Dynamics in Cybersecurity: Challenges to Sri Lanka's National Security

B Senaratne
Faculty of Defence & Strategic Studies, General Sir John Kotelawala Defence University, Sri Lanka
bhagya.senaratne@kdu.ac.lk

Abstract- *Technological developments in today's world which take place annually, make technology accessible to individuals and communities that were previously not able to access it. The advent of mobile technology, its accessibility and affordability has enabled its penetration to all walks of society. This has therefore even empowered non-state actors and terrorist groups, which increases the threat individuals and states face.*

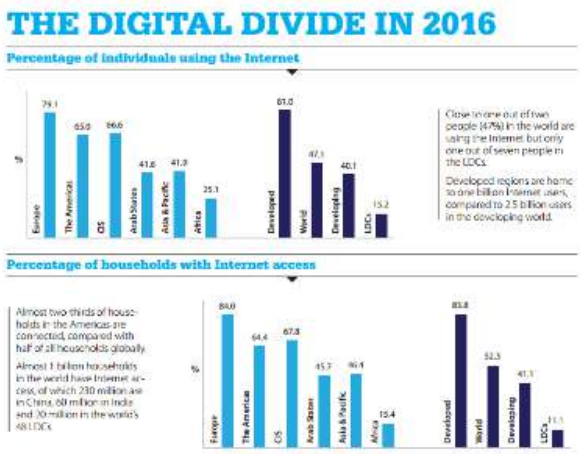
The objectives of this study are to examine whether Sri Lanka is prepared to face threats that could penetrate the country via the cyber domain and to illustrate what mechanisms the country needs to take to overcome these threats to national security. The methodology undertaken for this research is qualitative in nature, with primary data constituting of government policy documents, agreements and legal documents. A series of in-depth interviews too were conducted with professionals in the cybersecurity and legal spheres. Secondary data such as news clippings from newspaper articles, reputed web articles, journal articles and statistics from both the Department of Census and Statistics, Sri Lanka and the International Telecommunication Union too were utilised for this research. The study thus provides an assessment of the country's cyber security preparedness.

In conclusion, Sri Lanka needs to improve its legislature to implement the international treaties it is signatory to, as well as, empower its Armed Forces so that they are capable of assessing threats in the cyber domain and countering them. Furthermore, the country which is in the process of drafting a cybersecurity policy for the country, needs to identify mechanisms for implementation or a body that will monitor it.

***Keywords*— Cybersecurity, National Security, Sri Lanka**

INTRODUCTION

The world is witnessing an exponential growth in technology. Technological developments take place annually, making technology accessible to individuals and communities that were previously not able to access it. According to the International Telecommunication Union (ITU) 47% or approximately one out of two people in the world are using the Internet (2016, p.4). Mobile technology is penetrating every nook and corner of society due to its affordability, thus enabling even non-state actors and terrorist groups make use of it. Accessibility and affordability, thus increases the threat individuals, states and companies face. But it should also be noted, that even though technology is accessible, there are an equal number of the world population who still do not have access to this convenience and connection. According to Director of the ITU Telecommunication Development Bureau - Brahima Sanou, "over two-thirds of the population lives within an area covered by a mobile broadband network and that ICT services continue to become more affordable" (International Telecommunication Union, 2016, p.1).



Source: ICT Facts and Figures 2016, p.4.

As of 2013, the number of Sri Lanka's internet users was recorded as 21.90% of the total population, which is approximately a six percent growth from the previous year (International Telecommunication Union, 2014, p.1). Taking this growth projection, it can be understood that within a few years, half of the country's population will be connected to the internet, as a result to the entire world. Therefore, with these statistics and growth projections under its belt, it is crucial for Sri Lanka to contemplate on enabling national security by protecting itself from non-traditional security threats such as cyberterrorism and cybercrime.

Thus the primary objective of this study was to examine whether Sri Lanka is prepared to face threats that could penetrate the country via the fifth domain of warfare, i.e. the cyber domain. The secondary objective was to illustrate what mechanisms the country needs to take to overcome to face these threats to national security. Therefore, towards this end, the paper recommends policy initiatives and legal mechanisms that can be implemented to overcome this shortcoming.

