Achieving Resilience through Digitalization, Sustainability and Sectoral Transformation - What Are the Long Term Strategic Options and Reforms for Sri Lanka Armed Forces

Major General Robin Jayasuriya RSP, psc, ndc, MSc S&SS, MPhil[1#]

[1]Faculty of Defence and Strategic Studies, General Sir John Kotelawala University

[#] fgs-1001dsspr22006@kdu.ac.lk

***Abstract*—*Periodic circumstances in Sri Lanka's history have warranted strategic realignment of its instruments of national power to suit changing global and regional power dynamics. Recent global events and regional incidents have pushed Sri Lanka to look inward and among others rethink its Economic, Foreign and Military Grand Strategies. The paper touches upon unconventional/asymmetric warfare, cyber warfare and the use of Intelligence and clandestine operations as an alternative to ensuring national security and a war strategy for numerically inferior smaller states. Clausewitz asserts that the defensive mode of warfare possesses inherent strength surpassing that of the offensive. In order to overcome this formidable defensive strength, Clausewitz contends that an army's most effective weapon is the advantage of superior numerical strength. Based on this theoretical framework, it may be argued that a significant number of countries globally face economic constraints that prevent them from maintaining numerically superior military forces. In his book "Spec Ops," William H. McRaven postulates that smaller forces might attain a position of relative supremacy within limited timeframes. The paper does not establish a connection between the concept of relative supremacy and the instruments of power related to Diplomacy and Foreign Policy, Trade, and Economy. The concept is often emphasised in the military sphere as a feasible path of action.*

Key Words: Relative strength, unconventional / asymmetric warfare, numerically inferior

I. INTRODUCTION

The rise of complex super power competition in the Indian Ocean Region (IOR) has become the economic and political centre of gravity in the Indo-Pacific paradigm (Bhat, 2022) and Lanka appears to be right in the middle of this quagmire. The Indian Ocean Region (IOR) and global geopolitics created a new arena where major forces will compete, with far-reaching effects on the area and the entire world. In this context, defending the sovereignty and territorial integrity and safeguarding Sri Lanka's core values entrenched in the constitution become of paramount importance. Rebuilding Sri Lanka to forge new mechanisms between regional players in order for it to respond to these changing power politics and rethinking national security policy and strategy to achieve resilience through digitalization, sustainability and sectoral transformation is timely with contemporary long term strategic options and reforms for Sri Lankan Armed Forces.

While Sri Lanka is keeping open it's Diplomatic and Foreign Policy channels it is reorienting some of its economic policies in order to bail out the present economic crisis the country is facing.

In the military domain it has taken up the quintessential task of reorganising the Armed Forces to face new threats. However, even though Sri Lanka has the capability to defend limited geographic areas, the question remains if it can sustain a prolonged conflict of a high tempo attrition war with limited incursions in depth? In the paper the author from purely an academic point of view has suggested and broadly sketched out a strategy of unconventional warfare based on Willim H McRavens theory of Unconventional warfare and the concept of Relative Superiority where he hypothesizes that numerically inferior forces can achieve relative superiority for short periods through the use of unconventional warfare. With rapid development in the AI, information systems and technological domains the concept of unconventional/asymmetric warfare can be applied within the concept of relative superiority in the cyber domain as a strategy for national security.

II. CHANGING DYNAMICS AND STRATEGY FOR SRI LANKA

In the face of cognizant developments Sri Lanka has to posture its instruments of national power to orchestrate to

develop and execute a strategic option for Sri Lanka. Apart from the traditional instruments of power Diplomatic, Informational, Military, and Economy the author recognizes "Public Will" which also translates as the will of the strategic leadership and the will and resilience of the people as another instrument of national power. In addition, technology is also identified as a very important sub paradigm of national power.

Intangible economic assets, such as the volume of a state's gross national product (GNP) or the size of its defence sector, may naturally only provide a partial understanding of a state's military capability. According to van Crevald's research (1991, chapter 20), a higher morale and training can frequently compensate for a lack of superior armament. Other key intangibles are a state's organisational capacities and administrative prowess, which allow it to make the most of the resources it possesses and maximise their potential return on investment.

In context of conventional war and national security, the very reason states engage in defence coalitions or alliances are to improve relations with nations in order to deter potential adversaries or in expectation of collective protection from more powerful adversaries. Considering this the following strategic dilemma remains; (a) in the event an alliance is formed with a country, to what degree of action will it commit? and; (b) how reliable will the partnership be? (c) will the alliances risk sharing cyber, and information satellite platforms etc..(d) what is the collateral damage of that country losing its strategic autonomy?

Therefore taking all this into consideration the need to craft and implement coherent achievable strategies for Sri Lanka is very important. Also being self reliant economically and militarily is vital for the *honourable* existence of Sri Lanka. As strategy must be based on factual threat assessments and probabilities it should be realistic in concept and application[1].In this context, the threat landscape into the next decade or more will be shaped by geo-strategic, political, economic, nuclear military, space and cyber contours that will dictate future conflicts. Is Sri Lanka holistically ready to face these situations today? No. Therefore strategy must evolve as per ground reality and present and foreseeable future circumstances.

