Heterogeneity in Cyber Warfare and Need of Legitimizing Cyber Defense: A Case for Introduction of Developed and Transnational Cyber Laws in Pakistan

Syed Muhammad Aala Imran Sherazi
Sherazi Law Associates; Superior Law College; Pakistan College of Law; Department of Law and Parliamentary Affairs, Government of the Punjab
email: syedmuhammadaala@sherazilaw.com;

Abstract

Technological innovations in cyberspace have outpaced legal development in the same area. The use of botnets is a prime example, where technologically poor and dependent states such as Pakistan are under an incessant clutch of malware, while the victims are not even aware. The international dome is the best place to begin the discussion, as it has developed its approach with the passage of time. The current approach in the international arena assists in understanding how the transnational element should be addressed. The domestic law of Pakistan currently applied can be considered and its vague interpretation and inefficiency are discussed. In the light of these discussions, the writing proposes some aspects which can be used and utilized in the future, as they guide how a balance between transnational aspects, and fundamental privacy rights can be brought.

Keywords: Botnets, Cyber law, Cybersecurity, Cyberattack, Cyberspace, International Law, Malware, Pakistan, Transnational Laws.

Introduction

Technological advancement has made a huge impact on the development of domestic and international law. The twenty-first century is full of innovations, technology, and information technology. It goes without saying that the speed of technological development has led to changes in laws, social norms, and approaches towards them. It is right that the speed with which technological advancements are being made is far more than the speed with which the laws are developing. The laws are in mayhem

and there is often hesitation as to the application of any law, apart from it being the right one. Cyberspace laws are not a new term but an area with more cracks than closures. In a continuously developing area of cyberspace, the development of law is either absent or is so haphazard, arbitrary, or debatable that it appears as if the system is lawless or wild-west.

This writing intends to highlight the heterogeneity and intricacy caused by technological advancement and the meagerness of laws in the field of technology law. Moreover, it also intends to shed light on the absence of effective and transnational law in Pakistan. This writing uses the idea and concept of botnets to exemplify the lacuna in Pakistan's domestic law, as well as international law. It also takes guidance and references from the US of America's jurisprudence in this area for better understanding.

When the term 'botnet' is used in Pakistan, almost no lawyer is mindful of what this means or indicates. However, when the impact of botnets is observed in Pakistan, be it reported or unreported, there is no doubt that the use of botnets and malware is common. The main reason is the ignorance of the population. Most of the population is illiterate, or unaware of the safe use of the internet. A link shared by a botnet infects all devices or malware them, without the knowledge of the user. A click to a free meal results in the cell being malware. Without the knowledge or will of the user, the device is conscripted, and used as a tool and weapon by the 'botmaster'. When the audience and victims are unaware of what they have been subject to, there is going to be no legislation and precautionary actions. State personnel are also majorly unaware of the concepts and technological features that are used and employed by botmasters. The botmaster directs the devices to further their own *malafide* actions. The devices are used for hacking, spamming, and committing financial scams, to name a few. The botmasters are not necessarily well-known and can be anyone with technical knowledge and proficiency in this technology field of cyberspace. The botmasters can operate distantly, that is why the operator can act extra-territorially. This leads to two important questions i.e., what should be the responsibility of the state in retribution to cyber-threats and cyber-attacks. Secondly, what do international law, state practice, and experience of developed states say about it? With reference to the earlier question, an argument is raised that domestic laws should be enacted to safeguard the interests of the citizens.

However, even if this argument is taken at its face value, and accepted that domestic law needs to be placed, the transnational or extra-territorial effect of such matters are most likely not enforceable under domestic law. Domestic laws including penal laws may be a good option, but it requires in-depth analysis, which this writer will attempt in the succeeding portion. On the other hand, it cannot go without saying that some technologically advanced states do have the power, intent, and motive behind using cyber-attacks and cyberspace as a mode of furthering their espionage, surveillance, and data collecting interests. This is one of the subsidiary reasons why international law has to be referred to in this writing, to substantiate the arguments and submissions. For example, the USA is often alleged to be involved in the use of cyberspace. This is also an allegation levied on the Five Eyes. Briefly, the Five Eyes is an intelligence alliance under the UKUSA Agreement, of which the UK, USA, Canada, New Zealand, and Australia are parties. Thus, it can be said that cyberspace is not something that is open for use or misuse by individuals or outlawed or banned organizations, but it is equally open for states to be employed for furthering their own vital and intentional interests. The case for the inadequacy of domestic law has some weight, which is because of the transnational or extra-territorial limitation of domestic legislation. If this matter has to be addressed, the states have to either become a party to a binding treaty, convention, or pact, which will further its interest or as an alternative, establish the state practice of customary international law in its favor. The international arena has its own inherent limitations regarding enforcement mechanisms. Furthermore, there is a unique element to consider in such a debate i.e., despite the situation where there are states versus states in cyber warfare or cyberspace, there is also an equivalent chance of violation of the privacy of cyber-human rights of individuals (Iñaki Navarrete, 2020). For example, privacy laws, breach of confidential data, use of devices without consent, etc. The reason such rights are involved is that they found their basis in the pre-cyberspace era. This is a novel area and hard to research on and formulate a coherent description and analysis, however, the USA, through its Department of Defense, has been a great source to research on anti-botnet technicalities. Interestingly, this has a link with surveillance attempts used by the USA. Hence, it may give good hindsight to the titled discussion. In the light of these factors,

and after discussing the international, technical and domestic aspects, this article will conclude as to whether there is a need to have a specific enforceable cyber law, as opposed to vague, absurd, theoretical, unenforceable, impractical, legally barred legislations? At the same time, in the larger interests of public, and in analogy with the concept of self-defense under UN Charter and customary international law, there is a need for all states, to have such laws which authorise the state to engage in activities and enforcement mechanism that are founded on the principle of *bonafide* or good faith doctrine. Such laws are better enforceable through those states that can be termed as 'cyber-capable states'. The phrase bona fide, in my opinion, is itself very subjective and vague under international law. However, it is also to be kept in mind that the procedural norms and scheme are necessary for carrying out the technological solutions as per the substantive values under domestic and international law. In this line, it is worth mentioning that the development of international law and practical importance of the laws is more efficient through adoption of concepts of *ergaomnes* or communal recognized state duties to unsettle cybercriminals and expanded cooperation between nations in botnet disruption. It is similar to the war against terrorism, which is a matter falling under universal jurisdiction.

In other words, cyberspace is full of legitimate and criminal actions; however, it remains in oblivion as what counts as legal and what is illegal. This uncertainty led to the asymmetrical development of law and conduct in the international arena. Moreover, the illegal actions by botmasters or individuals can only be controlled if the state that is affected by the actions has the indispensable capability. In the same vein, it also requires the legitimization of actions made by law enforcement agencies, which would otherwise be illegal. For example, surveillance of traffic, data alteration, and interferences, recording, and monitoring of private data is an area where state actions can be considered to be qualifications on the rights of individuals under international human rights as well as domestic law. This writing has made special reference to botnets because they are a unique and highly complex classification under Cyberspace law and technology. Ingredients to produce botnets are merely small finances and good IT skills. They are also operable from distance by any client, operator, individual, and organization, or even state. Botnets can also target their objects and implement them with

precision and detail. The damage, scope of the damage, target, specific or general are all options available to the botmaster.

Operation Through 'Botnets'

'Botnets' can be considered as a money-spinning tool for the commission of cybercrimes, through upsetting businesses, governments, and even customers (Home Affairs, 2012). They are devices that are distantly operated by botmasters, without knowledge of the owners of those devices. The operation through botnets is centered upon the control of the computer or other devices. This is done through 'bot binaries'. These are servers or devices of botmasters that distribute the malware to botnets and devices. This results in two points i.e., limiting the bot binaries and botmaster's location; and spread and amplification of infection.

