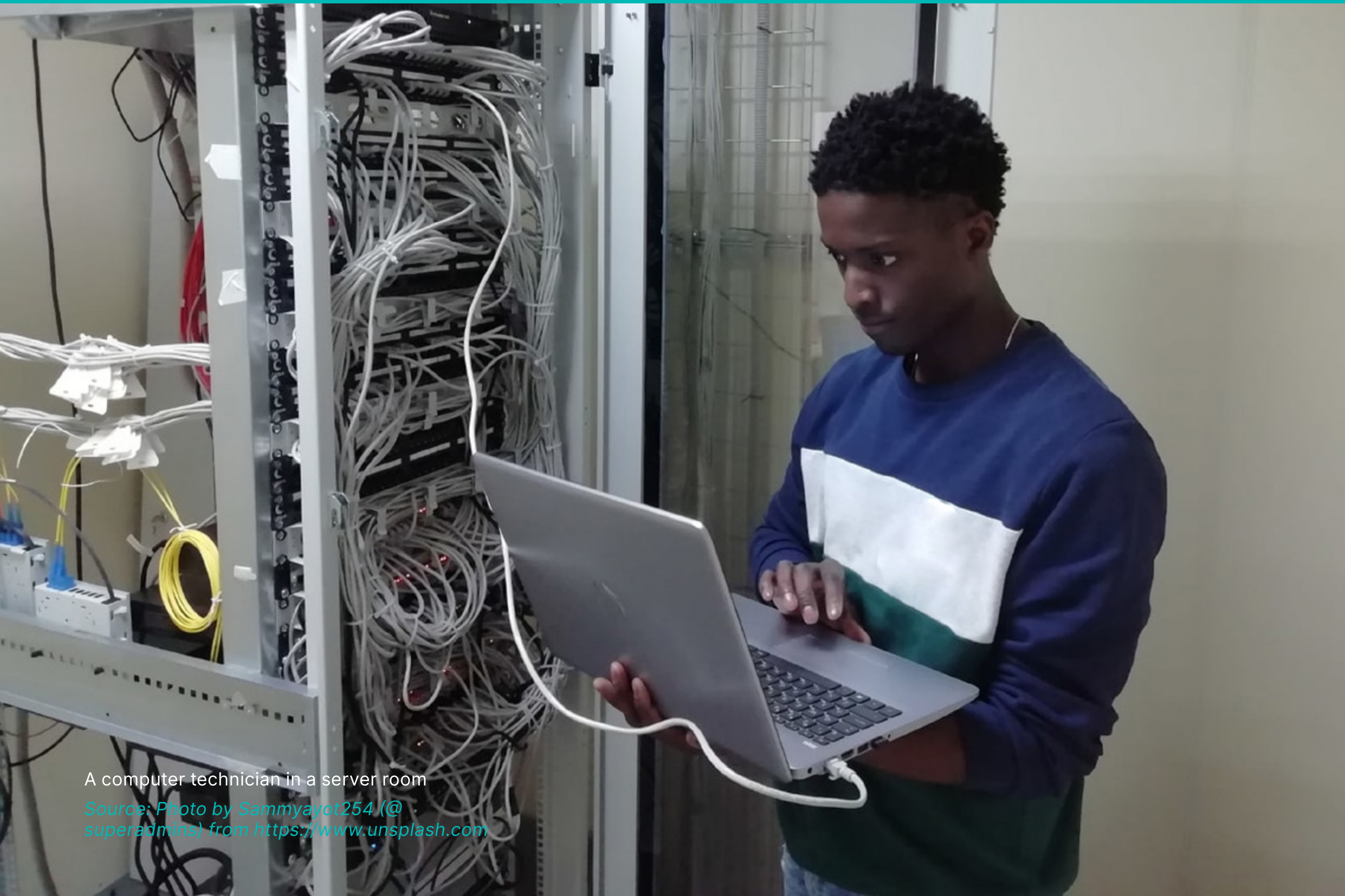
EXAMINING UGANDA’S FOREIGN POLICY

# The Influence of Cyber Norms in Fostering Uganda’s Bilateral and Multilateral Relations for Responsible State Behavior in Cyberspace

**Owiny Moses**



A computer technician in a server room

*Source: Photo by Sammyayot254 (@ superadmins) from https://www.unsplash.com*

# Table of Contents

## List of Acronyms

**AU:** African Union

**AISG:** African Internet Security guidelines

**GCSC:** Global Commission on the Stability of the Cyberspace's

**4IR:** Fourth Industrial Revolution

**ICT:** Information Communication Technology

**IGF:** Internet Governance Forum

**MOICT&NG:** Ministry of Information Communication Technology and National Guidance

**NITA-U:** National Information Technology Authority-Uganda

**NGGE:** Nations Group of Governmental Experts

**UCC:** Uganda Communications Commission

# 1.0 Introduction

The development of normative frameworks to reign over state and non-state activities in cyberspace has become a very critical issue at the moment. Currently, the global cyberspace operates without basic consensus on norms, principles and rules both by state and non-state actors[1] yet cyberspace should constitute a process in which both state and non-state actors, including the private sector, work towards achieving common norms, abide by rules applied in cyberspace, coordinate the core interests of one another, promoting responsible state behaviors and managing cyber threats effectively.[2]