1).Military modernisation: The process of defence modernisation involves the replacement of old obsolete weapons and weapon systems with more contemporary ones and also the change of doctrine form internal security to external security based on each countries threat perception of perceived and real threats. Even though economically underdeveloped countries will face difficulty in modernisation in the realm of national security this there is little option.

No military force that thirst for modernization can get by without nurturing, new technology, while the demands of war have always been the mid wife of new technology. During the gulf war , more than 500 kinds of new and advanced technology of the 80s and sent it to the stage to strike a pose, making the war simply seem like a demonstration site for new weaponry. (Qiao Liang, 2007, pp. 4-5) .The ability to coordinate multiple weapons over long distances in real time has resulted in an unparalleled combat capability, a development that was previously inconceivable prior to the advent of information technology. The advent of technological integration and globalisation has rendered traditional categorizations of warfare obsolete, thereby reshaping the dynamic between weapons and war. The emergence of novel conceptualizations and particularly innovative weapon concepts has progressively obscured the conventional understanding of warfare. Can a single cyber attack be considered a hostile act, or can the use of financial tools to destabilise a country be classified as a battle? (Qiao Liang, 2007, pp. 4-5). In this context, Sri Lanka cannot only be mindful of its physical borders, but has to be conscious of its virtual borders as well as both military and non-military means that are utilised to protect and safeguard national security. It is thus clear that the concept of national security is broad and that it has no clear and precise boundaries. (Senaratne, 2010). Given the conventional understanding of war, the startling realisation that non-war actions may potentially serve as novel elements in future warfare, further gives credence to the concept of unconventional and asymmetric warfare as a strategy to numerically inferior forces.

II. SECURITY CHALLENGERS

A. Threat Factor

There is no major conflict threat facing Sri Lanka following the 2009 conclusion of a long-running civil war. However, unresolved communal tensions are a problem, notably in northern and eastern provinces. Considering the present security environment as indicated in an article in the Ministry of Defence website "prior to 18th May 2022, the Indian intelligence had warned of a possible ex-LTTE to plan to carry out an attack in Sri Lanka (Dias, 2022). There is also a growing concern over Islamist

[1]Defence Academy of the United Kingdom.(2017). Getting Strategy Right. (Available online). https://www.da.mod.uk/Portals/0/Documents/RCDS/20170904CDS_Getting_Strategy_Right_Enough_Final.pdf?ver=2017-09-08-090748-807. [Accessed 2020]. Pg 22 .

radicalization and Islamic State claimed suicide attacks on churches and hotels in April 2019 (Crisis 24 Sri Lanka Country Report, 2023). Among other concerns Sri Lanka's geographical location between the golden crescent and golden triangle, two main drug production regions in the world has influenced the inflow of drugs into the country resulting in a growing drug problem in Sri Lanka (Dias, 2022). In addition to the aforementioned, the social movement that took place in Sri Lanka in 2022 shared characteristics with the 'Arab Spring' in the Middle East. The protests in Sri Lanka took place as the nation was going through its worst economic crisis since gaining independence. Apart from Terrorism, Religious Extremism Transnational Organised Crime and geopolitical competition in the region the use of social media and new social movements has come to the forefront of security concerns.

1) Cyber Security: The integration of technology in both our personal, professional and national security spheres has become increasingly intertwined, surpassing previous conceptions of possibility within an only few decades. Cyber-attacks, in support of conventional military operations have a great deal of potential to be force multipliers on today's complex battle fields. Imagine a simultaneous attack in cyber space and in the physical realm, designed to cripple a country's ability to communicate, both internally and externally, and making it virtually unable to defend against a military assault by conventional forces. In 2008, that very scenario was carried out in the Russo-Georgian conflict with Russian conventional operations supported and its success enhanced by a carefully coordinated cyber strike, via a surrogate force, that was able to render the Georgian Republic incapable of defending itself in either the cyber or physical domain. (Eidman, 2014).

The integration of cloud computing, mobile technology, and high-performance personal devices has fostered a culture characterised by convenience, enhanced collaboration, and increased productivity. (Roles and Responsibilities of Cyber Security Professionals, 2023). While the ease provided by this phenomenon might be acknowledged, it also facilitates the potential for hackers to acquire unauthorised access to our sensitive personal data, regardless of its location or the network it traverses. These individuals with malicious intent possess significant motivation as well, as there exists a profitable market for the trade and misuse of such data. Despite the presence of highly skilled Cyber Security Professionals, it is inevitable that hackers and cybercriminals will ultimately discover means to gain unauthorised access to one's data. (Roles and Responsibilities of Cyber Security Professionals, 2023) Nevertheless, it is important to note that not all circumstances are devoid of hope. Information technology security specialists are actively engaged in the forefront of combat, diligently striving to safeguard against the ever-changing array of threats.