How can an ordinary individual understand what botnet is, or how do they target? Among some common examples is phishing, spamming, links to use the malicious website, remote scanning, etc. When the 'bot binary' infects the device, it penetrates and alters its system in such a way that the ordinary functioning of the device is not affected. The importance of such penetration is that the owners are kept unaware and attempts to remove the virus are not made by owners. In addition to it, the botnets have a 'domain flux' wherein it constantly changes its domain, so that the botnet's network is inaccessible (Yu et al., 2014). Some use has been made of techniques to fingerprint or identify these botnets and binaries. These techniques are mostly focused upon the analysis of traffic data (Boukhtouta et al., 2013). Once the botnet binary infects the device and connects to its server, the IP address may be changed, as per the whims of the botmaster, because he can send updated binaries to the botnets and send commands or orders remotely (Hoang & Nguyen, 2018).

For example, distributed denial of service attack (DDoS), appropriation of privately-owned systems for cryptocurrency mining, phishing, spam emails are some of the cyberattacks (Furlan et al., 2012). Here, botnets contact the target server in a huge amount that exceeds the server's data processing capacity that results in a crash or non-operational of the server (Palla & Tayeb, 2021). It is important to discuss why these attacks are made? The reason may vary from mere harassment to revenge, and includes an intention to

highlight an issue, fraud at a huge scale (C., 2017), honeypot-aware botnets, advertising fraud, camera data theft, and extortion to cite a few (Leyden, 2018). The extent of harm can be outspread, for example, DDoS attack can cause a monetary loss in millions of dollars, to thousands of companies, corporations, and institutions (Deka & Bhattacharyya, 2016). It can also be repetitive and the scope of damages may even extend to loss of income, or loss of data of financial customers, in addition to the loss of reputation (Brickfield, 2019). The email-spams are something which we are facing most commonly. We all have spam emails in our accounts, why is this so? They contain malware and can infect the devices. Recent cases of botnets include data theft as well. There are botnets that steal or target the details and credentials related to finances such as credit card information. Similarly, there may be other botnets that may target and operate. This is capable of even inflicting the Electronic Voting Machines (EVMs) and rig elections (Saul & Heath, 2021). The state, its establishment as well as criminals can potentially use it for their political purposes.

In order to discuss the potential of electronic voting machines and other devices getting infected by it, reference can be made to the infamous Mirai botnet (Gerard, 2019b), which infected the internet of things ("IoT") and smart technologies (Zhang et al., 2020). When did the reader last time update or change its password? Or when did the reader work on the security settings of the devices? (Whittaker, n.d.). These inactions lead to potential vulnerabilities of the devices to cyberattacks and botnets. The Mirai botnets were created by teenagers and young lads, this is evidence of how easy it is to set up a botnet scheme, and conduct cyber activities (*Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybercrime Investigations*, 2018). This example also strengthens the proposition that a botnet or device made for recreational or targeted harassment may become a reason for a widespread criminal act of internet abuse by various botmasters (Barth, 2018). It is also possible that these botnets are varied, and then the updated and upgraded botnets start to invade (Goodin, 2017). The scheme of attack and objects may have no nexus between them (Evangelist et al., 2018). This is the reason that specialization in cyber technology and the command on the method of cyber-tool are more important than pondering about the creator of the botnet. The complexity and command of the cyber-attacker or botmaster

can be determined from the fact that if he or she intends, the DDoS signals may be kept below the breaking point of the targeted server. This will result in apparent no damage, and this technique can be used during cyber-defense. In such a situation, the cyber-defense analyst may keep the DDoS signals at the limit of the breaking point of the server, and in this way, the damage can be mitigated or even eliminated at all. This cyber defense mechanism can be achieved through the utilization of information security regulations, strong network structure, and obstacles in penetration of systems including black-holing DNS servers under influence of botmasters (Narayanan et al., 2020). The state of California has its own cybersecurity law with regards to IoTs and botnets, which is evidence that states may at their own level, take actions to mitigate the harm of botnets (Henry, 2018).

Understanding Cyber Space and Botnet Mitigation Laws in US

This section of the writing deals with the transnational and international effects of botnets. Under traditional law, the concept of territorial sovereignty had a literal interpretation; however, the introduction of technology and cyberspace gave a new dimension. For example, traditional warfare included ground, air, and water, which later on extended to space, and now, it includes cyberspace. With the inclusion of cyber-space, the traditional or classical concept has lost its significance.

The tools and methods devised above, are helpful in identifying the place or location of botmasters that can be identified within the territory or beyond the territorial jurisdiction (Fortinet, 2018). The origin of the attacks can be beyond jurisdiction. It is also possible that millions of devices from multiple states can cumulatively target a specific server. This is also an issue that has been faced numerous times at the international level. On the other hand, the state, the website, or the servers of which are targeted, have no obvious investigation right. For example, there is no agreement, MoU, contract, or understanding between Pakistan and any other nation, which is available in any official gazette, at the federal as well as provincial level, that entitles Pakistan to investigate such attacks. On the other hand, if the state is aware of any potential attack or intends to interfere with a DDoS or any botnet activity, it needs to have a transnational law or international agreement that allows such

explicit interference and intervention (Tapia, 2019). The rationale behind this is that intervention is done through interception of communication of DDoS, third parties, and Command and Control Centre of binary botnets. In order to identify, and interfere, trans-border actions may be required. This requires information sharing, cooperation, and legal assistance in investigation and trial (Margaret Jane Radin, 2016). Proposing a narrow interpretation of territorial sovereignty or strict application of the limitations on extraterritorial enforcement action, would not help the case. In this regard, there is a practical need to allow cyber-capable nations to intervene and invoke information-sharing agreements with nations. For example, in the USA, Congress passed the C.L.O.U.D. Act in 2018. Under this Act, the United States-based internet service providers are required to provide data on the request of USA law enforcement agencies, even if that data is stored extra-territorially (Houser, 2018).

When the extra-territorial issue is read along with international cooperation and mutual legal assistance rules, it appears that a treaty mechanism is a good option. However, it is important to point out that this treaty mechanism is slow and deliberate. For example, if a state intends to pass a request for cooperation and assistance to another state, the duration may even extend up to months or even years (Clark & et al., 2010). The CLOUD Act 2018 (US Code, n.d.) amended the Stored Communications Act 1986 (Wikipedia Contributors, 2019) to reduce such a period in America. However, like other principles, it has its own limitations. The example of the CLOUD Act is evidence of state practice; however, the international law is not well developed in this area, because international law requires a balance between protection of privacy law and adherence to the doctrine of sovereignty. Notwithstanding the above, it is also unclear how a legislation such as the CLOUD Act, or any other, in these lines, is capable of securing the internet. In other words, the CLOUD Act was specific legislation, and botnets are not specific to CLOUD, hence the scope of application of such legislation provides some guidance but not a holistically brilliant scheme. It is also pertinent to state that the world is no more unipolar, and the US is not the only technologically advanced state. So, if the US can have such a law, there may be Chinese, Russian, Malaysian, Indian, or similar other states that have the capability and may challenge the authority of the US legal system in the future. Hence, it can be

concluded that national law is one important aspect but needs to be in line and in consonance with international law. In absence of such law, guidance can be sought from treaties in the international arena and soft laws available (Waxman, 2017). In a single phrase, it is about assistance by the international community through the adoption of such norms, procedures, and laws that are helpful in technological advancement and acknowledge the technological capability of nations and authorise their interference.

States have been relatively new in responding to the threats of botnets and malware. The old players have been the corporations and private sector organizations, who developed the anti-botnet or botnet mitigation techniques. In the US, there is a public-private partnership, wherein the State has made the private corporations responsible to conduct actions on its behalf and protect its assets against cyberattacks, in an efficient way. However, the most important aspect in this regard is the transnational nature of cyberattacks. This includes the use of botnets and servers in the extraterritorial area i.e., cyberspace fails to adhere to the classical concept of territorial jurisdiction. The transnational aspect invites the application of international law, which is very uncertain to date. Under international law, the concept of state consent and practice adopted by them is important. On the other hand, it is also important to understand that the approach of any state depends upon its economic, social, and technological interests (Nye, 2016). If the cyber-interventions and cyber-attacks are to be restrained by a state which fails to counter cyberattacks, botnets, and associated malware, the states will propose the application of vague or inefficient laws, interpretations, and rights to constrain such interventions. On the other hand, if a state is technologically advanced and able to counter the cyberattacks and interferences, it will focus upon the scope of the cyberattacks, and actions made in cyber defense. The presence of such extremes has led to legal and non-legal documents that are aimed at streamlining the cyber-related utilities and legitimation of cyber defense mechanisms (Kello, 2021).