There is no doubt that norms can contribute and be an essential mechanism for averting inter-state conflict in the cyberspace. This is because, conflicts in the cyberspace are increasing as time and advancement in technology unfolds and its effects are damaging to both politics and the economics of the parties involved. Cyber-induced conflict has caused both diplomatic and economic problems between Uganda and Rwanda in recent past.

In fact, in 2019 the allegations where MTN Uganda Telecom was involved in aiding large-scale cyber espionage on the Ugandan government via its telecommunication networks and transferring it to Rwanda led to the deportation of the top MTN management workers in Uganda by Ugandan authorities. This strained diplomatic relations between the two countries.

Incidents of state-inspired cyberattacks and cyber espionage have caused conflicts in both the online and physical spaces. Cyber threats undermine international peace and stability which is hinged on the efficacy of multilateral co-operation. Therefore, the need to institute co-operative measures such as norm development and implementation is more than necessary. This study validates the relevance of norms as an indispensable mechanism for building cyberstability.

Nevertheless, effective engagement of all stakeholder groups in the process of normative development and implementation is a prerequisite for acceptance, adherence to the norms and shaping cyberstability. Policy makers should ensure there is sustained multi-stakeholder engagement and consultations of all actors, including civil society, private sector, academia and technical communities.

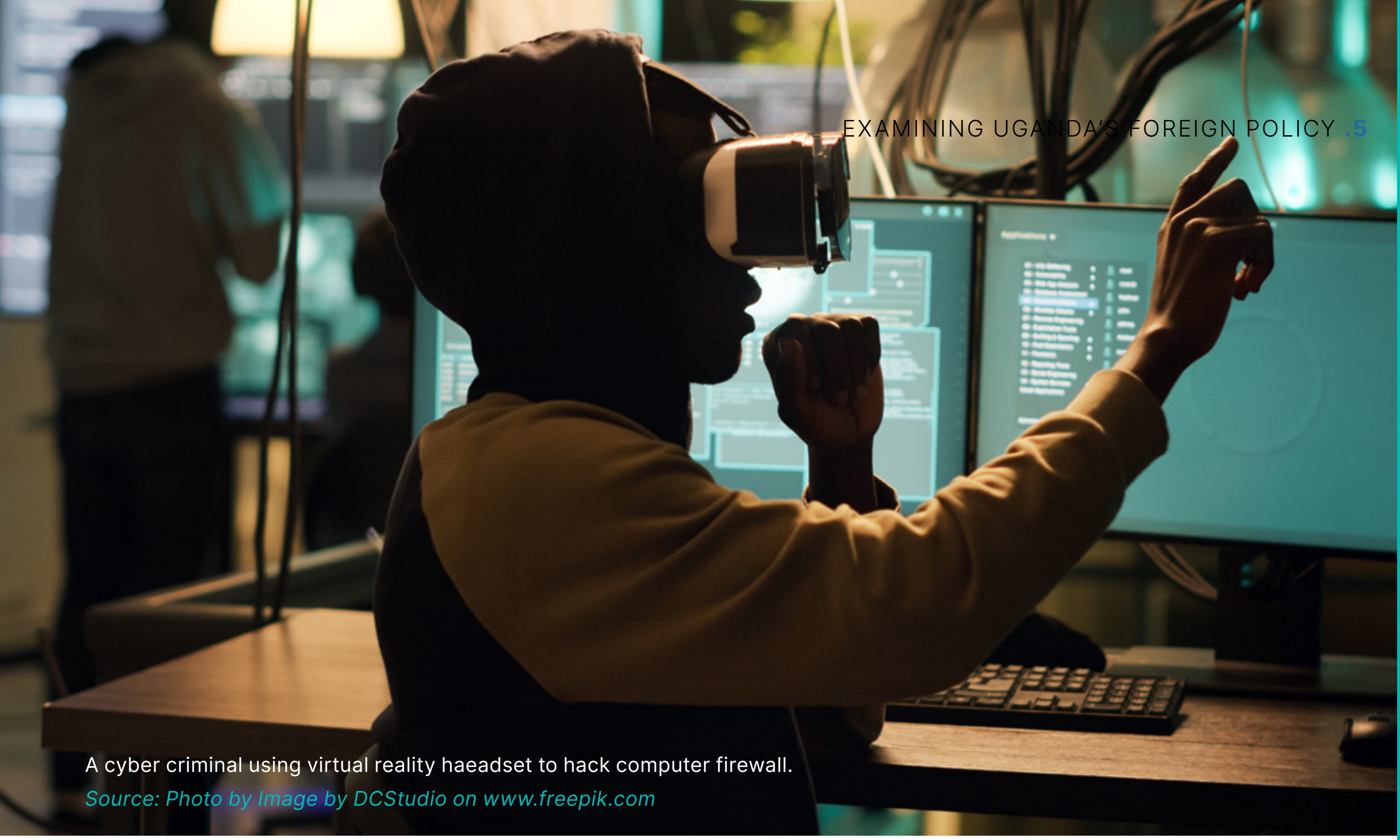
All these causes need to strengthen capacity-building of state institutions, notably those with cyber security-related mandates. But also strengthen organizational management, human resources and administrative competences of these state institutions that are critical for catalyzing the professionalization of the state bureaucracy. Moreover, respect for human rights both offline and online by government should be prioritized and then, sensitization and awareness should continue to top government priorities in the digital age.

