Journal of Law & Social Studies (JLSS)
Volume 5, Issue 1, pp 12-20
www.advancelrf.org

Legal Analysis of the Pakistan's National Cyber Security Policy in the Context of Cyber Warfare

Muhammad Asif Khan
Department of Law,
National University of Science and Technology Islamabad, Pakistan.
Email: ursasifkhan@yahoo.co.uk

Abstract

The application of international law in context of activities within cyberspace raises questions of diverse nature. This includes intervention in critical infrastructure of a state defying principle of non-intervention. The incidents of cyber espionage also raise multiple questions regarding the application of international law. Currently, states should bring forward their policies regarding the issues faced in cyberspace in context of actions which might amount to cyber warfare. Pakistan's cyber security policy is also in a begging state of clarity on different issues. With a readiness to improve its cyber defense system, Pakistan also requires bringing forward its policy and stance regarding the application of international law in context of cyber warfare. By taking a stance of terming cyber-attacks against its critical infrastructure as an act of aggression in its National Security Policy (2021), it has opened a plethora of questions regarding the applicability of international law in this context. It thereby needs to clarify its stance regarding the nature of cyber-attacks, attribution, dispute settlement and questions related with state sovereignty in context of cyberspace.

Keywords: Cyber Warfare, International Law and Cyber Warfare, Cyber Warfare and Pakistan, Principle of Non-intervention, Cyber Espionage.

Introduction

Cyberspace represents an important domain of human activity, and it has profoundly emerged as an indispensable feature of modern life. Nowadays, all actors within the international system rely upon cyberspace to conduct their activities and maximize their potential. At the same time, cyberspace can be 'used for purposes that are inconsistent with international peace and security'. Indeed, the threat landscape in cyberspace is multifaceted and dynamic, ranging from espionage, sabotage, theft and crime, social engineering, hacktivism, and subversion to cyber warfare. States may get involved in cyber espionage and intelligence gathering to cyber-attacks against the norms of international law. In addition, there are other threats attached with the use of cyberspace by distant individuals. In most cases these individuals evade legal responsibilities for their actions. There are potential criminals who use cyberspace as a tool for their malpractices. The actions might include selling of illegal objects through dark webs or getting private information through illegal means. Different state actors and non-state actors including organizations providing internet access tend to evade this threat through different means of countermeasures. The object of these countermeasure is to prevent these illegal measures through different software's, this is in accordance with penal requirements endorsed through the implementing of the Budapest Cybercrime Convention, or through participation in the

UNODC supported workgroup on preventing and combatting cybercrime. Different governments are introducing national laws to retaliate the criminals through a 'hack back' procedure in cases of violations of these laws.

With a multidimensional use of cyberspace, the legal difficulties to control and regulate these activities also become contentious. Some special laws have emerged to control these actions at national level, but with a common cyberspace these actions or their effects can easily become transnational. Transnational activities create ample questions regarding the legality and jurisdiction at the international level. In most cases the actions would come under the ambit of internal security measures, and in some cases, they may amount to warfare, now commonly known as cyber warfare. In this context the application of law where multiple actors are involved in activities related with conflict conducted from different territorial jurisdictions has always been contentious. Traditionally, the law was considered inapplicable in cases of armed conflicts. This drawback has been dealt with recently to include intrusions through cyberspace under the legal domain. The 2013 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security [GGE] affirmed that international law including the United Nations (UN) Charter along with other norms of international law for the protection of state sovereignty directly apply to cyberspace.

In furtherance to this the GGE reports (2015 and 2021) reaffirm the application of international law to cyberspace. In addition, NATO have also emphasized that in cases of violations of international law using cyberspace the relevant law will apply accruing state responsibility. As far as the application of law within the cyberspace is concerned, it always must neglect the technical aspects of the actions within cyberspace but concentrate on the physical involvement to control the contribution of objects, persons, spaces, relations, or their effects. Jack Goldsmith establishes that the involvement of the physical actors (mostly persons and corporations) can be regulated by the states keeping in view the established principles of state jurisdiction. Having said this, the use of cyberspace in almost every realm of life makes the identification of applicable law difficult and contentious. Intrusions through cyberspace can easily convert from a simple criminal activity to an international crime.