Under the basic international law, states joined minds and are generally of the view that responsive enforcement mechanisms are to be formulated and legitimized to criminalize the cyberattacks and infringements of privacy rights. This also led to an approach of international cooperation through data and information sharing, so

that the enforcement of cyber defense actions be open and disclosed (Rizov, 2018).

Before embarking upon the current scheme, a brief analysis of the evolution and case for the legitimization of the anti-botnet intervention can be presented. As soon as cyberspace was open for operation by criminals and foreign entities as a warfare method, the concept of sovereignty expanded to it (Menthe, 1998). As already provided, the initial or original attempts to defend the cyber defense were by the private entities as by the government, as they were the primary target of such activities. In other words, it was a private activity that later on got so expanded that it formed an extension to the world on public international law (Clark, 2015). Practical discussion and research pointed out that the history has been that people who were dealing or had to link with a specific industry used the insider knowledge and then used that knowledge for its detriment. This was why such criminal activity was dealt with by the private sector rather than by the government sector (Eichensehr, 2022).

In the second phase of development or evolution, reference can be made to seminal attempt of UCSB to take on a botnet, and mitigate its actions. They took over the botnet but in doing so they acted as governmental individuals as well as criminals. This impression is partly because of no direct concept of legalized cyber defense. The actions were primarily legal in my opinion, as they were aiming to get hold of the botnet and minimize the harm, and secure the data along with taking remedial actions. The counter to this assertion was that when they got hold of the botnet, they were going to be subject to criminal law. They can be an open target for criminals, cybercriminals as well as internet service providers, who may take adverse actions against them. In other words, they were not legally supported. They were involved in an activity that did not give them governmental support, backing, logistics, etc. for example, they were themselves in violation of privacy laws, including the Wiretap Act (US Code, n.d.-b) and traffic data laws as provided under the PATRIOT Act (US Code, n.d.-b). It goes without saying that such data has sensitive material including PIN code, bank account credentials, and credit card numbers which is also a violation of banking and computer fraud laws (US Code, n.d.-b). Similarly, Marcus Hutchins' attempt to counter MalwareTech (that caused WannaCry) (US Code, n.d.-c) by attacking private sector

organizations through denying access to networks unless they paid a ransom in bitcoin; adopted the blackhole technique (US Code, n.d.-d). However, he was prosecuted by F.B.I. the good actors, or heroes in this arena are still criminals unless the law legitimized cyber-defense actions (Pieters-James, 2017). This also led to a parallel approach by multinationals, wherein they demanded governmental authorization before taking down any botnet. For example, Microsoft has a thread of cases in these lines. It won its claim against Waledac botnet in federal court for violation of IP law (Worthen, 2018). A similar fate was achieved in its claim against ZeuS for IP violation (Meisner, 2012). This is a prime example of how the shift is taking place to allow corporations to sue on behalf of the government. But this also evidences a lacuna, perhaps a very huge one i.e., the court proceedings are expensive, time-consuming, and less beneficial as damages accrue in seconds (Karpiuk, 2021).

Lastly, the current regime is adopted from the inception of the extra-territorial nature of botnets attacks. This needed the government's input and role to legitimize it in the international arena. It is also because of the reason not everyone can afford the remedies available to Microsoft. Meanwhile when the private entities are using cyber defense for profit-making, then it is inevitable that they will not find a permanent solution otherwise, they will be out of their jobs. For example, if an antivirus is made for all viruses, then how will the production entity make its profit? This is the reason that the current scheme requires domestic legislation, domestic enforcement, international legislation, and international enforcement in this area. In the US, there is *H.A.C.C.S. Solution* for the legitimization of cyber defense actions (Karpiuk, 2021). It is an initiative by the U.S. Department of Defense. It is a state-enabled four-step procedure. The first step is locating botnet-conscripted networks. The second is fingerprinting them. Once this is done, the vulnerabilities known in the botnet will be used to insert Artificial Intelligence (AI) agents in it, also known as 'n-day'. This does the remedial and other actions as required. In my expression, it is more like hacking the hacker. Lastly, the neutralization process is implemented. It involves interference with systems and their data, which is potentially harmful to other neutral systems. So, this method can be used to allow cyber-capable states to engage in such activities even on the international stage. Hence, it is also an indication that governments

need to take control of the cyber-defense arena. Moreover, this is why public international law can include this matter.

Enforcement Issues

The practical issues outweigh the theoretical and jurisprudential talks. The theory is vague, absurd, and irrelevant if it is unable to evidence itself through practice. Similarly, even if the laws are valid, their enforceability is important for the efficiency of laws. In the current discussion, it is also pivotal, as the cyberspace arena has a large scope of discussion on the enforceability of laws. In other words, even if we have the laws, at domestic as well as the international arena, their enforceability remains doubtful. The more efficient system will be more easily enforceable and vice versa.

The lack of enforceability, or inefficient enforceability will be a tool and a pro for the criminals. But, does this mean that there is a need to have a sophisticated expert team of heroes who professionally provide cyber-defense, while being under the funds, and management of the government. The investment of public funds for the purpose of cyber security and cyber-defense is in need of time. As already provided that the government needs to take the laws, and its enforcement into its own hands, the reason is also founded in the argument that in the previous century, the criminals were a handful and the private entities could hire cyber-defense, but now, the tool of utilizing cyberspace is available to millions. The subjects of the attack are also ordinary citizens, and hence the responsibility to protect was best suited to the government.

The jurisdiction problem lies at the heart of the enforceability debate in transnational cyberspace laws. There are several questions in this field. For example, which law will apply, who will implement it, against whom it can be implemented, what can be done under such laws, and who will do what against whom under such laws. As territorial jurisdiction is a concept that cannot be applied in its traditional sense, the other modes of jurisdiction can be invoked, such as personal (if the culprit's nationality is known), effect, passive effect, prescriptive, adjudicative, and enforcement (Dodge, 2017). It is the last one that needs consideration under this heading as it discusses the state's power to prescribe and regulate activity over persons. It is also pertinent to mention here that Budapest Convention does attempt to harmonize domestic laws on cyberspace

to bring clarity in enforcement authority. On the other hand, the adjudicative jurisdiction deals with personal or national jurisdiction as it deals with the empowerment of the court to apply state's law to a person within its enforcement jurisdiction. At the basic level, the state can only exercise its laws within its territory, however, in transitional affairs, this is limited, only to the cases where the permissive rule is allowed (reference is made to Lotus case (Case Law, 1927) decided by the Permanent Court of International Justice or PCIJ). This is in line with the principles of territorial sovereignty and the doctrine of non-intervention. Under international law, consent is vital, as there is no sovereign with all states as its subjects. This is why Austin never considered international law as really a law. However, Austin's lectures were his own perspective of law, and need no detailed analysis here. But consent is required, as states cannot be compelled, at least theoretically, under international law, to act or refrain from action. Coming back to the topic, the concept of enforceability is crucial, and the concept of jurisdiction has been given more weight and broad interpretation than ever done. From the principles of the Lotus case, it can be concluded that international law's enforcement principles in the cyberspace arena will be that the jurisdiction lies with all those states whose victims and assets are involved. Moreover, the vast expansion of enforcement and jurisdiction concepts can equally mean that cyber defense is an erga omnes duty. Such an inference will mean that it will be analogous to terrorism. Although it is arguably justifiable that cyber-terrorism is equivalent to terrorism, it will include funding terrorist groups, or aiding them in their illegal actions.