2)Social Media: The concepts of 'traditional propaganda' and 'psychological warfare' have been vastly replaced by those of 'information warfare', 'information operations' and 'psychological operations' (Huhtinen & Rantapelkonen, 2003). Kotelenets & Barabash (2019) coherently compare and contrast the difference between the doctrines of propaganda and information war, where they note that propaganda mainly emphasises the positive perception of 'us', while information warfare is the act of emphasising the negative image of 'others'. On the other hand social media uses a combination of propaganda, psychological warfare and information warfare for mass mobilisation and exploitation of the public for political purposes to an extent that it has now become a threat to national security. Social media is also used to shape a political environment, to orchestrate large scale protest, move organisations, penetrate into all segments of society including school children and lastly to scale social stratification to mobilise from public sector trade unions (public and private sector) to private sector employees. As in many other countries of the world in Sri Lanka there appears to be a growing complicit secret social surround that serves to bring together likeminded individuals through the internet and other social media platforms. This is a medium that is hard to monitor and preventive action is hard to come by. Sri Lankan security sector is presently not geared to handle a large scale situation due to lack of expertise, technology and infrastructure.

3) Impact of Social Media: The impact of social media platforms on the political systems of diverse nations can exhibit significant variations. The impact exhibits variation across democratic and authoritarian governments, encompassing both inter- and intra-state dynamics. It primarily hinges upon three key political actors: domestic resistance, external factors, and the governing regime. The effects of social media can vary depending on the utilisation strategies employed by three players, namely individuals, organisations, and governments. Additionally, the impact is contingent upon the level of state capability and the type of political system in place. Consequently, four distinct effects of social media can be identified. The phenomenon under consideration can potentially undermine robust democratic regimes, amplify the power dynamics within strong authoritarian regimes, radicalise feeble democratic regimes, and induce instability within weak authoritarian regimes. (Guy Schleffer, 2021).

Coupled with these threats like many other countries in the region and the world Sri Lanka too is vulnerable and susceptible to a diverse range of cyber related occurrences, regardless of their goal or origin. According to statistics 63 percent (63%) of cyber attacks comes as internal threats (Threat Intelligence, 2023). The information transmitted within cyberspace is susceptible to being utilised for malicious objectives by both governmental entities and non-state individuals or groups. It is foreseeable that terrorists will soon be responsible for significant cyber incidents, as they have progressed beyond mere website defacement and are now capable of inflicting tangible harm onto their adversaries, particularly targeting key infrastructure. To this end, on 18th of May 2018, the organization called "Tamil Eelam Cyber Force", hacked the Sinhala version of the official website of the Ministry of Tourism Development and Christian Religious Affairs. Furthermore, they hacked the website of the Democratic Socialist Republic of Sri Lanka Honorary Consulate in Kerala. (Bulathgama, 2023). Further, Local media reported in August that year of a loss of an estimated two terabytes—or 2,000 gigabytes—of classified information from the Lanka Government Cloud (LGC), which risked endangering the business relationships of local drug companies with their foreign principals (ECONOMYNEXT, 2023). The implications of these development will have a profound impact on the whole security dynamics of Sri Lanka. In order to effectively address the challenges of cyber security and mitigate the risks of cyber war and cyber crimes, it is imperative to establish a shared vision and collaborative efforts on an international scale. Sri Lanka ranks 81st out of 175 countries in the National Cyber Security Index. In January, it scored a 0 for protection of digital and essential services. The country was, however, given nine out of nine points for education and professional development (Dobberstein, 2023). The threat landscape continues to expand with the increasing connectivity of devices and systems through the Internet of Things (IoT) and the proliferation of digital technologies. Cyber attacks such as ransom ware, phishing and insider threats remain pervasive and pose significant risk to enterprises, governments and individuals alike. Although these threats are nothing new, as data continue to be produced and stored in greater volumes, and as connectivity expands globally, the attack surface has become more exploitable with gaps and vulnerabilities that are appealing to criminal and nation-state hackers. In 2023, cyber threats are expected to rise as unrest around the world contributes to an increase in cybercrimes. Malware attacks (e.g., ransom ware attacks) are also expected to target more enterprises. (Lim, 2023). In a strategic environment that is shifting from conventional threats to cyber and information domains, the threat priority for Sri Lanka in the present should be cyber security and emphasise the need of including cyber security as part of unconventional defense strategy for Sri Lanka.

