for nation states globally.

b. Nation-states must contend with cyber threats, which target sensitive information, disrupt essential services and compromise national security.

c. Investing in cyber defence capabilities is crucial in safeguarding a nation's security and fostering sustainable development.

d. Developing effective and adaptive cybersecurity policies are essential in addressing national security challenges particularly Cybersecurity.

e. A well trained and aware workforce is key for effective defence against cyber threats.

f. Public-private partnerships/collaborations can enhance information sharing, technological innovation, and the collective ability to respond to and mitigate cyber threats.

RECOMMENDATIONS

The following are the symposium recommendations:

a. A national cybersecurity risk assessment be conducted to identify status of threats and vulnerabilities Kenya's Critical Information Infrastructure in Kenya.

b. Development of Kenya cybersecurity policy for defending Kenya's cyberspace against cyber threats and protecting Critical Infrastructure.

c. Development of policies for new technologies: Artificial Intelligence (AI), blockchain and distributed Ledger technology (DLT), Internet of Things (IoT), 5G and next generations networks, Biometric technologies such as facial recognition and iris scanning, Autonomous systems, quantum computing and cybersecurity technologies; to address the opportunities, challenges and ethical considerations associated with adoption and deployment in Kenya.

d. Install technical security controls (Firewalls), cyber threat detection/prevention systems at CII systems' gateways, and invest in secure communications infrastructure (protocols and encryption technologies) to protect sensitive government communications.

e. Set-up centralized cybersecurity operation centers at the Ministry of Defence (Under Kenya Defence Forces), Interior (National Intelligence Service), and MIC&DE to serve as hubs for monitoring and dedicated cybersecurity incident response.

f. Cybersecurity research, training and awareness:

(1) Implementation of Advanced cyber threat detection systems for detecting and analyzing cyber threats in real-time.

(2) Setting-up of centralized cybersecurity operation centers to serve as hubs for monitoring and dedicated cybersecurity incident response teams responsible for responding to and mitigating cyber incidents.

(3) Investing in secure communications infrastructure (protocols and encryption technologies) to protect sensitive government communications from interception or disruption.

g. Establishment of Public-Private Partnership framework aimed at mitigating cyber threats, increasing capacity and capability besides fostering collaboration between the government and private sector stakeholders.

CONCLUSION

The Symposium emphasized the critical role of cyberspace in national socio-economic development, underscoring the need to integrate cybersecurity in all aspects of digitalization. Furthermore, having a national cybersecurity policy, a well-trained workforce, implementation of cybersecurity capabilities and public-private collaborations were highlighted as crucial elements for countering national cyber threats. The recommendations provide a strategic pathway for a safe and resilient cyberspace for fostering Kenya's development.

PROPOSED ACTION MATRIX

SER	ITEM	ACTION BY	LEAD	TIMELINE(S)	REMARK(S)
(a)	(b)	(c)	(d)	(e)	(f)
1.	National Cybersecurity Risk Assessment	Office of the President, MoD, MINA, MIC&DE, NC4, NDU-K	NC4	Immediate	Multi-agency technical team
2.	National cybersecurity policy	Office of the President, MoD, MINA, MIC&DE, NC4, NDU-K	NC4	Immediate	A multi-agency taskforce
3.	Development of policies for new technologies: Artificial Intelligence (AI), blockchain and distributed Ledger technology (DLT), Internet of Things (IoT), 5G and next generations networks, Biometric technologies (facial recognition and iris scanning), Autonomous systems, quantum computing and cybersecurity technologies	MoD, MINA, MIC&DE, Treasury, Academia, NC4, NDU-K	NC4	Immediate	Multi-stakeholder taskforce

SER	ITEM	ACTION BY	LEAD	TIMELINE(S)	REMARK(S)
(a)	(b)	(c)	(d)	(e)	(f)
4.	Cyber Defence capabilities (Security firewalls and cyber threat detection systems, Cybersecurity operation centers, Secure communications infrastructure	MoD, MINA, MIC&DE, Private Sector	All Sectors	Immediate	- MOD - MINA - MIC&DE
5.	Cybersecurity Training, Research & Awareness programs	Office of the President, MoD, MINA, MIC&DE, MEd,Treasury, NDU-K	ALL NDU-K	Immediate/ Next phase	- MIC&DE - NDU-K
6.	Cybersecurity Public-Private Partnership Framework	Office of the President, MoD, MINA, MIC&DE, MEd,Treasury, NC4, NDU-K	MIC&DE	Next Budget	- Multi-stakeholder

