DEFINING CYBER WARFARE

Khawaja Dawood Tariq[*]

Abstract

Technological advancement is always a disruptive process; its impact on society, economics, politics, military and strategic affairs are profound but it takes a certain amount of time before the effects are visible. Cyberspace has been termed as the battlefield of the 21st century. It is considered the most potent threat to international security. With the speed of technological advancement, its wide-ranging affects, and its potential weaponization, a comprehensive study to reconcile the international legal paradigm and cyber warfare is warranted. This article is a discourse analysis to examine the unique nature of cyberspace, the taxonomy and role of cyber operations in the modern-day strategic sphere, and how international law interprets different kind of cyber operations.

Keywords: Cyberwar, International Law, South Asia, Use of force, Cyberspace, Cyber policy

Introduction

It was in the aftermath of First Gulf War in 1991 that prompted John Arquilla and David Ronfeldt of Rand cooperation to declare that 'cyber war is coming'.[1] Since then cyber warfare have been transformed into a sub discipline of security and strategic studies. There has been numerous research studies trying to explain what cyber warfare is, but like any other concept in strategic studies, the core components of cyber warfare remain highly contested. The speed of technological advancement, its wide ranging effects, and its potential weaponization is of serious concern to academics, and strategists alike.

Multiple terminologies can be used to define highly complex, technical, and sophisticated functions that are associated with cyberspace. These terminologies include, cyber war, cyber-attacks, cyber operations, information warfare, and so on. As there is an absence of disciplinary consensus, we start with the commonly accepted and simplest definition. A Cyber-attack is an act of coercion, involving attack on computer network. After this, there is no consensus on what constitutes cyber-attacks and cyber warfare.

[*]Mr. Khawaja Dawood Tariq M. Phil in Strategic Studies, and bachelor from LSE in International Relations. I was a Senior Research Associate at Strategic Vision Institute. I taught International Relations at Metropolitan International University College. I served as a Development Fellow at Planning Commission, Ministry of Planning, Development & Special Initiative. Presently, I am serving in Ministry of Defence.

The central objective of this research is to define what cyber warfare is and deconstruct a link between the weaponization of cyberspace and use of force in international law (warfare). This paper attempts to explain the taxonomy of cyber space, the difference between multiple terminologies, and types of cyber instruments. This research paper will probe what type of cyber-attack can if it is even manifest as an act of war or even possible to consider cyber-attacks as an act of war. Further, this paper will analyze the South Asian cyber operating environment. It is not easy to theorize on a type of warfare that has never really happened yet. This article is an exercise in discourse and content analysis; in an attempt to explain the weaponization of cyberspace.

Defining Cyber War

Moving forward, we will have to reconcile the concepts of violence, use of force, and lethality inherent in the conduct of war. Richard Clarke defines cyber war as, "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption".[2] Shakarian describes cyber warfare as, "an extension of policy by actions taken in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)".[3]

Duncan Hodges and Sadie Creese explain cyber-attack as, "An electronic attack to a system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital (such as data or information or a user account), digital services (such as communications) or a physical asset with a cyber-component (such as the process control system found in a building, aircraft or nuclear refinement facility). Typically, such attacks seek to compromise the confidentiality, integrity or availability of digital assets, and so cyber security controls seek to preserve these properties in some way".[4]

In light of US National Military Strategy for Cyberspace Operations, cyber operations are categorized under information operations, which are defined as "integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting our own" as defined by Joint Doctrine for Information Operations published in 2012.[5] ICRC refers to cyber operations as "operations against or via a computer or a computer system through a data stream. Such operations can aim to do different things, for instance to infiltrate a system and collect, export, destroy, change, or encrypt data or to trigger, alter or otherwise manipulate processes controlled by the infiltrated computer system".[6]

U.S DoD dictionary of Military and Associated terms defines it as "employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".[7] Tallinn Manual published in 2013, defines cyber operations as "the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace".[8] US National Military Strategy for Cyberspace Operations defines Computer network exploitation enabling operations (CNE) as, "enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks".[9]

NATO's Glossary of terms and definition describe Computer network exploitation enabling operations as "action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage".[10]Joint Terminology for Cyberspace Operation published in 2010, defines Computer network attacks (CNAs) as " A category of fires employed for offensive purposes in which actions taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves. The ultimate intended effects are not necessarily on the targeted system itself, but may support a larger effort, such as information operations or counter terrorism".[11]

The same manual published by Joint Chiefs, defines cyber warfare as, "an armed conflict conducted in whole or part by cyber means. Military operations conducted to deny an opposing force the effective use of cyberspace systems and weapons in a conflict".[12] These inherent contradictions and similarities are just a start of this complex cyber space, and this even before, we discuss the instrumental nature of war with regards to violence, use of force, and lethality.

There is a very valid question as to what amounts to war in this regard. Clausewitz defined "war is an act of force to compel our enemy to do our will". Experts have varied opinions on when it comes to the interpretation of use of force in international law. Similarly, not all cyber-attacks can be considered an act of war; neither can they be exempted from such classification. To understand the threat level of cyber war, we must familiarize with multiple classifications among cyber operations, and their range of effects on international security.