Through the years Sri Lanka developed its military capability mainly to counter terrorism and separatism with the LTTE as its primary adversary. In any conventional military eventuality Sri Lanka as an Island nation does not geographically have a strategic or even a tactical depth. Sri Lankan Armed Forces are not equipped and does not have the capacity of denying territorial gains to be able to take on an offensive posture by opening multiple fronts along its border and fighting a limited geographical battle and even gaining tactical victories. Nevertheless, the short term defensive battle will have to be fought to retain the initiative and deny penetration in depth. But, how about the long term strategy? Therefore, the author suggests a long term strategy totally opposite to conventional military thinking, which is a strategy of unconventional and asymmetric warfare.

B. The Strategy

Clausewitz states that "The defensive form of warfare is intrinsically stronger than the offense" and to defeat 'the stronger form of warfare' "an army's best weapon is superior numbers".[2] Given this theoretical construct most countries in the world cannot economically have the luxury of numerically superior forces. However, in his book "Spec Ops" William H McRaven hypothesize that numerically lesser forces can achieve relative superiority for short durations by the employment of Special Forces operations. In the paper the concept of relative superiority here is not associated to Diplomacy and Foreign Policy, Trade and Economy aspects of the National Instruments of Power. The concept is much highlighted in the Military and Cyber domain as a viable course of action.

IV. UNCONVENTIOANL WARFARE

Unconventional warfare which is always thought about as a broader area of special warfare could be another "course of action that integrates ends, ways and means to meet policy objectives"[3] in the long term. Here the author looks into concept of Special Operations as iterated by Willim H McRaven in his thesis "The Theory of Special Operations"

[2]William H McRaven.(1993). The Theory of Special Operations. Naval Post Graduate School. Monterey, California. Pg 2.

[3] Defence Academy of the United Kingdom.(2017). Getting Strategy Right. (Available online). https://www.da.mod.uk/Portals/0/Documents/RCDS/20170904CDS_Getting_Strategy_Right_Enough_Final.pdf?ver=2017-09-08-090748-807. [Accessed 2020].

where he uses the concept of Relative Superiority - "Relative Superiority can be defined as a condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well defended enemy"[4] which is an appropriate form of warfare for smaller forces to fight more advanced forces where the "concept of relative superiority theory" could be applied to unconventional warfare with ingenuity and cunning to gain advantage and retain initiative over larger forces. Unconventional Warfare is defined as "operations conducted by, with, or through irregular forces in support of a resistance movement, an insurgency, or conventional military operations".[5] The author also suggests in this paper using the concept of relative superiority to the cyber domain and as part of the strategy to achieving resilience through digitalization, sustainability and sectoral transformation as a part of reforms for Sri Lanka's Armed Forces. Given that Sri Lanka faces a number of security challenges, including terrorism, maritime piracy, and natural disasters digitalization can help the Sri Lankan military to address these challenges by improving its intelligence gathering, communication, and coordination capabilities as defensive and offensive cyber security measures.

1)The Human Factor: Unconventional warfare as a means to achieving strategic objectives lies more on the human factor such as motivation and will to fight, loyalty, and spirit de corps, strong belief in the cause, leadership and initiative and values more than in weaponry. However, in the future wars these values will not compensate for the lack of knowledge in the cyber domain while the manner or the modus operandi of unconventional warfare will depend on the larger context of the war, while the entire spectrum of war, whether it is large scale general or nuclear war or a cold war situation it will provide opportunities for unconventional warfare in the physical domain and in the cyber domain.

In this paper the author refers unconventional warfare as a strategy not only in the military domain as it alone is highly unlikely to achieve the desired outcome or end state unless it is applied with other available instruments such as digital and cyber domain[6], information warfare, psychological operations, intelligence and clandestine operations/ covert operations, exploitation of available fault lines and maintenance of a high degree of secrecy. Here, the author referrers to unconventional warfare not in the sense of using tactics opposite to conventional norms but goes beyond the military understanding of unconventional and include the condition between supported non state actors, perception or psychological warfare where rival nations try to impose their national interest by imposing on own strengths and weaknesses, subverting transnational information systems, drug warfare, financial warfare, cultural warfare, media and fabrication warfare (Qiao Liang, 2007, p. 12). For the strategy to work "as current UK doctrine notes, the instruments '...should act together, unified behind a common national goal"[7].

2)The military domain of unconventional warfare : The military domain of unconventional warfare will encompass all facets of guerrilla war from hit and run tactics to subversion and sabotage deep in the enemy rear areas from minor harassing tactics to chosen strategic assets or disrupting lines of communication in order to force the enemy to commit time, troops and resources as a defensive measure for numerically inferior forces. The smallest Special Forces team to be deployed should be four man teams as escape, evasion, concealment and survival is much easier in smaller numbers as opposed to company or battalion size infiltrations. This is another means of waging protracted attrition warfare in the offense and defence both. Also in the eventuality of incursion into depth areas mobilising local para-military and population as resistance and fighting in built up areas is also food for thought and doctrinal development. While this will stand good for the land warfare component the Air and Sea components will have to adopt a more conventional course of action. However, employing these components in support of unconventional warfare will be the ingenuity of military planners and the daredevil commitment of air and naval troops.