The doctrine of sovereignty has been duly discussed so that the preceding and subsequent discussion does not fall on its back on major principles under international law. It is also due to the fact that the concept of territory in cyberspace is very unique and different from our traditional concept of sovereignty. Hence, from the above and preceding discussions, it can be concluded that although states may criminalize certain actions, they may not do so extra-territorially, unless permitted by international law (effects-based jurisdiction). So, the Lotus case helps us to establish that in order to make permission to such effect, there must be states negotiated mutual assistance treaties that establish new norms of conduct in cyberspace. In my view, Stigall (Stigall, 2016) was right to point out that issues such as counter-terrorism in ungoverned

spaces such as cyber law are better dealt with when outside actors including states having capabilities, are allowed to intervene in affairs in which weaker or incapable states are unable to do so. I would only like to add the element of bonafide on part of the intervening state (Stigall, 2016). This is one good way to increase or promote global security. In this model, capable states will bear the burden to not only secure their own domains and territory but also to minimize trans-border harm. The key to the success of such a model will always be information sharing (Brilingaitė et al., 2022).
Although reference has been made to the Lotus case, it seems highly unlikely that this principle can be applied in its strict form, the technical reasons prevail, for example, the matter of jurisdiction on data or digital packets, and those data packets that are sent from trans-border, or even the ones sent from trans-border but without knowledge of the owner of the device (Zetter, n.d.). This matter may complicate even further as the data packets may be in millions and maybe from various sovereign states, and the identity of the botmaster can be hidden through layers of VPNs or proxies (Slobin, 2016).

Breaking into the International Cyberspace Law

In the beginning, it can be stated, despite possible criticism of it being a sweeping statement, that international law forbids state-controlled botnet crimes and intentional omission to act against culprits. However, such a statement can be supported, at least to some extent, by the Council of Europe's Committee on Cybercrimes' guidance notes (Cybercrime Convention Committee, 2013), and Budapest Convention. From the latter, the criminal law is aimed to be harmonized in a way that there is a positive duty to act on the international community regarding botnets while acknowledging that some nations are better equipped than others. Hence, creating a sense of reciprocal obligations on individual states to contain transnational threats emerging from within their borders to prevent infringement of peace and safety of other states (Shackelford, 2016).
As already pointed out and concluded, the domestic laws are incapable of efficiently controlling transnational harm, it is still important to use them (Gold, 2008). Even if this argument is criticized, there is still life in it when dualist states are concerned.

They cannot implement an international treaty without enabling it through an Act or domesticating legislation. However, some guidance can be taken in this regard from the NATO and ENISA report (Gold, 2008), which stands for the proposition that competing legal regimes will complicate the study of botnets and cyber defense actions (Efthymiopoulos, 2019). So, at this stage, we have two implications i.e., one is legal and the other is practical. Legal issues arise because of differences in domestic laws, violation of privacy and surveillance laws, violation of human rights, failure of international cooperation, information sharing, and weak international customary rules. The practical issues revolve around the capabilities of states, advancement in technology, trans-border complexities, and potential harm to private property and devices (Efthymiopoulos, 2019). Lacking domestic law is also apparent from the argument that it fails to differentiate between good-faith researchers and bad faith criminals.

(a) *ICCPR and ECHR*

This makes a fair case to discuss international law and its importance in cyber security and botnet mitigation. First, it is important to understand constraints placed by international law, before discussing the permissive and legitimized cyber defense. The constraints, as can be guessed from the previous discussion, are human rights, surveillance laws, and privacy laws. UDHR (United Nations, 1948) is a political document but is a declaration of civil, political, social, and cultural rights. The legal document on the same includes ICCPR (ICCPR, 1966) and ICESCR. The privacy laws are civil rights and are dealt with under the ICCPR. International privacy laws discuss the foreign surveillance and interpretations of provisions of ICCPR. Although some may argue that privacy laws are not directly concerned with botnet mitigation, this writing disagrees and discusses it as a hindrance and constraint on cyber defense. The USA's stance in UNHRC in 2014 was that ICCPR did not have an extra-territorial effect (Milanovic, 2015); however, rights under ICCPR and its interpretation are considered to be an erga omnes duty, which is to be given effect within as well as the outside territory of a signatory state. With respect to the digital age, former Secretary-General of the ESIL (Deeks, 2008) viewed, though reluctantly, that ICCPR does apply extra-territorially with

respect to digital rights (da Costa, 2013). This reluctance but ultimate acceptance was followed in the U.N. General Assembly's resolution 'The Right to Privacy in the Digital Age'. Hence, interpreting the right to privacy enshrined under Article seventeen of the ICCPR to be available offline as well as online. This is now the official stance of the USA (da Costa, 2013). In the report cited in the preceding footnote of this article, it was also made known that the USA was conducting surveillance while being in violation of the ICCPR. The interpretation of Art. 17 of ICCPR requires assessment of the principle of legality i.e., an act taken in accordance with the state's domestic law. This is no more issue for Pakistan as the same is available in the Constitution of the Islamic Republic of Pakistan, 1973. Secondly, the act in violation of Article 17 shall be justifiable as being non-arbitrary (i.e., proportional and necessary). Nonarbitrary means that the act is necessary to achieve a legitimate aim, proportionate to the aim sought. This is also in line with the jurisprudence of Art. 8 of the European Commission on Human Rights (Djeffal, 2012). In *Weber and Saravia v. Germany*, the ECtHR (ECHR, 2020) held that the State's interference in the privacy of its national can be reasonable if it was proportional to the national security interests. Proportionality has vast jurisprudence and interpretation in International Human Right Laws. For Kaye, it is 'the least intrusive instrument amongst those which might achieve the desired result' (Silva Santos, 2020). The jurisprudence between the interpretation of the same rights in ICCPR and ECHR shall be the same or in line with each other, to ensure universal standards for human rights. Some cannot be more human than others. The ECtHR, in *Big Brother Watch and Others v. the United Kingdom* (Silva Santos, 2020), privacy rights test for the propriety of bulk surveillance was considered. It may be of some guidance to cite the nine elements or limbs of the principle of legality of legislation devised by the ECtHR. The limbs are that the statute describes offenses and their nature which may give rise to an interception order; defined categories of people liable to have their communications intercepted; limitation on the duration of interception; procedure for examination, use, and storage of data; precautions for communicating the data to third parties; circumstances under which data must be erased or destroyed; arrangements for supervising the implementation of secret surveillance; notification mechanisms and lastly, remedies under

national law. Kaye's 'least invasive' is to assess whether the degree of interference exceeds what the goal requires. Applying this to the proposition of botnets, it needs to be discerned if the anti-botnet actions are non-arbitrary i.e., specific targeted objective or least intrusive instrument (United Nations, 1948).

After ascertaining the constraints on the international cyber laws, it is pertinent to discuss what law does cyber law in the international arena demands (Delerue, 2020). It is proposed that the best way forward is to establish procedural norms that cognize the technological shortcomings of surveillance without hampering bonafide attempts by the global community or technologically advanced states. Procedural norms regulate the procedural protections imposed by the state by their intelligence. It does not offer substantive definitions of privacy activities and legitimacy of state interference in privacy. Some procedural norms include legality, limits on reasons to collect data, periodic review of surveillance authorization, limits on retention of data, preference for domestic actions, and neutral oversight bodies.

(b) *Convention on Cybercrime*

Perhaps the most important binding and important treaty in the international arena is the Council of Europe's Convention on Cybercrime or the Budapest Convention (Permana, 2021). This is the latest convention, as it came into force in the 21st Century. It is the creation of the Council of Europe, and not the European Union. Its ultimate aim is to 'harmonize domestic criminal law governing cyberspace within the community of nations and to promote mutual assistance in information sharing and investigative authority' (Permana, 2021). Currently, more than sixty states are party to it and are required to harmonize substantive and procedural laws in this area. The convention is key to ensuring the enactment of legislation establishing a procedural framework for mutual legal assistance with evidence, extradition, jurisdiction, and preservation of evidence. At one end is the ICCPR, which is a limitation and pro-privacy law, whereas Budapest Convention is the one representing the other end. This international instrument is the best guidance for the international community as well as states like Pakistan for future legislation. Another key feature is the fact that it deals directly with botnet mitigation through a permissive regime of traffic-data

sharing for communications between signatories. The importance of this conventions' adherence to privacy laws is apparent from the mechanism it provides. Briefly, it is focused upon viewing traffic data (unopened packets), as they interfere less with privacy interests than viewing the content does.

The international cooperation element is also pivotal to the Budapest Convention. It obligates the states party to it, to provide mutual assistance with respect to the criminal offences 'for which real time collection of traffic data would be available in a similar domestic case'. It is clearly noticeable by now, that the Budapest Convention is procedural in nature. The importance of this approach is that it guides technical experts to design effective and pro-privacy protection gadgets. The transnational issue causes citizens and people to feel insecure and lack of confidence, whereas the scheme devised under the Budapest Convention is important as it boosts confidence as to economic security of people, no one will feel jeopardization of interests.