Uganda, like many other African countries, still grapples with cybersecurity challenges that has persisted even though the country has invested immensely in enacting cybersecurity laws, strategies and frameworks. Cybercrimes continue to intensify internally, ranging from incidents such as fraudulent SIM card registrations, swapping, online impersonation, unauthorized access, remote access vulnerabilities, malware, data manipulation and social engineering. In 2019, Cybercrime led to loss of UGX 11.4 billion, which is approximately $3.09 million dollars.

The recent hacking of the Parliament of Uganda

[1] GCSC (2018) Briefings from the research advisory group. Briefings to the global commission on the stability of cyberspace for the full commission meeting, Bratislava 2018. GCSC Issue Brief No.2 GCSC GSCS (2018) GCSC Issue Brief No.2 (2018). Available at https://cyberstability.org/wp-content/uploads/2018/06/GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf

[2] Ibid.



A cyber criminal using virtual reality haeadset to hack computer firewall.

*Source: Photo by Image by DCStudio on www.freepik.com*

website and that of the Civil Service College in Uganda affiliated to the Ministry of Public Service illustrates core examples of threats that the country is dealing with. Until recently when cooperation between Uganda and Rwanda was restored, bi-lateral relations and diplomatic efforts to resolve the conflict had proven difficult and futile. Diplomatic maneuvers and restoration of bi-lateral cooperation only succeeded when the President's son and then Commander Land Forces of the Uganda People's Defense Forces (UPDF), Gen. Muhoozi Keinerugaba intervened directly with the Rwandan President, Paul Kagame.

It's important to note that bilateral and multilateral efforts in the implementation of norms as a framework for resolving conflict in the cyberspace in Uganda is barely available. Equally to say, confidence-building measures and other cooperative approaches that could potentially lead to norm development is also unavailable. Norm acceptance and implementation don't exist at bilateral level most especially between Uganda and its immediate neighbors. There is no empirical evidence regarding the extent to which confidence-building measures with regard to cyberspace in Uganda have been enhanced or undertaken and how the measures at both bilateral and multilateral level have led to sustained norm development with the possibility for widespread acceptance.

Therefore, the research underlying this paper was designed to address the above knowledge gap by deliberately examining the relevance of cyber norms in fostering cyber peace and stability between Uganda and its neighbors. This study adopted the Global Commission on the Stability of the Cyberspace's (GCSC) definition of cyber norms, as social behaviors that are expected and appropriate that govern the behavior and actions of individuals, organizations and states in cyberspace.

Cyberspace is the term used to describe the electronic medium of digital networks used to store, modify and communicate information and it includes the internet but also other information systems that support businesses, infrastructure and services.

**The research assessed the following issues:**

1. Relevance of norms in strengthening Uganda's bilateral and multilateral relations
2. Uganda's stakeholder perceptions with regard to cyber normative frameworks for international peace and security
3. Institutional frameworks put in place to promote norms for responsible state behavior
4. Role and contributions of non-state actors in enhancing cyberstability.

## 2.0 Cyberspace, Peace and Stability in Uganda

It is now common that governments are also behind cyberattacks as they use technology as a weapon against adversaries even in times of peace. Because of this, the potential for interstate conflicts and the risks associated with it is very high. As pointed above, in 2019 the allegation that the South African-based telecom company MTN Uganda was involved in supporting large-scale cyber espionage on the Ugandan government via its telecommunication networks to Rwanda threatened the country's national security and strained diplomatic relations between the two countries.

A statement released by the then deputy police spokesperson, Polly Namaye confirming these allegations asserts that "security agencies were in close coordination with immigration officials investigating two foreign nationals working with a leading mobile telecom company over their engagements in acts which compromised national security".