1)Cyber warfare: Active cyber operations that involve hacking into computers frequently use an intrusion model. Although the approach is not technically or tactically oriented, it could be utilised as an operational concept to help intrusions in cyber operations attain their strategic targets. In this paradigm, every stage—reconnaissance, early exploitation, creation of persistence, lateral manoeuvres, and collection-exfiltration-exploitation—offers the chance to infiltrate a target's system and spy on, influence, destroy, collect, or even launch an attack (Hooren, 2022).

In a web article Peter Suciu claims that the 5 nations conducting the most cyber attacks are most It is no secret

[4] William H McRaven.(1993). The Theory of Special Operations. Naval Post Graduate School. Monterey, California. Pg 2.
[5] William Dave Driver,Bruce. E. DeFeyter. (2008). The Theory of Unconventional Warfare: Win, Loose and Draw. Naval Post Graduate School. Monterey, California. Pg 2.
[6] Digital security involves protecting your online presence (data, identity, assets). At the same time, cyber security covers more ground, protecting entire networks, computer systems, and other digital components, and the data stored within from unauthorized access.
[7] Ibid.

that China, Russia, North Korea, Iran and United States. Unfortunately, the threat vector continues to get worse, and hacking is now a domain where a not-so-secret war is being waged (Suciu, 2022). According to the Associated Press, in 2011 an executive order was signed by President Obama to delineate the rules of engagement for military commanders in the context of cyber strikes. The executive order delineates the many domains of responsibility, particularly in instances where the acquisition of presidential authority is necessary for the execution of a cyber attack. (Kyzer, 2011). This further substantiates the dynamic nature of the military environment, wherein the domain of combat has expanded to include cyber operations, and the significance of cyber attacks as a growing aspect of military endeavours. The consensus among academics and defence officials is that cyber warfare will play a significant role in the future of the defence and intelligence community. It is widely recognised that the preservation of robust offensive and defensive capabilities is of utmost importance. (Kyzer, 2011).

Further, in the year 2011, a sequence of synchronised cyber-attacks was carried out by non-state actors from Syria who were aligned with the Assad regime. These assaults were aimed at opposition forces, both domestic and foreign, with the intention of bolstering the regime's stance in the Syrian civil conflict. These events served as a demonstration of the regime's support (Eidman, 2014). There is potential for establishing a cyber-militia by utilising the pre-existing knowledge and skills of individuals who are loyal to certain governments, organisations, or engaged in proxy cyber operations. For nearly two decades infamous hacker groups anonymous has operated worldwide. In the recent Russian invasion of Ukraine in February 2022 a Twitter account 'Anonymous' with 7.9 million followers declared a cyber war on Russia and its president Vladimir Putin (Huddleston, 2022). This clearly indicates that the use of 'hacktivist' has been used as a force multiplier to leverage existing cyber militias or proxy organisations to serve the needs unconventional cyber warfare.

An organised and systematic prolonged offensive cyber campaign through "spear phishing", deploying "botnet" to deny services and subverting the enemy supply chain by deploying civilian and trained military hackers in large numbers to attack "Internet, telecommunications networks, computer systems, as well as embedded processors and controllers and data" to deter and deny these services for military or other purposes is the suggested concept of cyber warfare. Also overloading the network by indiscriminately targeting many devices, services or users as possible. Further, swarming of conspiracies through all available mediums of social media to spread fast obstructing law enforcement in real time will give impetus to an uncontrollable tempo of incidents of a 'viral insurgency' that will challenge law enforcement and cyber capabilities. Sensationalism is also another strategy to heighten recruitment and cooperation of other transnational militant social media groups.

In light of above, developing cyber capability and capacity will not only facilitate offensive operations but will also act as a strong deterrence. Incapacitating communications through physical and cyber means will also be crucial in unbalancing the leadership at all alvels. In the meantime express R&D and breakthroughs in AI, quantum computing and 5G is very important as all cyber attacks in the future will likely be carried out by AI systems which will surpass any human and will be able to cause rapid multiple disruptions on a wider front than before. Parity of status or surpassing capability in this domain will be a decisive factor for smaller states as large numbers can be compensated by AI reducing the number of cyber bayonets' or operators. These are areas where clandestine support could be envisaged from other interested parties. This indicates that capacity building in this area among others should be a national priority.

V: CHALLENGERS FOR SRI LANKA

With the increase of cyber threats and for defensive or unconventional offensive purposes the availability of qualified and skilled personnel in the field of information and communications technology cyber security domain is paramount to deter, protect and respond to cyber threats and attacks. According to the Centre for Strategic and International Studies by 2022, the global cyber security workforce shortage has been projected to reach upwards of 1.8 million unfilled positions (James Andrew Lewis, 2019). Given the global skills gap Sri Lanka requires to expend much resources towards capacity building in all cyber education and infrastructure related areas to combat cyber related threats. In Sri Lanka to date there is more to be done to address the shortage of cyber security experts. This needs to begin by reforming ICT education polices and opportunities in Sri Lanka. This is the foremost challenge.