Notwithstanding the above, the Budapest Convention provides certain online behaviors that are to be classified as criminal in nature. These include offenses against the confidentiality, integrity, and availability of computer data and systems, computer-related offenses, content-related offenses, and criminal copyright infringement. For the purpose of this article and in order to rebut an assertion mentioned above it can be stated that Budapest Convention does not explicitly provide for the botnets. However, this was in contemplation of the draftsmen of the Convention as they have used general and broad terms, which are so abstract that unforeseeable or technologically advanced crimes and tools can be interpreted or read into it (Budapest, 23.XI.2001, 2001). The Council of Europe's Cybercrime Convention Committee's guidance notes has been evidence of this fact (Cyber Crime Convention Committee, 2012). For example, in 2013, guidance notes on botnets were published. They referred to botnets as technology and suggested application of the Convention to it (Cyber, 2012). Hence, the Budapest Convention is the finest available model that can be and must be used by states like Pakistan to have laws that are in line with international law, and help in the technological advancement of the state while answering queries relating to transnational cyberattacks and widespread use of botnets and malware devices in Pakistan. It will also provide protection to the privacy of the people of Pakistan. Budapest

Convention puts a positive duty on states i.e., establishing a harmonious body of criminal law, as well as describing how this law prohibits a novel criminal enterprise, and lastly, imposing an obligation on signatory states to either enforce the law against known criminals or to permit participating states to exercise objective jurisdiction over them.

Case for Domestic Legislation in Pakistan

When a case is to be presented that cyberattacks are to be curtailed, the reasons are to be provided as well. One of the cases for having cybersecurity, cyber laws, and laws allowing cyber defense is that these laws will protect the privacy of citizens of the Islamic Republic of Pakistan. Another case is that such actions are a violation of the cyberspace and cyber territory of the State. Meanwhile, it is also a threat to the sovereignty as such attacks on the state's data storage means that the state's vital interests and confidential material may be open for auction on dark websites. However, does the Constitution allow such privacy rights to the citizen of the Republic? Even if this is the case, has the right been interpreted to include cyberspace in it. What is the role of ICCPR or international jurisprudence in the Constitution? Lastly, what else necessitates the development of such laws?

If the Constitution of the Islamic Republic of Pakistan, 1973 is given a reading, it can be seen that the citizens of the state are provided some fundamental rights. These rights are enshrined under Part II, Chapter I of the Constitution of the Islamic Republic of Pakistan, 1973 (Constitution of Pakistan, 1973). These fundamental rights are so important that under Article 8, it is provided that laws that are inconsistent with or in derogation of Fundamental Rights are to be void. It is pertinent to mention Article 8(2), which provides that the state shall not make any law that takes away or abridges the rights conferred under the Constitution. This is a double-edged knife; it can cut from both ends. If it is argued that the law on cyber security protects the privacy and that privacy is a constitutional right, then it can be counterargued that such laws are in fact infringement of privacy. However, the rebuttal of such an argument is apparent from the discussion in this document, which differentiates between infringements of privacy from the surveillance of the data traffic.

In addition to it, even if the laws are in violation of the Constitution, they can be made part of the First Schedule of the Constitution. Article 8(3)(b)(ii) of the Constitution provides that laws specified in the First Schedule are immune from the application of the general prohibition under Article 8 of the Constitution.

One unique prospect and attempt can be made to justify cyber defense under Article 9 of the Constitution. It provides for the security of a person. It is a term and provision that has been widely interpreted by the Apex Court of Pakistan (Shehla Zia v. WAPDA, 1994). It reads that 'no person shall be deprived of life or liberty save in accordance with law'. The case or argument is that when a DDoS attack and a server is down, is it not an infringement of the liberty of the people? Their access to a certain website, domain, or server forcefully stopped?

Under Article 14 of the Constitution of the Islamic Republic of Pakistan, 1973 it is provided that inviolability of dignity of man is a fundamental right. In plain words, it provides that the dignity of man and privacy of home shall be inviolable. Does the privacy of home extend to the privacy of websites, homepage, internet, and cyberspace? In my opinion, the right does extend and should be extended to cyberspace.

When a Pakistani domain is acquired, it is the asset and property of the owner, and in such circumstances, broad interpretation of fundamental rights attracts Article 23 of the Constitution, wherein it is the fundamental right of every citizen to acquire, hold and dispose of property in any part of Pakistan. The protection of those rights is envisaged under Art. 24 of the Constitution, which provides for protection of the property. When a cyberattack takes place, and appropriates the rights to the domain, or server. The cyber defence can be legitimized under Article 24 (3) of the Constitution. It provides that if any action is taken which is to prevent danger to life, property or public health, or which has been acquired by any unfair means, or in any manner, contrary to law; or is enemy property or if the law provides its management for a limited period, in the public interest. Hence, if these articles are interpreted, it is plausible that cyber defence is potentially legitimate.

It is pertinent to mention here there is no botnet case in Pakistan, and the matter has not appeared before the Court of law, in Pakistan. However, reference can be made to some case laws where the apex court discussed the concept of privacy in Pakistan. In recent and

seminal judgment of Justice *Qazi Faez Isa and others v The President of Pakistan and others,* 2021, the court stated that *'Surveillance was permitted in the limited area of anti-state or terrorist activities and that too under judicial and executive oversight. Outside such limited area, surveillance was constitutionally prohibited. Intelligence agencies did not enjoy a free hand in conducting surveillance but are subject to strict rules of compliance and oversight by the court.'* The interpretation of Article 14 has been done broadly by the court. It is not an absolute right but a qualified one. In the expression of the court, '*Privacy required that all information about a person was fundamentally his own, only for him to communicate or retain for himself…. Privacy attached to the person and not to the place where it was associated…Intrusion by the State into the sanctum of personal space, other than for a larger public purpose, was violative of the constitutional guarantees… Right to privacy was deeply intertwined with the right to life, right to personal liberty and right to dignity… Illegal and illegitimate surveillance, by both State and private actors, had the impact of intrusion into the private lives of citizens, not only violating their constitutional rights but also intruding on the very personhood, privacy and personal liberty of those surveilled…Surveillance had disparate impact, violating principles of non-discrimination and equality as enshrined in the Constitution…Illegally procured private information amassed by the agencies could be used to manipulate and blackmail people for promoting political agendas; this crippled human security and dismantled democracy, lowering it slowly into an abyss of totalitarianism*'. These comments by the court are double edged as the matter goes into turmoil. If these are adhered in their strict sense then the cyber-defence laws may be interpreted as ultra vires to the constitution. The Court joined Article 14 with Article 9, and viewed that it is a constitutional obligation on State authorities to protect the privacy and personal freedom of the citizens '*unless the law expressly authorised them to do otherwise in exceptional circumstances. In the absence of any law to the contrary, the rights to privacy and personal freedom became absolute and stood to protect the privacy and personal freedom of the citizen. No Government institution was to disclose the personal information of any citizen unless the law authorised the institution to do so. In the absence of any specific law, the umbrella of constitutional*

guarantees would come to cover and protect the citizen'. This is the way out of the turmoil. The balance has to be struck and cyber-defence actions are to be justified through legislation. The court held that the State functionary could only embark upon the investigation or collection of material about a citizen under (i) the authority of an enabling law, (ii) by a functionary designated under the law; and (iii) only for a justifiable cause or reason. These are the criteria which are established by the apex Court of Pakistan and can be used as guidance tool, while formulating law. Such law has to be assessed that it cannot be misused malafide by the state to collect personal information about its citizen, unless there was a just cause and legitimate purpose for doing so. Hence, in absence of the enabling law, and even in presence of the same, the vires and domains of the laws and the implementation of the same has to be robust and efficient. The limitation on the state, can be understood from the 'Marcel principle' (Court, 2016). The Marcel Principle encapsulates that '*where information of a personal or confidential nature is obtained or received in the exercise of a legal power or in furtherance of a public duty, the recipient will in general owe a duty to the person from whom it was received or to whom it relates not to use it for other purposes.'* Such principle and this duty are not absolute but qualified as well. When there is some action by the executive, wherein information has been '*obtained under statutory powers the duty of confidence owed on the Marcel principle cannot operate so as to prevent the person obtaining the information from disclosing it to those persons to whom the statutory provisions either require or authorise him to make disclosure*'.