The cyber-espionage allegedly involved eavesdropping on communications from Government of Uganda officials, providing financial intelligence on the finances of government officials and diverting such information to Rwanda – a country that accused Uganda of harboring dissident groups with the intention to overthrow the Kigali establishment. This alleged action strained diplomatic relations of the two countries which later led to the closure of Kabale-Katuna border that connects Uganda to Rwanda.

To support further use of cyberspace maliciously by state actors and mercenaries to incite cyber tension, a story reported by the *Daily Monitor* – one of Uganda's leading dailies exposes how Rwanda allegedly used Israeli-made spyware called Pegasus, wiretapped communications of the then Prime Minister, the then Foreign Affairs Minister and the then Chief of Defense Forces of Uganda. This incident alone had the potential to stir tension if not diplomatically and peacefully resolved.

Despite the above incident, it should be noted that Uganda established institutional and legal framework that earmarks ICT skills development as a key pillar for transforming the country into a knowledge-based income and globally competitive country. Recently, the National Task Force on the Fourth Industrial Revolution (4IR) developed a strategy which is geared towards seeing Uganda as a continental 4IR hub that enables a smart and connected Ugandan society. However, from the analysis it's not clear how these frameworks can contribute or are even relevant towards resolving tensions that may arise in the cyberspace at bi-lateral level. Clearly, the frameworks are insufficient to addressing matters of inter-state cooperation in the cyberspace as it was intended to spur the growth of the ICT sector domestically.

The institutions spearheading these frameworks are coordinated and supervised by the Ministry of Information Communication Technology and National Guidance (MoICT&NG) and its agencies, such as the National Information Technology Authority-Uganda (NITA-U) and the Uganda Communications Commission (UCC). These agencies, unlike the Ministry of Foreign Affairs do not have mandate to deal with complex bi-lateral matters arising in the cyberspace. But even then, the role of the Ministry of Foreign Affairs in managing tensions that escalate bi-laterally is not seen or felt at all. The Uganda Permanent Representative to the United Nations (UN) Office in New York, has some responsibilities but there is limited knowledge to the level of participation in cyber related processes bi-laterally but also at the UN such as on the Open-Ended Working Group on ICTs in the context of international security, or on the Adhoc Committee on Cybercrime to just mention but a few.

The legal and regulatory frameworks for cybersecurity primarily include the Computer Misuse Act 2011, the Electronic Transactions and Signature Act 2011, the Regulations on Interception of Communication Act 2009 and the Data Protection and Privacy Act 2019. Other relevant Acts governing Uganda's cyberspace include the E-government Framework and the National Information Security Framework, the NITA-U Act and the UCC Act, to mention just a few. But most of these regulatory frameworks were intended to resolve cybersecurity challenges domestically. Even though these agencies do have departments such as Computer Emergency Response Teams (CERTS), their level of coordination with other countries are not clearly documented. Perhaps, they are also constrained by financial, technical and human resource capacity of individuals to effectively coordinate and make their contributions meaningful and impactful.

The Regulations on Interception of Communications Act 2009 provides a basis for authorities to intercept communications on a telecommunication network through warrant but in certain cases, authorities may require persons to decrypt information which also raises the issue of safeguarding human rights in the digital space including limiting freedom of expression online. Again, these laws were intended to address the internal challenges of security and threats to network infrastructures, but they are inadequate in addressing bi-lateral matters that escalates in the cyberspace.

## 3.0 Discussions of Findings

This section presents and discusses findings from the study based on the research objectives of the study.

### 3.1 The Relevance of Norms in Strengthening Uganda's Relations

Norms and their implementation are good for enhancing Uganda's bilateral and multilateral relations. However, the challenge is always in norm implementation which undermines the effectiveness of these norms in maintaining cyber peace and stability. Even though there seems to be inadequate level of awareness of the relevance of cybersecurity normative frameworks for Uganda, the country's ability to domesticate other norms especially those negotiated at the United Nation's processes is still non-existent.

Ugandan government through its permanent mission in New York should actively engage in UN led cyber norm processes such as the Open-Ended Working Group (OEWG) on ICTs in the context of international security and devise strategies at country level to advance discussions, developments and implementation of these frameworks with other states which could help in forming a basis of understanding and the resolution of cyberspace tensions. For instance, there are already 11 non-binding voluntary norms that have already been adopted by the United Nations Group of Governmental Experts (GGE) that are relevant for Uganda and other countries to domesticate.

Uganda must be able to build alliances with other states, strengthen partnerships with multi-stakeholder groups to ensure that conflicts in the cyberspace can be resolved peacefully without escalation. Norm development and implementation could play a critical role in this regard. It's important for Uganda to carry out regular confidence building measures and institutional dialogues with broad participation of stakeholders, including the private sector, civil society and academia in the processes of setting and implementing the norms and principles of cyberspace stability.