A. ICT Education in Sri Lanka.

After almost two decades of investments in ICT infrastructure and teacher training in Sri Lanka, ICT as a stand-alone subject to be tested through examinations is well-entrenched in the educational system. A total of 3,500 schools offer ICT as a subject at GCEO/L or 35% of public schools. Up to 5% of public schools offer ICT at GCE A/L. (Gamage, 2020).

1)Student Population: The total student population in the Island is 4,048,937 Out of the given student population of 4,048,937 a number of 652,331 students are within the ordinary level (O/L Cycle (Grd 10-11) and a number of 426,964 students are in the advanced level (A/L Cycle (Grd 12-13). (Statistics Branch of Ministry of Education of Sri Lanka, 2021).

2) Government School statistics: The government functions a total number of 10,146 schools in all 09 Provinces of Sri Lanka. The schools have been further categorised as National schools 396 in number and 9750 Provincial level schools. The Government schools have been further categorised into 4 types as given in the table:

Table 1: Schools by category.

Type	Category	No of Schools
1AB	Schools having Science Stream classes in Advanced Level	1,011
1C	Schools having Advanced Level classes Other than Science Stream	1,941
Type 2	School Having classes only up to Grade 11	3,226
Type 3	School Having classes up to Grade 5 or Grade 8	3,968

Table 2: Students by A/L stream.

Category	No of students	%
Bio Science	46,064	10.8
Physical Science	47,775	11.2
Arts	182,487	42.7
Commerce	92,695	21.7
Technology Other	46,354	10.9
Other	11,589	2.7
Total	**426,964**	

Table 3: ICT education opportunities.

Source of knowledge	Total (%)	Urban	Rural	Estate
Private training course	17.4	17.0	17.7	11.7
School/ University	60.7	59.2	60.9	74.4
Govt. training centers	6.9	5.8	7.2	5.8

In considering table 1,2, and 3 above it is clear by table 3 that capacity for ICT education is made available to students and the majority get their ICT knowledge through the government education systems. However, table 2 indicates that that there are more numbers of students in the arts and the commerce streams compared to the science and technology streams. The number of students being educated in the technology stream is 10.9 percent out of the total 426,964 advanced level student population in Sri Lanka resulting in a very marginal percentage of children being trained for higher education in the Science, Technology , Engineering and Medical disciplines (STEM).

This is further reflected in the number of university admissions. According to university grants commission total undergraduate admissions to the computer science stream in 2020 are 5,253 as a UGC intake and for external and distance education a number of 7,799 with 6,272 as postgraduate students totalling to only 19,324 enrolling to computer science education out of a total of 394,092 that enter university. (University Grants Commission , 2020). It is alarming to note that the graduate output for ICT in academic year 2020 is 1,175 from the UGC intake and 921 from post graduate institutes totalling only 2096 in an academic year (University Grants Commission , 2020).

B. Challenges to Digitizing Armed Forces in Sri Lanka.

The digitization of Armed Forces is a complex and challenging undertaking. It requires a significant investment of resources, time, and effort. There are a number of factors that can affect the feasibility of digitization, including the country's political, economic, and cultural context.

1).Political and bureaucratic hurdles: The Sri Lankan government is often slow to make decisions and implement new policies.

2).Economic constraints: Sri Lanka is a developing country with limited financial resources and this will be the major constraint. The cost of equipment, software, and satellite and other platforms will

3).Cultural and societal factors: There is some resistance to change such as lack of knowledge, lack of resources, leadership roles, employee resistance to change, negative mindset, and lack of motivation are some cultural barriers to change.

4).Security concerns and potential misuse: There are concerns that digitalization could be used to spy on citizens or to misuse military power.

5).Technical Challenges: Some of the technical challenges of digitizing army forces in Sri Lanka include (a) limited telecommunications infrastructure, which could make it

difficult to transmit and receive data, (b) increase the risk of cyberattacks and (c) Capacity building for training and education of military personnel.

6).Budgetary Constraints: The budgetary constraints of digitizing Armed Forces in Sri Lanka include, (a) the cost of new technologies and equipment, (b) the cost of training and education, (c) the cost of maintaining and upgrading digital systems.

IV.CONCLUSION

Unconventional/asymmetrical wars as a strategy will have effects at the strategic, operational and tactical levels forcing leaders to be simultaneously committed to internal and external security threats immaterial of where and how it is generated as all actions from recruitment, training, resourcing and funding will be covert and clandestine. The new type of adversary will fight in three domains which are the physical, psychological and the cyber or electronic domain in contrast to known conventional war. The strategy will be to employ a battalions of hackers to exploit the available social, financial, economic and security vulnerabilities. While guerrilla warfare with limited technology can outflank high-tech conventional forces on one hand and on the other hand a few individuals with latest technology and a rudimental terrorists cell can commit large scale regular forces for counter terrorism. The intention of covert and clandestine action is to influence conditions and create high casualty rates that will make your opposing force commit a large scale protracted military commitment. The armed forces strategic reforms will mainly be in the doctrinal domain and capacity building and equipping of troops specifically dedicated for unconventional/asymmetric warfare to fight a land battle while capacity building in the cyber domain as a force multiplier. Both, within the conceptual frame of relative superiority.