More recently, the Honorable Lahore High Court explained the concept of liberty and privacy. It referred to the definition of privacy provided under the Merriam-Webster Dictionary (Eleventh Edition) and Black's Law Dictionary (Tenth Edition). It defined privacy, inter alia, as freedom from arbitrary or despotic control. It began with the historical development of the concept of privacy, referring to various religious texts including Bible, Holy Qur'an etc. It provided that right to privacy was originally for protection against arbitrary intrusion by the police but it has now developed into a general right of privacy and repose. It is also considered essential for democratic government because it fosters and encourages the moral autonomy of the citizen, as a central requirement of a democracy.

This judgment made reference to UDHR, ICCPR, Convention on Rights of Child (CRC), International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, European Convention on Human Rights, American Convention on Human Rights, Cairo Declaration on Human Rights in Islam; Arab Charter on Human Rights; African Commission on Human and People's Rights Declaration of Principles on Freedom of Expression in Africa; African Charter on the Rights and Welfare of the Child; Human Rights Declaration of the Association of Southeast Asian Nations; Asia-Pacific Economic Cooperation Privacy Framework; Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows; Council of Europe. Recommendation No. R (99) 5 for the protection of privacy on the Internet; and European Union Data Protection Directive (since replaced by the General Data Protection Regulation, 2018). His lordship provided detailed jurisprudence of UK, US, India and Pakistan regarding right to privacy. It also mentioned that the Global Internet Privacy Campaign postulates that the right to privacy has the following facets: (a) "Information privacy, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records; (b) Bodily privacy, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches; (c) Privacy of communications, which covers the security and privacy of mail, telephones, email and other forms of communication; and (d) Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

This leads to the end of the penultimate part of the substantive portion of this writing. The Constitutional provisions, and interpretation of the same, are helpful in making a case for introduction of legislation on cyber defence in Pakistan. The matter will fall within the competence of the Federal Government, and it is less likely that it shall overlap with other enactments. In addition to it, the current laws of PECA, 2016 (Parliament of Pakistan, 2016) are not well equipped to deal with advanced technologies around the

world. Even if the law is considered, albeit arguably, to be fit for use, there are more than enough evidence of inefficiency by officers. Prevention of Electronic Crimes Act, 2016 (PECA) extends to aliens if they are in Pakistan. This is in line with territorial sovereignty of Pakistan. Similarly, it is applicable extra-territorially to any act committed outside Pakistan by any person if the act constitutes an offence under PECA and affects a person, property, information system or data located in Pakistan. This may be arguably in line with the Budapest Convention. However, it needs further deliberation in subsequent analysis. Under section 2 of the Act, 'act' includes causing an act to be done by a person either directly or through an automated information system or automated mechanism or self-executing, adaptive or autonomous device and whether having temporary or permanent impact. In this way, bot binaries may be included in it, if the court understands. With regards to state's assets, or military sites, section 2 defines "critical infrastructure" as critical elements of infrastructure namely assets, facilities, systems, networks or processes the loss or compromise of which could result in, significant impact on national security, national defense, or the functioning of the state. However, major tasks include potential harm to the private and multinational companies. It appears from the perusal of the Act that it includes most of the cybercrimes, however, it has weak cyber defence provisions.

With reference to cyber defence actions, section 32 of PECA provides that service provider needs to retain its traffic data for a minimum period of one year in accordance with sections 5 and 6 of the Electronic Transactions Ordinance, 2002 (Khalid Zafar, 2002). Other than Cyber defence actions, the FIA may apply to court under section 33 for the warrant for search or seizure of data device or other articles that has been or may reasonably be required for the purpose of a criminal investigation or criminal proceedings which may be material as evidence. It is pertinent to mention that with reference to the privacy of the people, subsection (2) provides that in such cases where there is apprehension of destruction, alteration or loss of data, information system, data, device or other articles the officer shall immediately bring it into the notice of the Court. However, there is a provision which contradicts with the interpretation of the right to privacy under ICCPR, ECHR as well as Budapest Convention. This is section 34 that deals with disclosure of content data. Section 35(2) provides some protection to privacy

by striking balance between the opposing interests. It provides that the actions of the authority shall be with proportionality and shall take all precautions to maintain integrity and secrecy of the information system and data; and not disrupt or interfere with the integrity or running and operation of any information system or data that is not the subject of the offences. In addition to it, it also requires the officer to avoid disruption of the legitimate business operations and information system, programme or data not connected with the information system that is not the subject of the offences.

The cyber defence is not legitimized under the PECA. On the international cooperation, under Chapter VI, section 42 of PECA provides for extending cooperation to any foreign government for the purposes of investigations or proceedings concerning offences related to information systems, electronic communication or data or for the collection of evidence in electronic form relating to an offence or obtaining expeditious preservation and disclosure of data by means of an information system or real-time collection of data associated with specified communications or interception of data. Subsection (5) of section 42 is evidence of the need for harmonization, and an international document for Pakistan that can be used to ensure harmonization of criminal laws in this area in various states. Lastly, Chapter VI provides for preventive measures and this is the only provision for cyber defence. Under section 49, titled 'Computer emergency response teams', the government is empowered to constitute computer emergency response teams to respond to any threat against or attack on any critical infrastructure information systems or critical infrastructure data, or widespread attack on information systems in Pakistan. However, there is no notification on the same available to the public. Even if there was any, it is solely by the Government. How can private entities engage in it? Is Pakistan a good enough state to be called as cyber capable? Even in PECA, there is a need to have competent and trained judges, however, practical dilemmas are there. For example, FIA is the competent authority but practically insignificant as to its functions and duties. Similarly, under section 44, judges shall be specially trained on computer sciences, cyber forensics, electronic transactions and data protection. There is no provision that allows citizen protection from acts of government overreach. The cyber-defence and its scope are not adequately addressed by the laws of Pakistan. It has also failed to understand the concept that territory is

irrelevant on the internet highways. Installation of malware is a violation of our criminal code; but extraterritorial enforcement without prior notification and consent from the other state is also absent. Moreover, it fails to provide redress to thousands of private owners of the computers whose devices are knowingly hacked by botmasters.

Pakistan needs an update in cyber law because of the absence of laws that empower nations to act against extraterritorial threats, and in light of the transnational nature of botnets, nations must either act outside of the law or against it or they must simply hope that nations hosting criminal actors intervene. Similarly, recently EVM machines are aimed to be used in upcoming elections. However, if they are infected, it will also be a violation of many other fundamental rights. Hence, it may be concluded that such laws are in dire need of reform.

Conclusion and Recommendations

For Pakistan, it has to understand and recognize that it has to, along with other states, assume reciprocal obligations to contain transnational threats emerging within its borders. Under international law, no state is theoretically bound to do anything which it does not consent to. However, reality is different and we should not expect to live in fantasies. All states are sovereign and they need to consent that they will not do harm to other states, so that in return the other state also refrains or takes steps to ensure that no trans-border harm takes place. Even if it does so, it is to be accepted as a mutual threat, and to be dealt in accordance with the procedure and assistance. Hence, bargaining for it on equal and reciprocal values. While on the plane of practical reality, it has to be admitted that some are better than others while dealing with such issues. On the other hand, it has to be accepted that privacy laws are not absolute rights. They are qualified and, in such circumstances, if the content of data is not opened, they are not violated. The reference to Budapest Convention also made it clear that the development of customary international law is going to be in these lines, hence they need to be followed so that in future a better placed system is available at domestic level.

For Pakistan, there is no doubt that there is a positive obligation to ensure anti-botnet actions and mitigate botnet or cyberattacks. This

obligation is on the argument of customary international law. This is because such attacks infringe ICCPR's article seventeen (Abebe, 2011), that ensure protection of privacy rights, and the Constitution of Islamic Republic of Pakistan, 1973. There may be some criticism of interpretation of fundamental rights as provided under the constitution of Islamic Republic of Pakistan 1973, however, the reasoning in this writing may make a plausible case for broad interpretation. The state's responsibility contains a positive obligation to protect from cyberattack, to take appropriate and effective measures to investigate actions taken by third parties, and hold those responsible liable for it through adoption of deterring measures.