This approach if undertaken by the government of Uganda would be consistent with the African Internet Security guidelines that emphasize the importance of the multi-stakeholder model and collaborative security approaches in protecting the internet infrastructures. Uganda and other countries must establish mechanisms in which it adheres to standards that are set at bi-lateral and multilateral levels and translate them into local context and effectively implement the norms.

Additionally, findings reveal that norms are better enforced if they are written, backed by law and their application done within a framework of strong institutions. The cyber espionage on Uganda which catalyzed the conflict between Uganda and Rwanda, leading to the closure of border could have been resolved immediately and peacefully if cyber norms and other confidence building mechanisms had been applied to solve bilateral and multilateral conflict of such nature.

On the other hand, findings reveal that the Ugandan government sees the cyberspace domain as a space that 'allows opposition to mobilize against it'. Hence the legal frameworks that the government sets are pitched at stifling the activities of the perceived enemies of the state – the opposition, activists, human rights defenders and journalists because most of these state 'institutions are viewed as mere appendages of [the] military state'.

Nevertheless, there is a clear understanding of the concept of norms and its relevance in promoting bilateral and multilateral relations in cyberspace in Uganda and this demonstrates the critical importance of normative frameworks in building consensus and maintaining international cyberstability. There is still limited knowledge and scarcity of norms at state level. This highlights the need for a concerted effort to raise awareness, to domesticate the norms and engage policymakers at national level. This would popularize voluntary non-binding norms and also increase people's levels of knowledge and awareness of the norms.

Key informants expressed uncertainty as to whether Uganda adheres to international legal instruments and laws, drawing examples from cases of the internet shutdowns during the election period.

## 3.2 Uganda's Stakeholder Perceptions in Regard to Norms in Cyberspace

It's very important for government to fully understand their own cyberspace domain and the necessary mechanisms required to effectively secure them. Norms and norm implementation is one way of contributing towards prevention of conflicts arising from misunderstandings in the cyberspace. Government Ministries, Departments and Agencies such as the National Information Technology Authority Uganda (NITA-U) coordinates the proper functioning of the cyberspace and internet infrastructures across government bureaucracy together with other nation states. However, there is a general perception that the cyber infrastructure and capacity of government is generally weak and inefficient.

This reason could be attributed to increased cybercrimes in the country notwithstanding the legal and technical infrastructural investments that have been accorded to the ICT sector and agencies in the country. Uganda's cybersecurity infrastructures are generally perceived to be very weak because adapting to efficient technological innovation and practices including capacity to manage them is limited.

This view is backed by evidence of increased hacking of government websites and platforms as well as the reported trailing of the communications of Uganda's high-ranking officials by a neighboring state as clear signs of weakness. The Uganda's institutional and legal frameworks is believed to operate within the context of military temperature to imply that its sole intention is to serve the interest and security of the regime.

Regarding whether Uganda adheres or is capable of adhering to international law as it applies in the digital space, its believed that the country's adherence is contingent on appeasement of international actors and that there is no commitment to practically respect and adhere to international law both offline and online.

The incidents where authorities have blocked access to the internet, especially during the 2016 and 2021 general elections, the introduction of OTT taxes and the government levy of 12% taxes on the internet were deemed as a tactic by the state to violate human rights in the digital space and to limit people's access to the internet service as well as freedom of speech and expression online which is an infringement of international law. It should be noted that Uganda is a signatory to international law, and must respect, preserve and promote international human rights in accordance to their obligations.

For instance, states are barred from shutting down the internet and in this regard, internet shutdown in Uganda is a manifestation of the deliberate violation of the principle of restraint as advanced by the cyber stability framework. Blocking internet access and social media shows that the authorities are failing to uphold their international human rights obligations, including those relating to the right to free expression, which is provided for under Article 19 of the International Covenant on Civil and Political Rights (ICCPR) and Article 9 of the African Charter on Human and Peoples Rights, where Uganda is a signatory.

Lack of respect for human rights in the digital space in Uganda is a major challenge that its government must address. Uganda follows examples of other African countries that have invested in surveillance technologies to spy on citizens, human rights activists, journalists and opposition politicians. This is a deliberate violation of rights to privacy in the digital space especially where it's used without due repute to law and human rights safeguards.

Robust cyber infrastructure and systems are vital for securing the country's cyberspace and data protection and for ensuring privacy online. The associated regulatory frameworks are also key to promoting rights and freedoms. However, the weak cyber infrastructure, as well as the fact that state institutions operate on the notions of an increasingly militarized regime to exploit the regulatory frameworks, have placed serious strains on internet rights and freedoms in Uganda.

In regard to capacity building, a recent finding from the ICT Skills and Training Needs Analysis 2021 conducted by Ministry of ICT and National Guidance, notes that cybersecurity capacity-building is still lacking in government Ministries, Departments and Agencies. Government needs to prioritize the cyberspace and effectively build capacity at all levels.