At the outset of the paper the author identified 'public will' as an instrument of power. Here public consensus and support is needed for three aspects; for recruitment, for necessary economic and military industrial mobilisation and in the event there is to be a resistance type of war that has to be waged para-military forces and public mobilisation becomes vital and decisive. To effectively address the conventional superiority of forces one must develop strategies to frustrate the adversary in the least possible cost to time and resources.

In conclusion developing Sri Lanka 's military and cyber capacity and capability will solely depend on the economic factor. The economic disparity with other developing countries dictates that "***Time"*** is what Sri Lanka needs to achieve military, cyber, nuclear (for peaceful purposes) and space capability. This is a long term idealist's reality.

V. RECOMMENDATIONS

The following are broadly recommended:

*1).*Re-organise Armed Forces to suit unconventional warfare concepts.

*2).*Develop doctrinal concepts from own war fighting experiences and from lessons learnt from LTTE strategy and tactics.

*3).*Establish Combat Service Support doctrine.

4).Digitizing Armed Forces. .Digitizing Armed Forces is a complex and challenging undertaking, which is essential for Sri Lanka's security.

i. Establish digital platforms.
ii. Secure strong political leadership to effect digital transformation.
iii. Develop a clear vision for digitization of the Armed Forces.
iv. Address technical challenges.
v. Managing budgetary constraints through phased out development.
vi. Build public support through awareness campaigns and consensus.
vii. Strengthening judicial oversight and introducing new legislature for cyber protection / individual privacy
viii. Special recruitment policy for ICT professional in to the Armed Forces on a market value pay scale.

REFERENCES

Bhat, M. (2022, 03 30). *South Asia Monitor* . Retrieved 07 03, 2023, from Big-power rivalry is becoming more intense in the Indian Ocean Region: https://www.southasiamonitor.org/perspective/big-power-rivalry-becoming-more-intense-indian-ocean-region

Bulathgama, T. (2023, 08 10). *Cyber Terrorism an Emerging Threat to Sri Lanka's National Security*. Retrieved 08 10, 2023, from https://www.defence.lk/upload/doc/Thusitha_Bulathgama_Cyber_Terrorism_an_Emerging_Threat_to.pdf: https://www.defence.lk/upload/doc/Thusitha_Bulathgama_Cyber_Terrorism_an_Emerging_Threat_to.pdf

Crisis 24 Sri Lanka Country Report. (2023, 06 05). Retrieved 06 29, 2023, from Crisis 24: https://crisis24.garda.com/insights-intelligence/intelligence/country-reports/sri-lanka

Department of Censors and Statistics . (2021, 12 31). *Annual Buletin Computer Literacy-2021*. Retrieved 8 30, 2023, from Department of Census and Statistics: http://www.statistics.gov.lk/Resource/en/ComputerLiteracy/Bulletins/AnnualBuletinComputerLiteracy-2021.pdf

Dias, G. (2022, 12 15). *Fortifying National Security in a time of Crisis*. Retrieved 06 29, 2023, from Ministry of Defence: https://www.defence.lk/Article/view_article/26954

Dobberstein, L. (2023, 5 23). *It's 2023 and Sri Lanka doesn't have a cyber security authority*. Retrieved 8 28, 2023, from The Register: https://www.theregister.com/2023/05/26/sri_lanka_cybersecurity_authority/#:~:text=Sri%20Lanka%20ranks%2081st%20out,the%20National%20Cyber%20Security%20Index.

ECONOMYNEXT. (2023, 7 20). *Sri Lanka to introduce long-delayed cybersecurity legislation*. Retrieved 8 28, 2023, from ECONOMYNEXT: https://economynext.com/sri-lanka-to-introduce-long-delayed-cybersecurity-legislation-in-2023-official-124009/

Eidman, C. R. (2014, 6). *Unconventional cyber warfare: cyber opportunities in unconventional warfare* . Retrieved 09 01, 2023, from Naval Postgraduate School Monterey California : https://core.ac.uk/download/pdf/36734834.pdf

Gamage, S. (2020, 11). *ICT in Education in Sri Lanka*. Retrieved 09 01, 2023, from Research Gate : https://www.researchgate.net/publication/343962901_ICT_in_Education_in_Sri_Lanka

Guy Schleffer, B. M. (2021). *The Political Effects of Social Media Platforms on Different Regime Types.* Retrieved 8 26, 2023, from Texas NAtional Security Review : https://tnsr.org/2021/07/the-political-effects-of-social-media-platforms-on-different-regime-types/

