# Chapter 15

# The Threat of Cyber Warfare in the SADC Region:

## The Case of Zimbabwe

**Jeffrey Kurebwa**
*Bindura University of Science Education, Zimbabwe*

**Kundai Lillian Matenga**
*Bindura University of Science Education, Zimbabwe*

## ABSTRACT

*This chapter is based on a study that sought to understand the threats of cyber warfare in Zimbabwe. The effects of cyber warfare, cyber intelligence mechanisms in place, and the status of the harmonization of laws and collaboration of SADC countries in efforts to address cyber threats were also covered. Qualitative research methodology was used to conduct the study. A total of 15 key respondents drawn from information technology experts, academia, top military personnel, and lawyers participated in the study. The study revealed that Zimbabwe was vulnerable to cyber warfare due to increased use of technology and failure to keep up with technological advancements. The study noted that the current legislation does not explicitly address cyber warfare threats but focuses more on cybercrime. The study recommended that Zimbabwe enact effective legislation to curtail cyber warfare in order to enhance cyber security. Investment in cyber security in terms of research and human capital development should also be prioritized.*

## INTRODUCTION

The threat posed by cyberwarfare through the use of computer hardware and internet related software technology by state and non-state actors has emerged as a transnational problem requiring an integrated collective security across borders in the 21st century (United Nations Office on Drugs and Crime, 2012). The threat of cyberwarfare has prompted the telecommunications industry, law enforcement agencies, and nation-states to improve on cyberwarfare counter intelligence mechanisms to secure their computer related network systems (Geers, 2015).

DOI: 10.4018/978-1-5225-5927-6.ch015

The global security debates on cyberwarfare can be traced back to the events in Estonia in 2007 following the discovery of Stuxnet, a malicious computer worm (Healy & Grindal, 2013). Andress and Winterfield (2012) highlighted that in 2007 Estonia was attacked by hackers who were believed to have links with the Russian government. Tikk, Kaska, and Vihul (2010) cited in Rid (2012, p.9) noted that, "Estonia at the time was one of the world's most connected nations; two-thirds of all Estonians used the Internet, and 95 percent of banking transactions were done electronically." The cyberattack brought down the websites of Estonia's parliament, banks, ministries, newspapers, and broadcasters (Andress & Winterfield, 2012). This experience resulted in the disruption of infrastructure and economic loss thereby threatening peace and stability of the country (Nguyen, 2013 p.1127–8).

In January, 2012, Israel also experienced a wave of cyberattacks which targeted websites of Tel Aviv Stock Exchange and the national airport. The banking sector was affected by disclosure of credit cards security information and account details of Israeli nationals (United Nations Office on Drugs and Crime, 2012). Internet technology in cyberwarfare was also responsible for the Russia-Georgia war of 2008. Maurer and Janz (2014) alleged that botnets and kinetic military operations were used to deface websites and to conduct Distributed Denial of Services (DDoS) attacks, which overwhelmed websites and ultimately rendering them inaccessible. The war primarily targeted the Georgian government and media websites thereby disrupting communication channels and generating confusion during the crisis.

Russia was accused of internet intrusion and hacking of the United States of America's servers during the 2016 elections thereby determining the electoral outcome in favor of Donald Trump (National Intelligence Council, 2017). The accusations leveled against the Russian President Vladimir Putin were that he ordered an 'influence campaign' in 2016 designed at the US presidential election. The consistent goals of which were to undermine public faith in the US democratic process, denigrate Secretary Hillary Clinton, and harm her electability and potential to assume presidency (National Intelligence Council, 2017).

In the SADC region, Zimbabwe and South Africa have also been victims of cyberattacks. Techzim (2016) claimed that a hacker group known as Anonymous Africa was responsible for issuing Distributed Denial of Service (DDoS) attacks to critical national infrastructure (CNI) such as the national media. The Herald Newspaper of Zimbabwe was alleged to have been attacked by Anonymous Africa ahead of the country's 2013 harmonized elections (Techzim, 2016). These cases of cyberwarfare have increased attention of scholars to research further on the implications of cyberwarfare to nation-states.

Cyberwarfare is emerging as a potential threat to state security and world peace. Governments around the world have, in response, established policies that govern interaction and collaboration among government entities, the private sector, the academia and civil society in collective efforts to mitigate cybersecurity vulnerabilities and attacks. Orji (2015, p.105) argued that some African intergovernmental organizations have also developed legal frameworks for cybersecurity.

Therefore, there is a growing consensus that nations bear increasing responsibility for enhancing cybersecurity. A related recent trend globally has been the adoption of long-term strategic plans to help deter, protect and defend countries against cyber threats. These national cybersecurity strategies outline a nation's core values and goals in the territory of cybersecurity law and policy, from mitigating cybercrime and espionage to preparing for cyberwarfare (Shackelford and Kastelic, 2016 p. 895). Some of the legal instruments adopted in Africa include the African Union Convention on Cybersecurity and Personal Data Protection (2014), Directive on Fighting Cybercrime (2011), and Model Cybercrime Law (2011), and Model Law on Computer Crime and Cybercrime (2012).