There is a view that Uganda just like other African economies in general take cybersecurity as a luxury and not a necessity because its importance is not yet satisfactorily appreciated. However, this should not be the case and the Ugandan government must invest in this critical resource and domain if it's to remain vibrant and resilient to the ever-changing face of technological innovation.

## 3.3 Institutional Frameworks in Uganda for Promotion of Norms

There are several institutions and legal frameworks established in Uganda to deal with cybersecurity. These include: Ministry of ICT and National Guidance (MoICT&NG), the Uganda Communications Commission (UCC), National Information Technology Authority Uganda (NITA-U) and the Police Cybercrime Department. The key legal frameworks include the Computer Misuse Act 2011, the Electronic Transactions Act 2011, the Electronic Signatures Act 2012, the UCC Act, 2009 the NITA-U Act 2009 and the Data Protection and Privacy Act 2019. However, with such institutional and legal frameworks their effectiveness is limited towards protecting cyberspace domain and the security of individuals and communities.

This is evident by increased incidents of cybercrime such as hacking of government websites and other platforms which is an issue most institutions of government are currently dealing with.

The institutions of government also have a weak capacity to secure the cyber space domain. These include the inability to protect critical network infrastructures and software systems. There is lack of serious human resource capacity in government bureaucracy hence hindering its ability to detect and thwart cybercrime. The increase in cybercrime internally is attributed to 'incompetence of duty bearers', especially within the Uganda Police but also limited skills in forensic investigation and advanced knowledge of cybersecurity. The capacity of lawyers and state prosecutors and judges to investigate and prosecute and pronounce their opinion on cases of cybercrime is too low.

Government of Uganda should build capacity of police in cybercrime intelligence but also capacity building across all government agencies must be prioritized at all times. Delays in introducing pupils and students to digital literacy and paucity of courses focusing on cybersecurity at the tertiary level were cited as key shortcomings in the country's education system yet, this could potentially help to address the cybersecurity challenges that the country grapples with.

The awareness of the institutional capacity in Uganda to deal with the cybersecurity issue is a good step and speaks to how critical they are in fostering cooperation and norm development, implementation in cyberspace. However, concerns about the ineffectiveness of the institutions points to the need for wider stakeholder consultations and input on cyber-related matters.

The fact that key informants noted that the cyberspace domain is just emerging and key informants from government agencies state otherwise is a contradiction. Policymakers and state actors should prioritize widespread consultations among various stakeholder groups such as civil society, academia, the technical community and the private sector coupled with communication services to heighten awareness.

The government needs to widely sensitize the public on the relevance of the legal and regulatory frameworks such as the Computer Misuse Act 2011 and demystify and prove otherwise the fact that it is intended to crack down on dissent. Likewise, the government should re-evaluate the circumstances that have led to many Ugandans being arrested and charged under the Computer Misuse Act 2011. The case of Dr Stella Nyanzi – the former Makerere University academician – was cited. However, this trend of using the Computer Misuse Act 2011 was reported to have protracted and come to affect politicians, activists and journalists as well.

## 3.4 Role Non-State Actors Play in the Cyber Norm Debate and Stability

Non state actors such as civil society, the private sector and academia play important roles in shaping norm development and its implementation. Some of these roles include ensuring checks and balances on activities of the state, conducting research and advocacy, sensitization and awareness creation, capacity-building, integrating gender perspectives into policy and monitoring and documentation.

The role of non-state actors in regard to transparency and accountability was noted as contributing factor towards ensuring the safety, security and privacy of citizens and advocating against harmful technology and practices such as surveillance on citizens. Civil society's role is also very critical in the monitoring and evaluation of government programmes. The participation of civil society in spaces that they create by themselves is important even though civil society engagement in government-led multi-stakeholder consultation processes is very limited.

The role that non-state actors play and their engagement and effectiveness in cyber spaces is strongly regarded as critical in shaping the developments in the field of ICT and cyberspace. Non-state actors, notably civil society, participate and contribute meaningfully to platforms and spaces where they are invited or those that they create.

Civil society play pivotal roles such as ensuring checks and balances, conducting research and advocacy, sensitization and awareness creation, capacity-building, and integrating and amplifying the voices of minority groups. For instance, through integrating gender perspectives into policy and implementation. Non-state actors were also cited to play critical roles in monitoring and evaluation.