This research does not focus on the overall aspects of cyber security but identify the challenges created while applying international law in cases of infringements. Considering the application of international law in cyber warfare the policy of the government of Pakistan in this regard is examined. It is highlighted that the lack of clarity regarding cyber-attacks in the context of cyber warfare in Pakistan's National Security Policy leaves unanswered questions. The ambiguity adds to an already lack of consensus about the legality (or illegality) of the use of cyberspace in the context of cyber warfare.

Cyber Security in Pakistan

Cyber Security Issues for Pakistan

National security has always been a challenging issue for Pakistan. The unsettled and ongoing border issues with its neighbor India (in the east) has remained a focal point of security since its inception. In addition, the security problems within Afghanistan and active engagements with non-state armed groups in the last two decades have deepened the complexities of security issues for Pakistan. In addition, its ranking in the cyber security index is also not very promising. Keeping in view the changing dimensions of the regional and global security the situation is alarming for Pakistan. Pakistan, as most of the states, is vulnerable to cyber security threats including cyber espionage, cyber-crime, hacktivism, and cyber warfare. In this backdrop a National Cyber Security Policy (NCSP) was approved by the Pakistan's government in July 2021. The policy aims to use the relevant technological machinery for the socio-economic development of the country. The policy provides that this objective can only be achieved through providing more safety in the use of cyberspace and assuring the protection of the critical

infrastructure and information system. In addition, making the cyberspace within Pakistan safe for both internal and external users. In short, the purpose of the Pakistan's NCSP is to provide security to all public and private cyberspace users in Pakistan. In this article we will discuss the efficacy of Pakistan's cyber security system and its shortcomings in context of applicable international law.

Cyberspace is a broad term and includes all the actions conducted electronically which includes transnational actions carried out by the cyberspace users. In such cases asserting sovereignty over cyberspace by a state becomes problematic. Keeping in view the concept of sovereignty developed in international law, states can establish its sovereignty by establishing its jurisdiction over actions taking place in cyberspace within its territory. In addition, states may also establish jurisdiction over its citizens and nationals residing within its territory as well as non-nationals within its territory. Jurisdiction may also be established upon nationals of a state residing outside its territory, this is a state prerogative under the principles of active or passive nationality principles in international law. Through asserting jurisdiction by passive personality principle, the actions amounting to cyber terrorism may be dealt with by states. Applying the territorial principle of jurisdiction any information which is received or sent through the cyberspace from the territory of a state can be regulated by that state. In addition, if some web addresses are registered within a state, it can assert its jurisdiction based on this fact as its laws can be applied because of the origin of registration. The adoption of these principles is a state prerogative through its national criminal laws and states may differ in their approach.

The readiness against cyber-attacks through a robust cyber security and cyber defense system have two aspects i.e. the technical aspect and legal readiness. A detailed analysis of the technical aspects is beyond the scope of this research, as we focus more on the readiness through law and policy measures. Pakistan have adopted different criminal laws to enforce its sovereignty and prevention of crimes. The notion of sovereignty is defined generally within the constitution through article 2(A). The concept of active personality is observed through criminal law which extends to actions of citizens outside the territory of Pakistan. Pakistan had not adopted the approach of a passive personality principle through its criminal laws till 2016. Through the Prevention of Electronic Crimes Act 2016 (PECA) a passive personality principle is applied. Hence, according to other criminal laws (specifically Pakistan Penal Code 1869) a Pakistani national committing an act which is against the criminal laws of Pakistan can be prosecuted within Pakistan. However, a criminal action by a non-citizen against a Pakistani citizen committed abroad cannot be prosecuted in Pakistan. However, according to article 1(4) of PECA "It shall also apply to any act committed outside Pakistan by any person if the act constitutes an offence under this act and affects a person, property, information system, or data located in Pakistan."

The change in approach towards establishing jurisdiction in context of cybersecurity is not surprising, especially in context of cyber terrorism where passive personality principle has been adopted by different states. Other than the PECA there were a few legislations adopted for control of cyber-crimes, but PECA have subsided the other special laws. In context of issues relevant with cyber warfare we can now gauge the status and approach of Pakistan and then analyze the cyber security policy accordingly. Situations that may threaten international peace and security may be dealt with by applying public international law and enforced through state legislations. Let us now consider how the Pakistan's domestic laws deal with issues of non-intervention and espionage.

