The introduction of sophisticated technologies and the pervasive use of internet has increased the numbers of international cyberattacks exponentially. Such ever increasing cyberattacks leave a trail of damage in many States. This article outlines the application of public international law to international cyberattacks as it has been revealed that no international instrument nor any decisions of international tribunals has directly addressed the three common breaches of international obligations vis a vis cyberattacks, ie use of force, due diligence obligations and non-intervention principle. With this gap in the law, States can only respond to cyberattacks based on what they perceive as legal and not based on an objective international standard. Since the nature of such cyberattacks differs vastly from the conventional attacks, application of conventional approaches to these three international obligations in such instances were found ineffective and inadequate. Referring to the success of the United Nations Convention on the Law of the Sea ("UNCLOS") in solving various types of international maritime disputes, this article suggests that the international community should seriously consider to adopt a binding international legal instrument like UNCLOS containing provisions on suggested national framework to tackle prospective cyberattacks, encouraging international co-operation and setting up of international tribunal to deal with cyberattacks. Such initiatives may promise the best use and application of various information and communication technologies for the betterment of humanity.

Keywords: Cyberattacks, use of force, due diligence, non-intervention,


INTRODUCTION

Cyberattacks ie the attack on computer networks of a different country by nation states or violent extremist groups has turned to be a serious concern in recent times and can be "... as destructive as the terrorist attack on 9/11." With continuous advancements in technology, the number of cyberattacks has gone exponentially high around the world. From the live cyberattack maps developed by different bodies, it can be seen that in every single second, computers of various countries are attacked in the millions.
The number of cyberattacks increased after the internet was made available for individual, general, public and commercial use. Perhaps the first major cyberattack was reported in 1988 when a computer program by the name of the ‘Morris worm’ crashed thousands of computers in the United States of America (USA), with effects akin to a contagious ‘biological infection’.\(^6\) In 2007, a Distributed Denial-of-Service (DDoS) cyberattack, allegedly perpetrated by Russia, targeted Estonia’s infrastructure, disabled all of the government websites, two major banks, several political parties, news systems, prominent Estonian universities, and the parliamentary email server.\(^7\) Just like most States, Estonia has been relying on the Internet for its critical infrastructure. The country also relied on electronic networks which are crucial in government operations, power grids, banking services and even Tallinn’s water supply.\(^8\)

Another notable attack was reported in 2010, where Iran’s nuclear program was disabled after its centrifuges spun out of control. This alleged attack was made by Stuxnet, a ‘worm’ that was likely tested by Americans and Israelis.\(^9\) Recently, cyberattacks by Russian intelligence were allegedly carried out against the 2016 American Presidential Election\(^10\) and the 2017 French Presidential Election.\(^11\) Further, the WannaCry cyberattack has affected more than 150 States, and it was deemed ‘the biggest ransomware attack ever’.\(^12\) Even within the developing world, in countries like Malaysia, at least 9,915 cyber-related incidents were reported in 2015 alone.\(^13\)

Cyberattacks can sever the economic, scientific and political lifeline of a State. More disturbingly, even technologically advanced States like the USA and France are vulnerable against the perils of cyberattacks, especially when the election of leader of the country now lies in the hands of cyber attackers. Since the consequences of cyberattacks are dire, ascertaining whether cyberattacks breach any international obligations is pertinent. As cyberattacks are relatively new occurrences, there is hardly any specific international law on this. Despite a litany of cyberattacks, none has been brought to any international court. Thus, States that are accused of cyberattacks from different corners were not held liable, nor has their actions been officially declared unlawful. There is still very limited scholarship and little consensus among scholars pertaining public international law and cyberattacks. In light of the increasing dangers of cyberattacks, it is high time to examine the effects and adequacy of applying public international law principles in cyberattacks.

With this aim in mind, this article is divided in nine parts, including introduction and conclusion. Though it is tough to define ‘cyberattacks’, an attempt will be made to define ‘cyberattacks’ for the purpose of this article. After that, some of the legal concerns in cyberattacks will be shared and the inadequacy of international law provisions in dealing with cyberattacks will be highlighted. The issue of use of force, due diligence and principle of non-intervention under public international law will be discussed and the extent to which these are applicable in case of cyberattacks will be evaluated. Linking the issue of cyberattacks with that of the UNCLOS, finally the need for framing binding international instrument in this regard will be suggested. This article tries to argue that though already various countries have taken many fragmented initiatives to fight cyberattacks, one single but comprehensive initiative under the auspices of the United Nations as it was done in case of UNCLOS may offer a better solution.

**CYBERATTACKS: DEFINITIONAL CHALLENGES**

Although cyberattacks bear serious consequences, there is a lack of internationally accepted definition of the term, which creates problems. According to Finland, ‘cyber’ is usually the prefix for a term, which relates to electronic information processing, information technology, electronic communications or information and computer systems.\(^14\)

The word ‘attack’ means a malicious activity to collect, disrupt, deny, expose, alter, disable, degrade, or destroy information systems or breach security policies with the objective to gain advantage or harm a third party. The USA has defined ‘attack’ as any malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.\(^15\) On the other hand, the International
Organisation of Standardisation (‘ISO’) has defined ‘attack’ as attempts to destroy, expose, alter, or disable an Information System and/or information within it or otherwise breach the security policy. Germany views this term as an intentional form of threat, namely an undesirable or unauthorised action with the objective to gain advantages or harm a third party respectively.

Hitherto, no state has adopted a definition on ‘cyberattack’. The closest definition emanates from the US Department of Defense's Dictionary of Military Terms, which defines ‘computer network attack’ as ‘Actions taken through the use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and networks themselves.’ This definition mirrors that of NATO Glossary of Terms and Definitions, but the latter added that a ‘computer network is a type of cyberattack.’ However, it does not define cyberattacks, and the word ‘cyber’ is only found in this reference of the entire document.