Hooren, J. v. (2022, 12). *The Integration of Special Forces in cyber operations* . Retrieved 9 1, 2023, from Nethrlands Ministry of Defence : https://nps.edu/documents/110773463/135759179/The+Integration+of+Special+Forces+in+Cyber+Operations.pdf/fafb3a1f-876d-e174-7294-4a8b5795fb77?t=1652136095474

Huddleston, T. (2022, 3 25). *What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia*. Retrieved 9 03, 2023, from CNCB: https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

James Andrew Lewis, W. C. (2019, 01 29). *The Cybersecurity Workforce Gap*. Retrieved 8 30, 2023, from Center for Srategic and International Studies : https://www.csis.org/analysis/cybersecurity-workforce-gap

Jayasuriya, R. (2017). The Influence of Global Islam Radicalisation to Sri Lanka. *International Research Conferance Articles KDU IRC 2017* (p. 8). Colombo: General Sir John Kotalawela Defense University .

Jayasuriya, R. (2023). Transnational Organised Crime and its impact on Sri Lanka. In S. D. Bhagya Senaratne, *"Sri Lanka's Post Independence Defence Policy: Past Present and Future Projections",*. Colombo: General Sir John Kotalawel Defense University.

Kyzer, L. (2011, 6 23). *Cyber War Rules of Engagement Being Crafted*. Retrieved 9 3, 2023, from https://news.clearancejobs.com/2011/06/23/cyber-war-rules-of-engagement-being-crafted/

Lim, A. (2023, 8 22). *An Executive View of Key Cybersecurity Trends and Challenges in 2023*. Retrieved 8 28, 2023, from ISACA: https://www.isaca.org/resources/news-and-trends/industry-news/2023/an-executive-view-of-key-cybersecurity-trends-and-challenges-in-2023

Qiao Liang, W. X. (2007). *Unrestricted Warfare.* Dehra Dun: Natraja Publishers.

Roles and Responsibilities of Cyber Security Professionals. (2023, 08 01). Retrieved 08 26, 2023, from

Simplilearn : https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article

Senaratne, B. (2010) Dynamics in Cybersecurity:Challenges to Sri Lanka's security . *General Sir John Kotelawala Defence University International Research Conference* (p. 7). colombo : General Sir John Kotelawala defence university.

Sri lanka Export Development Board . (2017, 5 12). *ICT Education in Sri Lanka* . Retrieved 8 30, 2023, from Export Development Board : https://www.srilankabusiness.com/blog/ict-education-in-sri-lanka.html

Statistics Branch of Ministry of Education of Sri Lanka. (2021, 12 31). *Annual School Census of Sri Lanka summary report 2021*. Retrieved 8 30, 2023, from Ministry of Education : https://moe.gov.lk/wp-content/uploads/2023/02/School_Census-2021_Summary-Tables-Final-Report1.pdf

Stepan, A. (2015). India, Sri Lanka, and the Majoritarian Danger. Journal of Democracy. *26* (01).

Suciu, P. (2022, 10 17). *The Not-So Secret Cyber War: 5 Nations Conducting the Most Cyberattacks*. Retrieved 9 3, 2023, from https://news.clearancejobs.com/2022/10/17/the-not-so-secret-cyber-war-5-nations-conducting-the-most-cyberattacks/

Threat Intelligence. (2023, 03 16). *Threat and Risk Assessment: What is it, Guides and Benefits*. Retrieved 08 11, 2023, from Threat Intelligence: https://www.threatintelligence.com/blog/threat-and-risk-assessment

University Grants Commission . (2020). *Sri Lanka University Statistics* . Retrieved 09 01, 2023, from University Grants Commission : https://www.ugc.ac.lk/downloads/statistics/stat_2020/Chapter%203.pdf

ACKNOWLEDGMENT

I acknowledge with thanks the guidance, instructions, and assistance by Dr Harendra Vidanage for this opportunity and Major General Milinda Peiris for making it possible. I would like to place on record my humble thanks to Dr Sanath De Silva for his continuous efforts to guide me during the process. I also thank Mr Pradeep Ranaweera who supported me in many ways and particularly the staff of the Faculty of Graduate Studies at the Kothalawela Defense University.

AUTHOR BIOGRAPHY

Major General Robin Jayasuriya RSP, ndc, psc, MScS&SS, MPhil is currently holding the appointment as the Rector of the Southern Campus of the General Sir John Kotalawela Defence University. He holds a Master of Philosophy in Defense and Strategic Studies from the Madras University, and a Masters degree in Security and Strategic Studies, Kothalawela Defence University. His research areas for higher studies have been in Conflict Resolution, Comparative Study of the LTTE and JVP and Collective Security Structures to Counter Violent Extremism and Terrorism in Sri Lanka and South Asia.