The methodology undertaken for this research is qualitative and exploratory in nature, with primary data constituting of government policy documents, agreements and legal documents, interviews with officials from the Armed Forces, the civil and diplomatic services in addition to speeches and strategy documents. The research also utilised information gathered during workshops and panel discussions on Cybersecurity in Sri Lanka. Further, the research utilised secondary data such as academic publications, newspaper articles, reputed web articles, journal articles and statistics from both the Department of Census and Statistics, Sri Lanka and the International Telecommunication Union. The study thus provides an assessment of the country's cybersecurity preparedness and undertakes its analysis via the realist notion of power. The study provides an assessment of the country's cybersecurity preparedness and undertakes its analysis via the realist notion of power. Towards this end, the research utilised both the PESTLE, i.e. politics, economic, social, technological, legislation and environmental, and STEEP, i.e. society, technology, environment, economy and politics, analysis tools to evaluate the cyber security challenges to Sri Lanka.

An understanding of concepts such as cybersecurity and its correlation between cybercrime is required as these will be drawn on to explain the salient points of this paper. It is equally important to comprehend the concept of national security, as the main argument of this paper is based on the threats faced by Sri Lanka at present and a foresight on the future threat perception.

A. Cybersecurity

The term cyberspace was coined by William Gibson in 1984 with reference to the internet and other networks, which proceeded to the prefix 'cyber' being used with phrases like 'crime' and 'security' (Fernando, 2016a). According to Jayantha Fernando, "cybercrime is not defined in legal conventions or treaties" (2016a), this definitional shortcoming leads to difficulties in implementing proper policies to curtail the occurrence of internet based crime and violence.

According to the International Telecommunication Union, cybercrime can be defined in both a narrow sense (computer crime) and a broad sense (computer-related crimes). The narrow sense defines cybercrime as an illegal activity "that target the security of computer systems and the data processed by them" (2012, P. 19). In the broader sense, cybercrime refers to "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (International Telecommunication Union, 2012, p.19). Further, it can be simply termed as acts that harm the security and privacy, data and information of individuals, organisations or states. These crimes are various in nature such as hacking; phishing; harassment via e-mails, social media such as Facebook, Twitter etc.; e-mail spoofing; cyber trespassing, cyber-squatting, malware transmission; violations to Intellectual Property; crimes against government; cyber terrorism; crimes against society at large; financial crimes (Fernando, 2016a). This illustrates that cybercrime encapsulates a broad range of activities which are both illegal and harmful to the victim.

The United States Department of Homeland Security (DHS) views cybersecurity as illegal activities that undermine the safety of the cyberspace by targeting its vulnerabilities. It further defines that these threats can be either physically or technically executed by either persons skilled in information technology or nation-states (2016). Activities that can be highlighted as threats against cybersecurity are related to "…steal[ing of] information and money …developing capabilities to disrupt, destroy, or threaten the delivery of essential services" (United States Department of Homeland Security, 2016). The DHS further adds that a wide variety of traditional crimes related to child pornography, banking and financial fraud and intellectual property violations are now being committed via the cyberspace (2016).

It needs to be understood that cyberwarfare is largely connected with information warfare. According to James Adams, information warfare can be categorised into three definite areas. They are, "…perception management where information is the message, systems destruction where information is the medium, and information exploitation where information is the opponent's resource to be targeted" (1998, P. 17). This definition showcases the enormity of the problem at hand and the critical importance of cybersecurity.

Cybersecurity is seen as increasingly necessary and mandatory for a country due to its ability to organise and conduct traditional threats via the cyberspace, as well as because it can harm the bilateral relations between countries via its various illegal activities. Security in this space is vital as the next battle space will be determined by bits and bytes, not bullets (Adams, 1998, p.14).

B. National Security

The legal definition provided by US Legal refers to national security as "…the protection of a nation from attack or other danger by holding adequate armed forces and guarding state secrets." The term entails within itself other aspects of security such as economy, energy, environment, military, natural resources and politics. (US Legal, n.d.). This shows that these are areas of concern for Sri Lanka when seeking to protect its national security in the cyber domain. Not only does the term emphasise that

it is the foundation of freedom and prosperity within a nation, it also underscores sovereignty. Papp and Alberts define national security as "… the protection of a state, its territories, and its peoples from physical assault by external forces, as well as the protection of important state economic, political, military, social, cultural, and valuative interest[s] from attacks emanating from foreign or domestic sources which may undermine, erode or eliminate these interests, thereby threatening the survival of the state" (2000, p.245). This illustrates that in the future Sri Lanka cannot only be mindful of its physical borders, but has to be conscious of its virtual borders as well. The duo discuss about both military and non-military means that are utilised to protect and safeguard national security (Papp and Alberts, 2000, p.245). It is thus clear that the concept of national security is broad and that it has no clear and precise boundaries. However, factors such as wealth, geography and military force affect and influence this broad concept.