Applying the Principle of Non-Intervention

The prohibition of intervention is widely accepted throughout international law in both customary international law and treaties. It has also gained wide acceptance in the international community and has been reaffirmed multiple times in different international contexts. The ambiguity with regard to non-intervention exist in cases where intervention takes place through cyberspace, however states have done little to clarify the contents of the norm. In this scenario non-intervention may become

irrelevant in the coming decades, unless states do more to adapt non-intervention to emerging forms of interference enabled by cyberspace and new technologies.

The ambiguity in applying the principle of non-intervention in actions related with cyberspace arise because of the nature of actions possible through new technologies. Any state-sponsored cyber operation against the domestic or foreign affairs of another state has challenged the efficacy, relevancy, and clarity of the principle on non-intervention. A cyber operation against another state is possible through a cyber-attack, digital election interference, and deep fakes, and use of social media tools for negative propaganda. To establish that a cyber operation is against the principle of non-intervention it must be proved that the action(s) was coercive and against a protected state prerogative (*domaine réservé)*. Looking into the type of cyber operations, the two constitutive elements of non-intervention i.e. coercion and *domaine réservé*, are becoming increasingly difficult to apply in the context of cyber operations.

The claim of sovereignty over its territory is specifically mentioned within the constitution of Pakistan. The jurisdiction of the Pakistan's government is established within its territory i.e., its land, sea and airspace. Although it is not mentioned in any domestic law or the constitution that the jurisdiction also extends to its cyberspace, but we may infer from PECA that the government intends to establish a complete sovereignty over its cyberspace. The jurisdiction established within the act based on passive personality principle refer towards the criminalization of acts from outside the state, including any kind of interventions. The relevant articles of PECA are articles 3 to 9. Article 3-9 can be used for multiple purposes and refer to different forms of cybercrimes. Any interference within the information system – which may include public and private electronic databases – by any person (and assumingly a group of persons) from outside Pakistan can be investigated and punished accordingly. In cases where it is deemed that the person or group of people are directly linked with a government of another state the principle of non-intervention can be applied.

However, the act does not refer to or identify the consequences in such circumstances. Moreover, the burden of attribution to a state if it is allegedly involved in such intervention is on the victim state. The Prevention of Electronic Crimes Investigation Rules 2018 (PECIR) which clarifies the investigation procedure do not refer to any cases or forms of investigation where a state may be involved. Article 3 - 9 can therefore be used as a yardstick to identify an intervention. The qualification of such intervention if attributed to a state can then be analyzed by identifying whether the intervention was coercive in nature and against critical government infrastructure (*domaine reserve*) to claim that it defied principle of non-intervention. Additionally, the critical government infrastructure needs to be identified to know whether a target-based approach is adopted, or a consequences-based approach is adopted by Pakistan. Article 10 prescribes that any act of Cyber Terrorism if attributed to a state can be taken as against the principle of non-intervention.

Cyber Espionage in Pakistan

The use of cyberspace for espionage has recently increased and pointed as a matter of concern by different states. Incidents such as the Edward Snowden's disclosure of certain classified documents in 2013 raise several important and novel questions concerning the legality of cyber espionage under international law. Cyberspace has become a heaven for persons involved in spying because of several reasons. First, There is a lot of confidential information stored on cyberspace which is of potential interest for people involved in espionage. Second, the identification of intruder is a hectic task in cyberspace as it is termed as an anonymous domain. Third, in cases where the identity of the intruders is uncovered, the jurisdiction of states is limited in applying its laws upon the intruders, this makes espionage a risk-free task in cyberspace.

Espionage in Pakistan is conventionally dealt through the official secrets act 1923 (OSA). The act is mostly used in military trials against people accused of espionage. The act does not mention any information gained through cyberspace or through an act of hacktivism but a broad interpretation of sub clause 2 may include any actions within the cyberspace. Other then OSA the articles of PECA (especially article 6-8) might also apply to acts of espionage. However, the punishment for espionage under the OSA is capital punishment (including death penalty), whereas the punishment mentioned for actions under article 6,7 and 8 in PECA are imprisonment up to 3, 5 and 7 years respectively. The intention of PECA to include espionage as one of the crimes seems limited. However, any act of cyber espionage from within or outside Pakistan can be considered as a crime under PECA. The next question arises if an act of cyber espionage may be considered as an attack against Pakistan? Keeping in view the international law and the approach of Pakistan through its national legislations, the answer to this question will be in negative.