## 4.0 Key Recommendations for Policy Actions

1. There is need for more engagement of all stakeholder groups in shaping cyber norm debate, its development and implementation in Uganda collectively.
2. Government should establish effective institutions that are not corrupt, efficient, meritocratic and respect rule of law.
3. Policy making by government requires broad participation of stakeholders such as civil society, the private sector, academia and technical communities.
4. Government should build the capacity of state institutions with regard to their organizational, human resources and administrative aspects. This will catalyze the professionalization of a state bureaucracy that is strong, effective and unbiased.
5. Government and civil society groups and private sector should sensitize the population and raise awareness as this is a big challenge in the context of ICTs, cybersecurity and network infrastructure protection.
6. Government should respect human rights in the digital age just as they would in the offline world and must adhere to the principles of international law. For instance, the report of the UN Secretary General's High-Level Panel on Digital Cooperation clearly states that human rights apply fully in the digital space, too.

## 5.0 Reference List

1. IGF 2020 Reports. Internet Governance Forum (2020). Available at https://www. intgovforum.org/multilingual/ igf-2020-reports.
2. GCSCS (2019) Advancing Cyberstability. Homepage. Available at https://cyberstability. org/wpcontent/ uploads/2019/11/GCSC-Final-Report-November-2019. pdf.
3. Fact Sheet: (2015) President Xi Jinping's State Visit to the United States," Statements and Releases, the White House of President Barack Obama. Available at https:// obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xijinpings-state-visit-united-states.
4. GCSC (2017) Briefings from the research advisory group. Briefings to the global commission on the stability of cyberspace for the full commission meeting, New Delhi, 2017 GCSC Issue Brief No.1.
5. What's off-limits to cyber-attacks? The US – Russia Summit in Geneva in context. Available at https:// cyberpeaceinstitute.org/news/whats-off-limits-to-cyber-attacks-theu-s-russia-summit-in-geneva-in-context.
6. Without specifics, Putin says US-Russia reached an agreement to consult on cybersecurity. Available at https://www.politico.com/news/2021/06/16/putin-bidencybersecurity-494875.
7. GCSCS (2019) Advancing Cyberstability. Homepage. Available at https://cyberstability.org/wp-content/ uploads/2019/11/GCSC-Final-Report-November-2019. pdf.
8. CPNI (n.d.) Cyber security. Available at https://www. cpni.gov.uk/cyber.
9. The Council of Economic Advisers, White House (2018). The Cost of Malicious Cyber Activity to the US Economy, February 2018. Available at https://www. whitehouse.gov/ wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber- Activity-to-the-U.S.Economy. pdf.
10. NCSC glossary (2018) UK National Cybersecurity Centre, January 5, 2018. Available at https://www.ncsc. gov.uk/information/ ncsc-glossary.
11. Stuxnet. Available at https://en.wikipedia.org/wiki/ Stuxnet.
12. Zetter, Kim (2014) An Unprecedented Look at Stuxnet, the World's First Digital Weapon, Wired, November 3, 2014. Available at https://www.wired.com/2014/11/ countdown-tozero-day-stuxnet/.
13. Reuters (2017). Factbox: U.S. intel report on Russian cyberattacks in 2016 election, Reuters, January 6, 2017. Available at https://www. reuters.com/article/ us-usarussia-cyber-intel-factbox/factbox-u-s-intel-report-on-russian-cyber-attacks-in- 2016-election-idUSKBN14Q2HH.
14. WannaCry. Available at https://en.wikipedia.org/wiki/ WannaCry_ransomware_attack.
15. GCSC (2018) Briefings from the research advisory group. Briefings to the global commission on the stability of cyberspace for the full commission meeting, Bratislava 2018. GCSC Issue Brief No.2. Available at https://cyberstability.org/wp-content/ uploads/2018/06/ GCSC-Research-Advisory-Group-Issue-Brief-2-Bratislava.pdf.
16. Microsoft (2020). Digital Peace in Cyberspace: An invisible Pillar for the United Nations Sustainable Development Goals. Jean-Yves Art, Daniel Akinmade Emejulu Available at https://onestreamprod.blob.core. windows.net/events/unga/Digital%20Peace%20 in%20 Cyberspace%20-%20An%20Invisible%20Pillar%20 for%20the%20UN%20 SDGs%20-%20September%20 2020.pdf?sp=r&st=2020-09-24T07:06:37Z&se=2021-1001T15:06:37Z&spr=https&sv=2019-12-12&sr =b&sig=hiLJF0To1nTUHk4q3z2U91VSwNFgw tLy9b535RCS5vg%3D.
17. Centre for Multilateral Affairs (2020) Cyberspace and responsible state behavior within the context of international security. Accessed July 22 2021 https:// thecfma. org/cyberspace-and-responsible-state-behavior-within-the-context-of-internationalsecurity-what-way-forward-for-developing-countries/.
18. Softpower. Ugandan Security Deport 2 Senior MTN Staff Including Rwandan for Compromising National Security. Available at https://www.softpower.ug/ ugandasecurity-deport-2-senior-mtn-staff-including-rwandan-for-compromising-nationalsecurity/ accessed 20 July 2021.
19. Daily Monitor (2021) Rwanda tapped phones of top Uganda officials. Available at https:// www.monitor. co.ug/uganda/news/national/rwanda-tapped-phones-of-top-ugandanofficials-3480900.
20. United Nations (n.d.) Group of Governmental Experts: United Nations Office for Disarmament Affairs. Available at https://www.un.org/disarmament/group-ofgovernmental-experts/.
21. UN GGE and OEWG https://dig.watch/processes/un-gge.
22. Brown, D and Estherhusyen, A (n.d.) Unpacking the GGE's framework on responsible state behavior: Cyber norms. Accessed online file:///C:/Users/Mowiny/ Desktop/ unpacking_gge_cyber-norms.pdf.
23. G7 Principles and Actions on Cyber, https://www.mofa. go.jp/files/000160279.pdf.
24. 2015 G20 Leaders' Communiqué, http://www.g20. utoronto.ca/2015/151116-communique. html.
25. 2nd ASEAN Cyber Norms Workshop, https://ict4peace. org/activities/policy-research/ policy-re-search-cs/2nd-asean-cyber-norms-workshop-in-singapore-supported-by-ict4peace.