From a realist and neo-realist prism, national security can be defined as maintaining or safeguarding the state's elements of power in the fields of military, economy and politics (Waltz, I979). Furthermore, Buzan describes security as "…the pursuit of freedom from threat and the ability of states and societies to maintain their independent identity and their functional integrity against forces of change which they see as hostile" (1991, p.432).

The national security policy (NSP) of a country is the framework document which explains how a country will safeguard its citizens and borders from internal and external threats. According to the Geneva Center for the Democratic Control of Armed Forces (DCAF), an "NSP has a present and future role, outlining the core interests of the nation and setting guidelines for addressing current and prospective threats and opportunities" (2005). It is also the policy document in which actors that safeguard national security are described in. Therefore a National Security Policy performs an important role in safeguarding the national security of a country.

II. CHALLENGES TO SRI LANKA'S NATIONAL SECURITY

It must be noted that non-traditional security threats from the cyber domain or information warfare is a very recent security challenge to Sri Lanka as the island was facing threats from the traditional spheres up until the first decade of the 21st century. Even though this phenomenon is relatively new to the South Asian country, it has been a problem worldwide since at least the end of the Cold War, when a fundamental revolution in warfare occurred (Adams, 1998, p.14). For developed countries like the United States "information warfare was already a reality" by the end of the 20th century (Adams, 1998, p.14).

Many businesses have gone online in Sri Lanka and even government institutions have implemented e-governance in an attempt to create more access and convenience to the public. Therefore, the vulnerability of businesses and individuals to attacks is increasing and would continue to increase in the future with the increased move to digital platforms. "Businesses … and societies have become networked by means of ICT," stated Minister for Telecommunication and Digital Infrastructure Harin Fernando at the third annual Cyber Security Summit (Illanperuma, 2015). He further stated "within this context, cyber security plays a key role and should be regarded as the highest priority, with its power to potentially paralyse an organisation as well as play havoc with people's lives." This showcases that the Sri Lankan government has identified the threat the country faces within the cyber domain.

The fact that unauthorized actors can come and establish themselves in Sri Lanka is worrying. It is equally alarming that illegal money can enter the country to be transferred to other global actors. It is advantageous that Sri Lanka managed to identify "…a dubious NGO … that tried to sneak in millions of US dollars stolen by Chinese hackers from the Bangladesh Central Bank…" (Samath, 2016). Instances such as this are causes for concern for Sri Lanka's national security, as it undermines the country's financial capability.

According to Abhaya Induruwa, "[c]yber threats are growing in intensity and scale. We've seen significant breaches at government agencies and in private businesses...", a situation he claims has brought about a lot of awareness among the layman, in comparison to before when knowledge of threats from the cyber domain were restricted to the knowledge of the IT professionals (Ceylon Today, 2017). Sri Lanka was extremely fortunate to have witnessed only one attack from the WannaCry Ransomware attack that took place in May 2017 (EconomyNext, 2017). However, this does not alleviate the possibility that Sri Lankans could be the victims of far greater a security threat.

When analyzing Sri Lanka's cybersecurity challenges according to PESTLE, it can be understood that there are direct threats to the country's political, economic, social and technological spheres. It also poses absolute threats to the country's legislation, as it will require new legislation relevant to the Sri Lankan context to be prepared in order for the country to face these new challenges in the fifth domain of warfare.

According to Clausewitz, 'war is a mere continuation of politics by other means', which showcases that various political goals can be brought to action even via the cyber domain using it as a means to cause discomfort and harm

to various segments of society, be it the political hierarchy, businesses, military or even the ordinary citizen. As per Thomas Rid, there might be economic repercussions in a society that is highly networked, even if the attack was not meant to be violent in nature (2014, p.410).

As much as wars are fought using conventional weapons, a majority of them are now using modern technology to ensure communication within the systems (Adams, 1998, p.17). Thus the functioning of systems would depend on for example modern microprocessors. Therefore, despite the common understanding that a cyber-attack would primarily harm the information systems and financial sector of the country, little attention has been paid to the damage that can be derived from such an attack on modern military equipment. As stated above, wars are intrinsically connected with politics, as all attacks are politically motivated. Hence, it is important to understand that Sri Lanka's conventional military hardware too are at a risk of attack as much as its networked infrastructure.

