Chapter 13
National Security, Media, and Cybersecurity Threats:
A Strategic Framework for Secure Cyberspace Governance in Developing Countries

Kursim Leonard Fwa
National Institute for Policy and Strategic Studies, Nigeria

ABSTRACT

This chapter discusses the nexus between national security, media, and cybercrime in cyberspace governance. To achieve good governance within nations cyberspace, it becomes essential for the policymakers to exercise political, economic, and judicial procedures in a manner that ensures that the people are given their freedom to fulfil their duties and resolve their disputes in accordance with rule of law. The chapter provides policymakers with insights on how to improve the effectiveness of national security, counter cybercrimes within cyber governance institutions, and processes in the face of the changing nature of the use of media and its platforms. The chapter discuss the problematic, the concept cyberspace, cyberspace, and the changing dynamics and cybersecurity crime: trends, method, risks, and vulnerabilities. The chapter provides a strategic framework for a secure cyberspace in developing countries, taking cognisance of the realities and constraints within a developing milieu of the developing countries.

In battle, there are not more than two methods of attack—the direct and the indirect; yet these two in combination give rise to an endless series of manoeuvres.

—Sun Tzu, The Art of War

DOI: 10.4018/978-1-6684-4107-7.ch013

INTRODUCTION

The mass espousal of the Internet in the 1990s brought about an era of hope and optimism. Here was a platform that enabled instant communication and the sharing of and access to information. Early proponents asserted that access to the Internet would democratise societies in the long run. However, as The Economist points out, 'these days it is the Internet's defects, from monopoly power to corporate snooping and online radicalisation, that dominate the headlines.'(The Economist, 2019). Indeed, disregard for personal data by media by extension the social media networks, the notoriety of fake news and deep fake content, as well as the growth of cybercrime have dampened the early enthusiasm for connected societies. There is also an increase in cyber fatigue, as Internet users are constantly bombarded with privacy and safety warnings.

At the outset of the digital age, it was hoped that technology would inevitably bring about more openness, freedom and democracy. Unfortunately, since then authoritarian states have learnt how to manipulate technologies to silence dissidents and use the Internet as a propaganda outlet. These states furthermore cite security concerns, claiming protection of their citizens when they limit their rights to access social media platforms and messaging apps. The rise of fake news in a post-truth world has indeed been exploited by certain states, non-states actors, individuals and politicians, who create their own narratives as part of information warfare against local and foreign dissenters and critics. Anyone who has an opposing point of view is typically labelled as a 'foreign agent'. This is often followed by attacks on the person's integrity and character on social media and may be coupled with physical harassment or intimidation in the real world.

However, now that humanity is no longer viewing technology through rose-tinted glasses, it may be more mature about the regulations required. The road ahead is not paved or even well lit. Legislation and regulation are necessary to both enable the rights of citizens on the Internet and protect them from cybercrime and the unauthorised use of personal data (Turianskyi,2020:p 3). Governments need to perform a balancing act in these matters to ensure that there are appropriate regulations in place that allow them to deal with cybercrime without infringing on online freedoms or providing opportunities for security services to spy on their citizens. Maintaining a balance between protecting citizens from cybercrime and maintaining their Internet freedoms is indisputably difficult and is further complicated by the fact that technology tends to be years ahead of policy. Therefore, policymakers need to work with technology experts to stay up to date with the latest developments, as well as to ensure that regulation does not stifle innovation

The continuous development of the internet in the last few decades together with the resulting growth, innovation and capital investment in related technologies, compel developing nations to establish and mature its cybersecurity environment in order to mitigate the threats that accompany the vast capabilities that these innovations provide. The growing access of developing countries to cyberspace, requires that all such countries should have a proper plan to help secure their cyberspace. Although some documents for this purpose do exist, they are usually long and complex and do not provide simple and clear-cut guidance on where to start securing cyberspace. Developing countries, because of financial and expertise constraints, cannot do everything at the same time – so a more basic document is needed with clear steps on how to start

The structure of the Internet itself, which comes down to interconnected networks using standardised routing protocols and websites that may reside anywhere in the world, even on privately owned infrastructure, exacerbates the regulatory problems resulting in jurisdictional issues. The Internet is decentralised