It has to be accepted that the method proposed in this writing has used or proposed adoption of the US model, and model in Europe, but it does not mean that this is the only possible solution. For example, the approach of Russia to cyberspace laws and norms is in opposition to that of the USA (UN, 2018). Similarly, Philippines and France have proposed adoption of their own norms in cyberspace. However, in my opinion, the best method and clearer picture is the one present in the Budapest Convention and USA's domestic legal system. They both focus upon information sharing and mutual assistance in investigations. The efficient element in the USA legal system is that it imposes a duty to combat cyberthreats within jurisdiction and allows cyber-capable entities to aid in case of transnational harm. Such a model can be alternatively described as 'if you cannot stop the thief, make him the sheriff'. The technological advancement is way speedy than the development of law, and international as well as domestic law need to pace up. Pakistan is way back in its jurisprudence and understanding. It is full of potential but less efficient in the cyber space arena. If the proposed method and ideology is accepted, and followed, the void in this area may be fulfilled and a positive law will be available for the equipped law enforcement agents. Hence, through the adherence to the proposed system, it is possible to provide people of Pakistan, a secure internet. The Federation of Pakistan, through its Majlis-e-Shoora (National Assembly and Senate) shall take this as an opportunity to reform the law, and fill the lacunas in it.

References

Abebe, A. M. (2011). Special Report—Human Rights in the Context of Disasters: The Special Session of the UN Human Rights Council on Haiti. *Journal of Human Rights*, *10*(1), 99–111. https://doi.org/10.1080/14754835.2011.549715

Barth, B. (2018, February 22). *FYI, the OMG Mirai botnet variant turns IoT devices into proxy servers*. SC Media. https://www.scmagazine.com/home/security-news/iot/fyi-the-omg-mirai-botnet-variant-turns-iot-devices-into-proxy-servers/

Boukhtouta, A., Lakhdari, N.-E., Mokhov, S. A., & Debbabi, M. (2013). Towards Fingerprinting Malicious Traffic. *Procedia Computer Science*, *19*, 548–555. https://doi.org/10.1016/j.procs.2013.06.073

Brickfield, A. S. (2019). *Columbia Journal of Transnational Law: Writing Prize in Comparative and International Law, Outstanding Note Award*; Columbia Journal of Transnational Law.

Brilingaitė, A., Bukauskas, L., Juozapavičius, A., & Kutka, E. (2022). Overcoming information-sharing challenges in cyber defence exercises. *Journal of Cybersecurity*, *8*(1), tyac001. https://doi.org/10.1093/cybsec/tyac001

Budapest, 23.XI.2001. (2001). *European Treaty Series -No. 185*. https://rm.coe.int/16800cce5b

C., O. (2017). Securing Cloud Server from DDOS Attack. *International Journal of Advance Engineering and Research Development*, *04*(5). https://doi.org/10.21090/ijaerd.rtde31

Case Law. (1927). *The Case of the S.S. Lotus, France v. Turkey, Judgment, 7 September 1927, Permanent Court of International Justice (PCIJ)*. Www.worldcourts.com. http://www.worldcourts.com/pcij/eng/decisions/1927.09.07_lotus.htm

Clark, P. (2015). Can the State Foster Food Sovereignty? Insights from the Case of Ecuador. *Journal of Agrarian Change*, *16*(2), 183–205. https://doi.org/10.1111/joac.12094

Constitution of Pakistan. (1973). *NATIONAL ASSEMBLY OF PAKISTAN*. https://na.gov.pk/uploads/documents/1549886415_632.pdf

Court, T. S. (2016). *R (on the application of Ingenious Media Holdings plc and another (Appellants) v Commissioners for Her Majesty's Revenue and Customs (Respondent) - The Supreme Court*. Www.supremecourt.uk. https://www.supremecourt.uk/cases/uksc-2015-0082.html

Cyber Crime Convention Committee. (2012). *Guidance Notes*. Cybercrime. https://www.coe.int/en/web/cybercrime/guidance-notes

Cybercrime Convention Committee. (2013). *T-CY Guidance Note #5 DDOS attacks*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e9c49

da Costa, K. (2013). Marko Milanovic, Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy. *Human Rights Law Review*, *13*(2), 417–420. https://doi.org/10.1093/hrlr/ngs041

Deeks, A. (2008). European Court of Human Rights Decision: Case of Saadi v. Italy. *International Legal Materials*, *47*(4), 542–577. https://doi.org/10.1017/s0020782900029466

Deka, R. K., & Bhattacharyya, D. K. (2016). Self-similarity based DDoS attack detection using Hurst parameter. *Security and Communication Networks*, *9*(17), 4468–4481. https://doi.org/10.1002/sec.1639

Delerue, F. (2020). *The Threshold of Cyber Warfare: from Use of Cyber Force to Cyber Armed Attack* (F. Delerue, Ed.). Cambridge University Press; Cambridge University Press. https://www.cambridge.org/core/books/abs/cyber-

operations-and-international-law/threshold-of-cyber-warfare-from-use-of-cyber-force-to-cyber-armed-attack/18EED20277D22CAE25E71F63A27C8009

Djeffal, C. (2012). Law of the European Convention on Human Rights Cases and Materials on the European Convention on Human Rights The European Convention on Human Rights. *Archiv Des Völkerrechts*, *50*(1), 106–109. https://doi.org/10.1628/000389212800961146

Dodge, W. S. (2017). Jurisdiction in the Fourth Restatement of Foreign Relations Law. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2972612

ECHR. (2020). *HUDOC - European Court of Human Rights*. Coe.int. https://hudoc.echr.coe.int/fre#

Efthymiopoulos, M. P. (2019). A cyber-security framework for development, defense and innovation at NATO. *Journal of Innovation and Entrepreneurship*, *8*(1). https://doi.org/10.1186/s13731-019-0105-z

Eichensehr, K. E. (2022). Not Illegal: The SolarWinds Incident and International Law. *European Journal of International Law*. https://doi.org/10.1093/ejil/chac060

Evangelist, D. H.-W. S., F5February 15, & 2018. (2018, February 15). *The Mirai Botnet Is Attacking Again…*. Dark Reading. https://www.darkreading.com/partner-perspectives/f5/the-mirai-botnet-is-attacking-again/a/d-id/1331031

Fortinet. (2018). Fortinet Threat Landscape Report. *Computer Fraud & Security*, *2018*(6), 4. https://doi.org/10.1016/s1361-3723(18)30050-2

Furlan, B., Gächter, M., Krebs, B., & Oberhofer, H. (2012). Democratization and Real Exchange Rates. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2102067

Gerard, G. (2019a). Botnet Mitigation and International Law. *Columbia Journal of Transnational Law*, *58*, 189.

https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjtl58&div=7&id=&page=

Gerard, G. (2019b). Botnet Mitigation and International Law. *Columbia Journal of Transnational Law*, *58*, 189. https://heinonline.org/HOL/LandingPage?handle=hein.journals/cjtl58&div=7&id=&page=

Gold, S. (2008). Cyberdefence moves to the top of the Council of Europe/NATO agenda. *Infosecurity*, *5*(3), 6. https://doi.org/10.1016/s1754-4548(08)70030-5

Goodin, D. (2017, October 27). *Assessing the threat the Reaper botnet poses to the Internet—what we know now*. Ars Technica. https://arstechnica.com/information-technology/2017/10/assessing-the-threat-the-reaper-botnet-poses-to-the-internet-what-we-know-now

Hackers' Cooperation with FBI Leads to Substantial Assistance in Other Complex Cybercrime Investigations. (2018, September 18). Www.justice.gov. https://www.justice.gov/usao-ak/pr/hackers-cooperation-fbi-leads-substantial-assistance-other-complex-cybercrime

Henry, S. (2018). Oxford Scholarship Online. *Notes*, *74*(3), 480–484. https://doi.org/10.1353/not.2018.0027

Hoang, X., & Nguyen, Q. (2018). Botnet Detection Based On Machine Learning Techniques Using DNS Query Data. *Future Internet*, *10*(5), 43. https://doi.org/10.3390/fi10050043

Home Affairs, D.-G. for M. and. (2012, February 4). *Tackling crime in our digital age: Establishing a European cybercrime centre | Digital Watch Observatory*. Https://Ec.europa.eu/Transparency/Documents-Register/Detail?Ref=COM(2012)140&Lang=En; https://dig.watch/resource/tackling-crime-our-digital-age-establishing-european-cybercrime-centre.