III. MECHANISMS TO OVERCOME CYBERSECURITY CHALLENGES

According to William Lynn, "Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air and space" (Rid, 2014, p.408). Therefore whatever mechanisms Sri Lanka is taking, attention also needs to be given to empower the Tri-Forces to face this threat. As much as the Sri Lanka Computer Emergency Response Team [SL|CERT] is capable of countering certain threats and creating awareness among the public about security threats from the virtual domain (Palliyaguru, 2015) such as with the WannaCry Virus, it is equally important for the armed forces and police to be equipped with the know-how to counter future security breaches.

Sri Lanka became a signatory to the Budapest Convention or the Convention on Cybercrime in September 2015 which was drafted by the Council of Europe. This convention looks at addressing criminal activities online. Prior to this, Sri Lanka enacted specific legislation on cybercrime via the Computer Crime Act 2007. It further became signatory to the United Nations Convention on the Use of Electronic Communications in International Contracts in 2015.

Induruwa, a pioneer in Sri Lanka's information and communication technology (ICT) industry stressed on "…the concept of enhanced public/private information sharing and developing standards, and crafting a cybersecurity framework for Sri Lanka that addresses risks across government and industry" at The Cyber Security Forum held In July 2017 (Ceylon Today, 2017). He further highlighted that a cybersecurity framework should facilitate economic growth and create an enabling environment for innovation.

It was observed during this study that even though Sri Lanka has ratified numerous international treaties, it does not have an officially recognised national cybersecurity policy to implement internationally recognised cybersecurity standards. This is an area the government and lawmakers need to look into as implementation of laws and policies are essential in curtailing threats to Sri Lanka's national security. The ITU too has observed this lacuna in its 2014 report which states "Sri Lanka does not have any officially approved national (and sector specific) cybersecurity framework for the certification and accreditation of national agencies and public sector professionals." The researcher learned that while the Sri Lankan Armed Forces have initiated several mechanisms towards securing their virtual borders, the present government is keen on implementing a National Cyber Security Agenda inclusive of a Cybercrime Framework with the objective of ensuring trust and confidence for electronic transactions through legislative and policy measures (Fernando, 2016b; Illanperuma, 2015).

According to a former Commander of Sri Lanka Army, the LTTE might not be the only non-state actor that is interested in attacking Sri Lanka (2011). Therefore, having recognised that information warfare or cyberwarfare is an actuality even for a small state like Sri Lanka, it is important for Sri Lankan authorities to assess the vulnerability and determine from where the country's virtual borders would be most vulnerable to attack.

However, irrespective of the method followed in ensuring threats to Sri Lanka from the cyber domain are mitigated, these efforts need to not only be a whole-of-government approach, but a multi-stakeholder approach where both the public and private entities come together to address this very current problem.

IV. CONCLUSION

When Sri Lanka's cybersecurity is applied to the 'STEEP' model, it indicates that the country will face immediate and long-term threats to its national security due to the threats posed to the technological realm which will also trickle into the economic and political spheres. According to Buzan, security needs to be viewed from a comprehensive approach, therefore, enabling security in the cyber domain is important for Sri Lanka to ensure other elements of its national security are safeguarded.

Towards this end, there are many steps Sri Lanka has to take to ensure the country's political, economic and technological spheres are safeguarded. And one of the key elements in this regard is to initiate local legislature to implement the international treaties Sri Lanka is signatory

to. Moreover, measures need to be taken to empower Sri Lanka's Armed Forces so that they are capable of assessing threats in the cyber domain and countering them.

In conclusion, Sri Lanka needs to assess its vulnerability to determine what steps need to be taken in preparation of such threats. Further, it is necessary for Sri Lanka to initiate a multi-stakeholder approach to its conceptualisation of addressing cybersecurity threats. Towards this end, it is essential to engage with the Armed Forces and the Police, the public sector and the private sector in formulating a National Cyber Security Policy. Sri Lanka has to strengthen its law enforcement capabilities in the cyber domain by empowering a specific body, thus ensuring stringent measures are taken towards the implementation of such laws and frameworks that are enacted.

C.References

Adams, J. (1998) *The Next World War: The Warriors and Weapons of the New Battlefields in Cyberspace.* London: Hutchinson.