Scholars have tried to gauge the lack of definition by defining cyberattacks as ‘any action taken to undermine the functions of a computer network for a political or national security purpose’. The definition implies that any action, ie hacking, bombing, cutting, or infecting would qualify as cyberattacks if it disrupts the function of a computer network. Since this narrow definition hinges on the function of the computer network, neither cyber-espionage nor cyber-exploitation constitutes cyberattacks as they do not affect the function of the computer network, even if they compromised the computers’ security. This definition also emphasises the need for a political or national security purpose and consequently distinguishes cyberattacks from simple cybercrimes. The distinction is important because cyberattacks may breach public international law while cybercrimes do not. A cyberattack initiated by Kremlin Kids who shut down Georgian Internet during Russia’s invasion of South Ossetia invoke principles of state responsibility; whereas a cybercrime done by Onel de Guzman who infected millions of computer with a ‘love bug virus’ do not. ‘Cyberattacks’ is again defined as the ‘premeditated use of disruptive activities, or threat thereof, against computers and networks, with the intention to cause harm or the further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives’.

By construing these three definitions, cyberattacks may most accurately be described as disruptive actions taken against computers or computer networks with social, ideological, religious, political or similar purposes. Therefore, the elements of cyberattacks include: (a) intention; and (b) disruptive action towards computers or computer networks. This definition is not confined to only disrupting the functionality of computers, as some cyberattacks may only affect information, but not the computers’ function.

Cyberattacks can be of different types. The most common mechanism of cyberattacks is the ‘buffer overflow’ method, which overwrites the computers' memories and takeovers the computer system. Another type of cyberattack is the distributed denial-of-service (DDoS) cyberattack, whereby cyber attackers (ie botnets) gain unauthorised access to many computers to invoke a coordinated, large scale cyberattack against one or more targets.

**LEGAL ISSUES IN CYBERATTACKS**

Some obligations arise in cyberattacks and three international obligations namely, use of force, due diligence and the principle of non-intervention are very serious in such instances. These obligations fall under the umbrella of state sovereignty. It is axiomatic that all States enjoy sovereign equality, and can enjoy the rights inherent in full sovereignty. To preserve sovereignty, the States cannot invoke the use of force to infringe another State’s territorial sovereignty; due diligence must be performed by States to prevent harm to another State; and intervention to the affairs of another State is prohibited.

Although the concept of sovereignty was developed before the rise of cyberattacks, scholars opined that it could be applied to cyberattacks. If such application is denied, the States deploying cyberattacks will be free to cause severe economic and political harm to other States with no consequence, thus
diminishing sovereign equality. Therefore, it is pertinent to ascertain and apply international law to cyberattacks to preserve States’ sovereignty.

Regarding the three breaches of international obligations, cyberattacks invite us to ponder whether such acts constitute a use of force under the UN Charter. Clarifications on this provision can be found in the US Department of Defense Law of War Manual and various scholarly publications. About States’ due diligence obligations, the United Nations General Assembly (‘UNGA’) resolutions which encourage States to secure national infrastructure from misuse would be explored. Further, the principle of non-intervention would be discussed together with the Friendly Relations Declarations, the Declaration on the Inadmissibility of Intervention and Interference in the Domestic Affairs of States and the International Court of Justice (‘ICJ’) case of Corfu Channel.

PAUCITY OF INTERNATIONAL LAWS PERTAINING CYBERATTACKS

The sources of international law are international Conventions, custom, general principles of law recognised by civilised nations and subsidiary laws, ie publicists’ opinions and judicial decisions. In the absence of the former three laws on cyberattacks, subsidiary laws, state practice and soft law like the UNGA resolutions may be relied upon.

There is a breach of an international obligation by a State when an act of that State is not in conformity with what is required of it by that obligation, irrespective of its origin or character. It is submitted that cyberattacks breach international obligations when they are conducted by States to circumvent their international obligations.

The central problem with cyberattacks is the paucity of specific laws. A plain reading of article 2(4) of the Charter of the United Nations (‘UN Charter’) which provides that ‘All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations’ will preclude cyberattacks because so far no international law case has associated ‘force’ with cyberattacks. Nonetheless, state practice and scholars have linked article 2(4) and cyberattacks by analysing the physical effects produced, destruction to any national critical infrastructure and the nature of the computer program used.

Moving on, the due diligence principle stems from the Corfu Channel case, where it was held that ‘it is every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States’. Numerous scholars agree that this principle extends to cyberspace. However, the application of this principle differs in different contexts, ie when States have actual knowledge of cyberattacks, when States monitor or adopt preventive measures against cyberattacks or their response towards cyberattacks. Neither States nor scholars have agreed on a fixed due diligence standard for these different situations.

The non-intervention principle prohibits States from intervening in matters within the jurisdiction of another State, such as the economy and politics. As aforementioned, some cyberattacks cripple States economically or hold political sway; they may be unlawful. In the absence of treaties and custom relating to cyberattacks, only scholars have acknowledged the nexus between non-intervention and cyberattacks.

In the absence of any specific international law sources on cyberattacks, the initiatives taken by the North Atlantic Treaty Organisation’s (‘NATO’) deserve special attention. NATO in the 2002 Prague Summit and the 2006 Riga Summit has classified cyber defence as an important political agenda. The Lisbon Summit in 2010 enabled NATO to develop an in-depth NATO cyber defence policy called the Strategic Concept. Through the Chicago Summit in May 2012, NATO’s networks came under centralised protection, and technological upgrades were implemented. At the 2014 Wales Summit, NATO further refined its cyber defence policy to keep up with evolving cyber threats. In the 2016 Warsaw summit, NATO added