26. African, Union (n.d.). African Union Convention on Cybersecurity and Personal Data.
27. Protection. Retrieved from http://certmu.govmu.org/English/Documents/CMCA_.
28. Amendment/AU%20Covention%20on%20Cybersecurity.pdf.
29. Internet Society, African Union (2017) Internet Infrastructure Security Guidelines for Africa. Available at https://www.internetsociety.org/resources/doc/2017/internetinfrastructure-security-guidelines-for-africa/.
30. UNECA (2014). Policy Brief. Tackling The Challenges of Cybersecurity in Africa. Retrieved from https://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_ brief_1.pdf.
31. Laws and regulations https://www.nita.go.ug/laws.
32. Uganda's National 4IR Strategy. Available at https://ict.go.ug/wp-content/uploads/2020/10/Executive-Summary-Ugandas-National-4IR-Strategy.pdf.
33. Barefoot Law (2019) Cyber Laws of Uganda: How Laws and Regulations affect online activities in Uganda, 2019. Available at https://barefootlaw.org/wp-content/uploads/2018/04/BarefootLaw-Cyber-Laws-of-Uganda-201937923844.pdf.
34. Serianu (2019) Africa Cybersecurity report, Uganda 2019/2020 Available at https://www.serianu.com/downloads/UgandaCyberSecurityReport2020.pdf.
35. Observer Newspaper. Plan attacks on Government Websites. h Available at ttps:// observer.ug/news/headlines/69140-hackers-plan-attacks-on-government-websites. Accessed 18 July 2021Hackers.
36. Nir Kshetri (2019) Cybercrime and Cybersecurity in Africa, Journal of Global Information Technology Management, 22:2, 77-81, DOI: 10.1080/1097198X.2019.1603527
37. Amnesty International (2020) Uganda: Authorities must lift social media block amid crackdown ahead of election. Amnesty. Accessed online 24 June 2020 https://www. amnesty.org/en/latest/news/2021/01/uganda-authorities-must-lift-social-media-blockamid-crackdown-ahead-of-election/.
38. Privacy International (2017). For God and My President: State surveillance in Uganda Available at https://privacyinternational.org/sites/default/files/2017-12/Uganda_Report_1. pdf.
39. Uganda government websites hacked by international hackers 'Anonymousx64' over the weekend. Available at https://techrafiki.com/uganda-government-websites-hacked-byanonymous/.
40. For God and My President: State surveillance in Uganda Available at https:// privacyinternational.org/sites/default/files/2017-12/Uganda_Report.
41. Human Rights Watch: Uganda: Elections Marred by Violence Available at https://www.hrw.org/news/2021/01/21/uganda-elections-marred-violence.
42. Ministry of ICT & National Guidance. Draft ICT Skills and Training Needs Analysis. June.
43. 2021 Accessed during stakeholder consultation and validation workshop in July 2021.
44. United Nations: the age of digital interdependence. Report of the UN Secretary General's High-level Panel on Digital Cooperation. United Nations. Accessed online 20th.
45. June 2020 https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf.

For more information, please contact us:

KONRAD
ADENAUER
STIFTUNG

Centre for
MultiLateral
Affairs

**Konrad-Adenauer-Stiftung**
**Uganda & South Sudan**
E: info.kampala@kas.de

51 A, Prince Charles Drive, Kololo
P.O. Box 647, Kampala, Uganda
**www.kas.de/uganda**

@KasUganda

**Centre for MultiLateral Affairs**
E: info@theCfMA.org
T:+256-782-752198
T:+256-789-581006

Plot 67, Bukasa Road, Namuwongo
P.O Box 4411, Kampala Uganda
**www.theCfMA.org**