Aneez, S. (2016) Sri Lankan in Bangladesh cyber heist says she was set up by friend. *Reuters.* 31 March 2016. Available from:http://www.reuters.com/article/us-usa-fed-bangladesh-sri-lanka-idUSKCN0WX1UI(30 April 2017)

Buzan, B. (1991) New Patterns of Global Security in the Twenty-First Century. *International Affairs (Royal Institute of International Affairs 1944-)*. Vol. 67, No. 3 (Jul., 1991), Blackwell Publishing p.431-451. Available from: http://www.jstor.org/stable/2621945

Ceylon Today. (2017) SLT holds industry forum on cyber security. 10 July. Available from: http://www.ceylontoday.lk/print20170401CT20170630.php?id=25109

EconomyNext. (2017) Inter-agency cyber security effort mooted for Sri Lanka. 22 May. Available from: http://www.economynext.com/Inter_agency_cyber_security_effort_mooted_for_Sri_Lanka-3-7977-7.html

Fernando, J. (2016a) International Dimensions of Cyber Security & Cybercrime. *Lecture.* November 2016.

---. (2016b) Cyber security & Cybercrime Strategies Sri Lankan Experience. *Lecture.* 18 April 2016. Available from: http://unctad.org/meetings/en/Presentation/dtl_eweek2016_JFernando_en.pdf

Geneva Center for the Democratic Control of Armed Forces. (2005) National Security Policy. *Backgrounder: Security Sector Governance and Reform.* November 2015. Available from: www.dcaf.ch/publications/backgrounders

Illanperuma, S. (2015) Harin to create "digital democracy" with cyber security protection. *Circa Holdings.* 30 September. Available from: http://www.cicra.lk/harin-to-create-digital-democracy-with-cyber-security-protection/

International Telecommunication Union. (2016) ICT Facts and Figures 2016. P. 4. Available from: http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2016.pdf

---. (2014)
Available from: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx

---. (2013) ITU statistical market overview: Sri Lanka. Available from:
http://www.itu.int/net/newsroom/GSR/2012/reports/stats_sri_lanka.aspx

---, (2012) Understanding cybercrime: Phenomena, challenges and legal response. Available from: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

Palliyaguru, R. "The Role of the CERT in Supporting a National Strategy". *GLACY International Conference.*Available from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680303cdf

Rid, T. "Cyber war will not take place". *Strategic Studies: A Reader*. Ed. Thomas F. Mahuken and Joseph A. Maiolo. 2nd Edition. London: Routledge.

Samath, F. (2016) Sri Lankan teller helps bust world's biggest bank fraud. *Sunday Times.* 13 March. Available from: http://www.sundaytimes.lk/160313/news/sri-lankan-teller-helps-bust-worlds-biggest-bank-fraud-186459.html

Sri Lanka Army. (2011) "'Be Prepared for the Cyber War after the Physical War' â€" Commander of the Army". Available from:http://www.army.lk/news/%C3%A2%E2%82%AC%CB%9Cbe-prepared-cyber-war-after-physical-war%C3%A2%E2%82%AC%E2%84%A2-%C3%A2%E2%82%AC%E2%80%9C-commander-army-0

United States Department of Homeland Security. (2016) Cybersecurity Overview. 27 September. Available from: https://www.dhs.gov/cybersecurity-overview

Waltz, K. N. (I979) *Theory of international Politics*. Reading, Mass.: Addison-Wesley. P. I29-3I.

BIOGRAPHY OF AUTHOR

Bhagya Senaratne is a lecturer at the Department of Strategic Studies, Faculty of Defence & Strategic Studies, General Sir John Kotelawala Defence University. She contributes extensively to both local and international publications. Her most recent article titled "Elements of Sri Lanka's Geopolitics: Impact on United States' Foreign Policy" appeared in the *Maritime Affairs: Journal of the National Maritime Foundation of India* (Routledge, 2016) and she has also contributed a book titled *Maritime Safety and Security in Indian Ocean* (Vij Publications, 2016). She recently edited the publication

titled *Pakistan-Sri Lanka Relations: A Story of Friendship* to which she also contributed a chapter titled "Economic Relations: A Sri Lankan Perspective" which was a joint collaboration between KDU – Sri Lanka and NDU - Pakistan (NDU Pakistan, 2017). An alumnus of the Ship for World Youth Programme organised by the Cabinet Office of Japan and the Geneva Center for Security Policy - Switzerland, she has also represented Sri Lanka in numerous international fora. Ms. Senaratne is presently reading for her MPhil leading to a PhD at the University of Colombo. Her research interests are Diplomacy, Strategic Communication, Foreign Policy, Cyber as an Emerging Security Threat and Sri Lanka's role in the Indian Ocean Region.