International Law Cyberspace and Pakistan's Policy

So far, rules of international law on the use of force and the conduct of hostilities in the context of cyberspace have not specifically been dealt with in the cyber security policy presented by the Pakistan government. The PECA (as referred to above) refer to the defensive use of cyberspace in context of 'hybrid warfare'. The National Security Policy 2022 (NSP) also highlights the importance of defense in "Hybrid Warfare" in the context of spreading misinformation or information against the state's interest. The term 'Hybrid Warfare' is referred to the interference in the information systems to degrade and target the national security by promoting anti-state information. It is specifically mentioned in the NCSP to implement the PECA to deal with the interference within the information systems. It also clarifies Pakistan's concern for establishing an active cyber defense system. The cyber defense system will be enabled and supported to provide a defense mechanism for all internet-based services. More importantly the policy identifies the importance of defending the governments infrastructure including the national critical information structure.

In addition, Pakistan will develop a response mechanism for cybercrimes having effect within its territory. The actions (laws and policies) within the purview of hybrid warfare are enforced within the national jurisdiction of a state, whereby a state must respond to and confirm allegiance to its international responsibilities (especially its human rights responsibilities) when drafting and enforcing such legislations and policies. The question of compliance by Pakistan with its international responsibilities in this matter is beyond the scope of this research. Below, it will be pointed out how Pakistan's national laws and the security policies - in context of cyber warfare - comply or contradict with the norms of international law.

Act of Agression in Cyberspace

In context of cyber warfare the NCSP also focusses on deterrence in cases of attacks on critical infrastructure or the critical information infrastructure. It declares that a cyberattack on any critical infrastructure or critical information infrastructure will be considered as an "act of aggression" against national sovereignty and all necessary and retaliatory steps will be taken. This statement clearly refer to article 51 of the UN Charter and claims to invoke the right of self-defence in cases of cyber-attacks against its critical infrastructure and critical information infrastructure. This particularly means that NCSP places cyber-attacks at par with an armed attack and is linked to its national security strategy. This policy step is probably taken because of the lack of advanced cyber defence system in Pakistan. The reliance against a cyber-attack is henceforth referred to through "necessary and retaliatory steps" which may include steps outside cyber defence and through using a more conventional armed force. This statement requires further explanation. In the absence of any clarification by the government and any effective legislation clarifying an attack on critical infrastructure and critical information infrastructure the reliance to explain this statement will be based on the principles of international law, whereby the

act of aggression is well defined in context of *jus ad bellum* and the consequences-based approach to the cyber-attacks in context of armed conflicts is well accepted.

Further, the act of aggression is referred to as an armed attack by the UN General Assembly Resolution 3314 (XXIX). According to the UNGA resolution the act of aggression is accepted as an armed attack or using the consequences-based approach in context of cyber warfare it may amount to an attack the consequences of which is similar to that of an armed attack. The approach adopted in the NCSP is similar to that of a target-based approach. This approach apparently seems flawed as a cyber-attack on a critical infrastructure or critical information infrastructure may be against the principle of non-intervention but cannot be termed as an act of aggression unless it leads to consequences similar to that of an armed attack. Hence, the right of self-defence may not be invoked unless the cyber-attack is accepted as an armed attack by the UN Security council.

Relying on the approach of the state cyber security policies it may also be argued that the dispute settlement related with cyber-attacks be carried out through peaceful means. In addition, while considering a cyber-attack as an act of aggression the attribution of the attack to a state is of immense importance. Currently, the burden of attribution of the attacks is on the victim state. Collaboration with other states in this regard is of immense importance. Although, it is mentioned within the NCSP that Pakistan will seek collaboration with other state to improve cyber security, it should step forward and call for an international body in order to;

- Provide technical assistance in attribution of cyber-attacks; and
- Peaceful settlement of disputes among states through mediation and arbitration.