Houser, K. (2018, March 26). *Everything you need to know about the CLOUD Act*. Futurism. https://futurism.com/everything-need-know-cloud-act

ICCPR. (1966). *International Covenant on Civil and Political Rights (ICCPR) Equality and Human Rights Commission*. Www.equalityhumanrights.com. https://www.equalityhumanrights.com/en/our-human-rights-work/monitoring-and-promoting-un-treaties/international-covenant-civil-and#:~:text=ICCPR%20is%20an%20international%20human

Iñaki Navarrete, R. B. (2020, September 24). *Cyber Espionage*. 10.1093/OBO/9780199796953-0212; https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0212.xml.

Karpiuk, M. (2021). The obligations of public entities within the national cybersecurity system. *Cybersecurity and Law*, *4*(2), 57–72. https://doi.org/10.35467/cal/133971

Kello, L. (2021). Cyber legalism: why it fails and what to do about it. *Journal of Cybersecurity*, *7*(1). https://doi.org/10.1093/cybsec/tyab014

Khalid Zafar. (2002). *Electronic Transaction Ordinance, 2002*. Khalid Zafar & Associates. https://khalidzafar.com/laws-of-pakistan/electronic-transaction-ordinance-2002/#:~:text=The%20Electronic%20Transactions%20Ordinance%2C%202002

Leyden, J. (2018, June 2). *OMG, that's downright Wicked: Botnet authors twist corpse of Mirai into new threats*. Www.theregister.com. https://www.theregister.com/2018/06/01/mirai_respun_in_new_botnets/

Margaret Jane Radin. (2016, December 9). *Microsoft Corp. v. United States*. Harvardlawreview.org.

https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/

Meisner, J. (2012, March 25). *Microsoft and Financial Services Industry Leaders Target Cybercriminal Operations from Zeus Botnets*. The Official Microsoft Blog. https://blogs.microsoft.com/blog/2012/03/25/microsoft-and-financial-services-industry-leaders-target-cybercriminal-operations-from-zeus-botnets/

Menthe, D. C. (1998). Jurisdiction in Cyberspace: A Theory of International Spaces. *Undefined*. https://www.semanticscholar.org/paper/Jurisdiction-in-Cyberspace%3A-A-Theory-of-Spaces-Menthe/8fa907cd2400e9e63a149ba81a7ac272af1712be

Milanovic, M. (2015). *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*. *56*(1). https://www.ilsa.org/Jessup/Jessup16/Batch%202/MilanovicPrivacy.pdf

Narayanan, N. N., Kumar, A., Sukumaran, K., & Leena, A. P. (2020). An Ayurvedic Protocol to Manage Retinitis Pigmentosa - A Case Report. *International Journal of Current Research and Review*, *12*(13), 25–32. https://doi.org/10.31782/ijcrr.2020.12135

Nye, J. (2016). Deterrence and Dissuasion in Cyberspace. *Journal of Cyber Policy*, *1*(2), 44–71. https://doi.org/10.1162/ISEC_a_00266

Palla, T. G., & Tayeb, S. (2021). Intelligent Mirai Malware Detection for IoT Nodes. *Electronics*, *10*(11), 1241. https://doi.org/10.3390/electronics10111241

Parliament of Pakistan. (2016). *[AS PASSED BY THE MAJLIS-E-SHOORA (PARLIAMENT)] A BILL to make provisions for prevention of electronic crimes.* https://na.gov.pk/uploads/documents/1470910659_707.pdf

Permana, W. P. N. (2021). Reviewing Information and Electronic Transaction Act from a Convention on Cybercrime of 2001. *Journal Hukum Novelty, 12*(2), 267. https://doi.org/10.26555/novelty.v12i2.a17679

Pieters-James, L. (2017). Does your Cyber Security make you WannaCry? *Journal of Forensic Sciences & Criminal Investigation*, *5*(3). https://doi.org/10.19080/jfsci.2017.05.555663

Rizov, V. (2018). Information Sharing for Cyber Threats. *Information & Security: An International Journal*, *39*(1), 43–50. https://doi.org/10.11610/isij.3904

Saul, B., & Heath, K. (2021). Cyber terrorism and use of the internet for terrorist purposes. *Research Handbook on International Law and Cyberspace*, 205–230. https://www.elgaronline.com/view/edcoll/9781789904246/9781789904246.00020.xml

Shackelford, S. (2016). The Law of Cyber Peace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2805061

Shehla Zia v. WAPDA. (1994). *Ms. Shehla Zia v. WAPDA, PLD 1994 SC 693*. ESCR-Net. https://www.escr-net.org/caselaw/2015/ms-shehla-zia-v-wapda-pld-1994-sc-693#:~:text=Ms.-

Silva Santos, E. C. A. da. (2020). The Internet and Cancellation Culture: The Impact of the Public Opinion on the Exercise of the Individual Right to Freedom of Expression. *Annals of Bioethics & Clinical Applications*, *4*(1). https://doi.org/10.23880/abca-16000169

Slobin, C. G., Sarah. (2016, October 5). *Where your data flows on the internet matters, and you have no control over it*. Quartz. https://qz.com/741166/where-your-data-flows-on-the-internet-matters-and-you-have-no-control-over-it/

Stigall, D. E. (2016). Counterterrorism, Ungoverned Spaces, and the Role of International Law. *SAIS Review of International*

Affairs, *36*(1), 47–60. https://doi.org/10.1353/sais.2016.0011

Tapia, C. T. B., Alan Charles Raul, Snezhana Stadnik. (2019, August 5). *New York Enacts Stricter Data Cybersecurity Laws*. Data Matters Privacy Blog. https://datamatters.sidley.com/new-york-enacts-stricter-data-cybersecurity-laws/

UN. (2018, November 15). *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased*. Council on Foreign Relations. https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased

United Nations. (1948, December 10). *Universal Declaration of Human Rights*. United Nations. https://www.un.org/en/about-us/universal-declaration-of-human-rights

US Code. (n.d.-a). *18 U.S. Code § 2703 - Required disclosure of customer communications or records*. LII / Legal Information Institute; Legal Information Institute. https://www.law.cornell.edu/uscode/text/18/2703

US Code. (n.d.-b). *GovInfo*. Www.govinfo.gov. Retrieved December 8, 2022, from https://www.govinfo.gov/app/details/USCODE-2011-title18/USCODE-2011-title18-partI-chap119-sec2511

Waxman, M. (2017, March 22). *International Law and Deterring Cyber-Attacks*. Lawfare. https://www.lawfareblog.com/international-law-and-deterring-cyber-attacks

Whittaker, Z. (n.d.). *Fear the Reaper? Experts reassess the botnet's size and firepower*. ZDNet. Retrieved April 28, 2021, from https://www.zdnet.com/article/reaper-botnet-experts-reassess-size-and-firepower/

Wikipedia Contributors. (2019, April 27). *Stored Communications Act*. Wikipedia; Wikimedia Foundation. https://en.wikipedia.org/wiki/Stored_Communications_Act

Worthen, N. W. and B. (2018). *Microsoft Battles Cyber Criminals*. WSJ. https://www.wsj.com/articles/SB10001424052748704240004575086523786147014

Yu, B., Smith, L., & Threefoot, M. (2014). Semi-supervised Time Series Modeling for Real-Time Flux Domain Detection on Passive DNS Traffic. *Machine Learning and Data Mining in Pattern Recognition*, 258–271. https://doi.org/10.1007/978-3-319-08979-9_20

Zetter, K. (n.d.). *Bredolab Bot Herder Gets 4 Years for 30 Million Infections*. Wired. Retrieved December 8, 2022, from https://www.wired.com/2012/05/bredolab-botmaster-sentenced/

Zhang, X., Upton, O., Beebe, N. L., & Choo, K.-K. R. (2020). IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers. *Forensic Science International: Digital Investigation*, *32*, 300926. https://doi.org/10.1016/j.fsidi.2020.300926