LIST OF ORGANIZATIONS

S/No.	Sector	Organization
(a)	(b)	(c)
1.	Ministries, Counties, Departments and Agencies (MCDAs)	1. Ministry of Defence (MoD) 2. Ministry of Information, Communications and the Digital Economy (MIC&DE) 3. Ministry of Interior & National Administration (MoINA) 4. State Law Office 5. Communications Authority of Kenya (CA) 6. State Department for Immigration & Citizen Services 7. National Computer and Cybercrimes Coordination Committee (NC4) 8. Office of the Data Protection Commission (ODPC) 9. Konza Technopolis 10. Kenya Institute for Public Policy Research and Analysis (KIPPRA) 11. Kenya Network Information Center (KeNIC) 12. Kenya School of Revenue Administration (KESRA) 13. Kenya Power and Lighting Company (KPLC) 14. Telkom Kenya Ltd 15. Anti-Counterfeit Authority (ACA) 16. Judiciary 17. Kenya Civil Aviation Authority (KCAA) 18. Geothermal Development Authority 19. Kenya Electricity Generating Company (Kengen) 20. Kenya Revenue Authority (KRA) 21. Kenya Airports Authority (KAA) 22. Nakuru County Government 23. Kenya Space Agency (KSA) 24. Office of Directorate of Public Procurement (ODPP) 25. National Commission for Science, Technology and Innovation (NACOSTI)

2.	Defence and Security Sector	26. Kenya Defence Forces (Kenya Army, Kenya Airforce & Kenya Navy) 27. National Intelligence Service (NIS) 28. National Intelligence and Research University College (NIRUC) 29. National Police Service (NPS) 30. Directorate of Criminal Investigation (DCI) 31. Kenya Prison Service (KPS) 32. Defence Forces Canteen Organization (DEFCO) 33. Defence Forces Medical Insurance Scheme (DEFMIS) 34. Defence Sacco Society Ltd (Desacco) 35. National Security Advisor (NSA) 36. National Security Telecommunications Service (NSTS) 37. International Peace Support Training Centre (IPSTC) 38. National Defence College (NDC) 39. Defence Forces Technical College 40. Kenya Military Academy (KMA) 41. Defence College of Health Sciences (DCHS) 42. Joint Command and Staff College (JCSC) 43. Defence National Security Industries (DNSI) 44. Kenya Shipyard Ltd (KSL) 45. Kenya Ordinance Factories Corporation (KOFC)
3.	Banking and Finance Sector	46. Central Bank of Kenya (CBK) 47. Kenya Bankers Association (KBA) 48. Kenya Commercial Bank (KCB) 49. Kingdom Bank 50. Cooperative Bank of Kenya 51. SBM Bank (Kenya) Limited
4.	Academia	52. The National Defence University-Kenya (NDU-K) 53. Jomo Kenyatta University of Agriculture and Technology (JKUAT) 54. Daystar University 55. Kabarak University 56. Strathmore University 57. Egerton University 58. Dedan Kimathi University of Science & Technology 59. Moi University

5.	Private Sector	60. Huawei Ltd 61. Safaricom PLC 62. Airtel Ltd 63. Sancom Ltd 64. Mastercard PLC 65. Serianu Ltd 66. Atlantis Technologies Ltd 67. Liquid Intelligence Technologies 68. Kenya BioVax Institute 69. Microsoft 70. Cisco Systems Inc. 71. GIZA Systems 72. Global Centre for Policy and Strategy (GLOCEPS) 73. Global Centre for Policy and Strategy (ISACA) 74. Kenya Cybersecurity & Forensics Association (KCSFA) 75. Africa Centre for Data Innovation

The Chief Guest, Cabinet Secretary Ministry of Information, Communication and Digital Economy Mr. Eliud Owalo, Cabinet Secretary Ministry of Defence Hon. Aden Bare Duale in a photo with NDU-K Council and speakers.

COLLEGES OF NATIONAL DEFENCE UNIVERSITY-KENYA

NATIONAL DEFENCE UNIVERSITY-KENYA
P.O. Box 3182 - 20100,
Nakuru-Kenya

info@ndu.ac.ke www.ndu.ac.ke @DefenceUniversity @NDUKenya