Application of the Law of Armed Conflicts

Pakistan does not appear to have enacted any domestic legislation specifically implementing rules of International Humanitarian Law (IHL) applicable in cyber warfare. IHL does not apply to cyber operations taking place, and cyber-crimes committed, outside armed conflicts, and such non-military activities are subject to other areas of law, including domestic criminal and administrative law. However, IHL applies to cyber operations conducted in context of an armed conflicts, as far as the consequences of such operations are comparable with those of conventional operations. In particular, the principles of distinction and proportionality must be complied with, and precautionary measures must be taken to avoid or reduce the causing of harm to civilian persons or objects. With no example of cyber operations during an armed conflict the debate is mostly academic. There is no consensus on how to incorporate IHL in context of cyber warfare through national legislations. The ICRC may take a lead in this regard and draft a model legislation with consensus to assist the states to adopt more specific laws to counter cyber-attacks during armed conflicts.

Awareness about the application of IHL during armed conflicts is the sole responsibility of states. Pakistan is no exception and under a responsibility to equip its military forces and public and private institutions in general with necessary training and information to avoid intentional or unintentional transgress of IHL during conflict situation. Along with the state responsibility the ICRC may co-operate with state institutions to create awareness about the application of IHL in context of cyber warfare, in addition, to enhance an academic debate to foster local acceptance. In Pakistan, no awareness campaign has taken place to enhance an academic debate or assist the government institutions to adopt laws relevant with application of IHL through national laws.

Recommendations

In view of the above discussion, the following recommendations are presented:

1. State Practise (policies) for actions in cyberspace violating principle of non-intervention must be clarified to develop this principle and avoid declaration of actions in cyberspace as acts of aggression.

2. State laws regarding espionage must be updated to include instances in cyberspace. Pakistan needs to clarify its stance by updating PECA and Official Secrets Act 1923.

3. A Cyber Attack resulting in damage to the critical infrastructure and critical information infrastructure should be mentioned separately in PECA with a punishment amounting from seven years to life imprisonment.

4. Pakistan needs to declare the recognition of its cyberspace as a similar domain to land, air and sea.

5. State cooperation and technical assistance in cases of attribution of cyber-attacks is important. Pakistan should improve its technical capability to investigate any cyber-attacks against it, additionally it should focus more on state cooperation in such cases.

6. Settlement of disputes arising because of actions in cyberspace must be in peaceful manner. Declaring a cyber-attack as an act of aggression should be on case-to-case basis i.e., when an act fulfils specific criteria of being an act of aggression according to International Law.

7. A "model law" is required to be adopted by states to deal with application of IHL in instances of cyber-attacks during conflicts.

References

Arrest Warrant Case (Democratic Republic of Congo v Belgium) (Joint Separate Opinion of Judges Higgins, Kooijmans and Buergenthal) [2002] ICJ Rep 3, para 47; Restatement of the Law Third, The Foreign Relations Law of the United States (1986) para 402.

Corfu Channel Case (United Kingdom v. Albania); Assessment of Compensation, 15 XII 49, International Court of Justice (ICJ), 15 December 1949, 35.; UN General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, 24 October 1970, A/RES/2625(XXV) para. 3; Case Concerning Military and Paramilitary Activities In and Against Nicaragua (Nicaragua v. United States of America); Merits, International Court of Justice (ICJ), 27 June 1986, paras. 202, 205, 251.

Council of Europe, 'Convention on Cybercrime 2001' (2001) < https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185> accessed 23 May 2022.

David R Johnson and David G Post, 'Law and borders: The Rise of Law in Cyberspace' (1996) 48 Stanford Law Review 1367; Jack L Goldsmith, 'Against cyber anarchy' (1998) 65 University of Chicago Law Review 1199 <https://chicagounbound.uchicago.edu/uclrev/vol65/iss4/2/> accessed 26 April 2022.

Ewen Macaskill and Gabriel Dance, 'NSA Files: Decoded: What the Revelations Mean for You' (The Guardian, 1 November 2013) <https://www.theguardian.com/us-news/the-nsa-files> accessed 12 May 2022.

Jack L Goldsmith, 'Against cyber anarchy' (1998) 65 University of Chicago Law Review 1199.

James Lewis, Senior Vice President at the Centre for Strategic and International Studies, quoted in David P Fidler, 'Tinker, Tailor, Soldier, Duqu, 'Why Cyberespionage is More Dangerous than You Think' (2012) 5 International Journal of Critical Infrastructure Protection 28, 29.

Kubo Mačák, Laurent Gisel and Tilman Rodenhauser, 'Cyber Attacks against Hospitals and the Covid-19 Pandemic: How Strong Are International Law Protections?' (Just Security, 27 March 2020) <https://www.justsecurity.org/69407/cyber-attacks-against-hospitals-and-the-covid-19-pandemic-how-strong-are-international-law-protections/> accessed 2 July 2022.

NATO, 'Wales Summit Declaration' (5 September 2014) paras 72 and 73 <https://www.nato.int/cps/en/natohq/officialtexts112964.htm> accessed 16 June 2022.

'National Cyber Security Policy 2021' (Ministry Of Information Technology & Telecommunication, July 2021) < https://moitt.gov.pk/SiteImage/Misc/files/National%20Cyber%20Security%20Policy%202021%20Final.pdf> accessed 24 May 2022.

National Security Division, 'The National Security Policy of Pakistan' (2022) <https://static.theprint.in/wp-content/uploads/2022/01/NSP.pdf> accessed 18 June 2022.

Netherlands Ministry of Defence, 'The Defence Cyber Strategy' (2012) 4, <https://www.itu.int/en/ITUD/ Cybersecurity/Documents/National Strategies Repository/Netherlands2012NDL-Cyber StrategyEng.pdf> accessed 2 June 2022.

Nicole Hong, 'Silk Road Creator Found Guilty of Cybercrimes' (2015) Wall Street Journal <https://www.wsj.com/articles/silk-road-creator-found -guilty-of-cybercrimes-1423083107> accessed 17 May 2022.

Nicholas Tsagourias, 'Electoral Cyber Interference, Self-Determination And The Principle of Non-Intervention' (6 August 2019) EJIL: Talk! < https://www.ejiltalk.org/electoral-cyber-interference-self-determination-and-the-principle-of-non-intervention -in-cyberspace/> accessed 21 May 2022.

Nottenbohm Case (Lichtenstein v Guatemala) [1955] ICJ Rep 4, para 23: Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI: EU: C: 2014: 317, paras 32–41.

Oona Hathaway, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817.

Pakistan Penal Code,1860

Pakistan ranked 74th in Cyber Security index and 148th in ICT development index in the world by the Global Security Index 2020 Report (National Cyber Security Index Report) <at https://ncsi.ega.ee/country/pk/.> accessed 20 April 2022.

Peter Sommer, 'Police Powersto Hack: Current UK law' (2012) 18 Computer and Telecommunications Law Review 165.

Pete Warren, 'State-sponsored Cyber Espionage Projects Now Prevalent', (The Guardian, 30 August 2012) <http://www.theguardian.com/technology/2012/aug/30/state-sponsored-cyber-espionage-prevalent> accessed 30 June 2022. Prevention of Corruption Act, 1947.

Prevention of Cyber Crimes Act, 2016

R v Sheppard & Amor [2010] EWCA Crim 65; Sean Kanuck, 'Sovereign discourse on cyberconflict under international law' (2010) 88 Texas Law Review 1571, 1573–5.

'Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security', UN Doc A/76/135 (14 July 2021) para. 71(b).

Robert Chesney and Danielle Citron, 'Deepfakes and the New Disinformation War' (Foreign Affairs, January 2019) < https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> accessed 16 May 2022.

Russell Buchan and Iñaki Navarrete, Cyber Espionage (2020) Oxford Bibliographies, https://www.oxfordbibliographies.com/view/document/obo-9780199796953/obo-9780199796953-0212.xml.

Sean Watts, 'International Law and Proposed U.S. Response to the D.N.C Hack' (Just Security, 14 October 2016) <https://www.justsecurity.org/33558/international-law-proposed-u-s-responses-d-n-c-hack/> accessed 25 June 2022.

UN Secretary-General, Foreword, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/68/98 (24June 2013) 6.

UNGA 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (UN Doc A/68/98, 24 June 2013) paras 19–20.

US v Bin Laden, 92 F.Supp.2d.189 221 (S.D.N.Y., 13 March 2000).