Types of Cyber Attacks

There are multiple types of cyber-attacks. Each one has distinct characteristics. If a website is hacked and defaced, it cannot possibly constitute an act of war but if a cyber-attack is directed towards sabotaging a nuclear reactor, it can be considered an act of war.

One of the most infamous incidents of cyber operation, which prompted Estonia to call upon NATO to invoke Article 5, was DDoS attack on Estonia in 2007. NATO never invoked Article 5; however, it did invite experts and issued guidelines on international law applicable to cyber warfare. NATO and Estonia blamed Russia for this cyber-attack, albeit it was never proven.

The Distributed Denial of Service attack referred to as DDoS, began on April 27, 2007. It targeted the Estonian government, banking, and telecom industry. "DDoS attack is simple technique use to shut down servers and websites by sending massive flood of data traffic which servers do not have the capacity to handle."[13] These DDoS attacks were conducted by botnets; botnets are network of computers operated by unauthorized user. These cyber-attacks did not result in injury or death of people, destruction of property or any other form of physical damage to justify it as use of force or as an act of war. In strategic terminology, it is considered an act of subversion, it can be considered an inconvenience at most.

Sabotage

When we imagine an attack on a nuclear power plant, we normally picture, a squadron of F-16's flying in all its might and speed, dropping laser guided, bombs. Well not any more, discovery of Stuxnet, a cyber-weapon employed to target Supervisory Control and Data Acquisition (SCADA) system of Iran's Natanz nuclear plant, with an aim to destroy Iran's nuclear program has changed the strategic implications for taking such an action.

Stuxnet was termed as the first incident of weaponization of malware for the purpose of physical damage to infrastructure. It is considered a highly sophisticated and customized weapon, which destroyed a quarter of Iran's nuclear centrifuges in 2009-2010. The kind of operation required meticulous planning and considerable strategic capital is now that possible to execute with keystrokes. Stuxnet is considered to be part of cyber operation code named "Operation Olympic Games",[14] jointly conducted by U.S and Israel. The weapon was highly customized to infect and damage only handful of select computer systems. Any kinetic attack of this nature on critical national infrastructure by an adversary would be considered a use of force or an act of war, but it did not cause any major violence or destruction, which are part and parcel of kinetic attacks. Thomas Rid classified these kind of cyber operations as sabotage.

Some would suggest they were simpler times when we could just destroy nuclear plants with fighter jets and bombs, as was the case with "operation outside the box", conducted by Israeli Defense Forces. The target of Israeli airstrikes was a nuclear reactor in Deir ez-Zor region in eastern Syria. This nuclear reactor was of North Korean design, partially funded by Iran. For over a decade, Israeli establishment had maintained a strict censorship, however in

March 2018, Israeli Ministry of Defense released video footage confirming the strike.[15]

One of most important component of the airstrikes was role of IAF's Sky Crows Squadron. This squadron was successful in deactivating Syrian air defense system, before Israeli jets crossed into Syrian airspace.[16] Simply put, when Israeli fighter birds were maneuvering in Syrian airspace, the air defense controllers in Damascus were seeing what IAF's electronic warfare unit wanted them to see, which was absolutely nothing. Operation out of the box was a kinetic military operation preceded by cyber-attack.

Espionage

Remember Operation Olympic Games, stuxnet was only part of broader operation. A more sophisticated malware, code named 'Flame', was discovered in 2012. It is considered more complex than stuxnet, with rather completely different objective. Flame is designed to collect information; to spy and steal data from infected computers. It also creates a backdoor for attacker to remotely control the system.[17] It targeted Iranian political and military leadership, with Iran's computer emergency response team, discussing publicly the extent of harm it can cause.[18]

Flame is a quintessential example of good old spying. These are some of most infamous incidents of cyber operations in interstate conflict. Surprisingly none of them had violent or lethal effects as compared to kinetic operation. This is where it becomes difficult to reconcile cyber operations with the natural facet of warfare.

'Titan Rain' was a code name given to series of 'Advanced persistent threats' (APTs).[19] These coordinated attacks started in 2003 with the target of stealing sensitive information from U.S government and defense contractors including Lockheed Martin, Sandia National Labs, World Bank, NASA, and Redstone Arsenal among others.

Ghostnet discovered in 2009 was massive scale cyber-spying operation. Its primary targets were diplomatic offices of Dalai lama and NGOs working on Tibetan cause.[20] The aim was to extract communication and information stored on computer networks. Malware was purely designed for espionage, and was not configured for destruction.

Similarly, Operation Aurora was a series of APT attacks occurred from December to January 2010.[21] These attacks targeted major technical and financial firms. The firms included Google, Yahoo, Adobe, Morgan Stanley, Wells Fargo, DuPont Industries, Dow Jones, and Standards and Poor among others. These attacks again were neither violent in nature nor did they produce any lethal effects.

Thomas Rid argues that "all known political cyber offenses, criminal or not, are neither common crime nor common war. Their purpose is subverting, spying, or sabotaging".[22] Considering war has an instrumental nature, which is to achieve political gains through use of violence and force; use of cyber operations would be considered a tactical maneuver at best. Estonia's Prime Minister Andrus Ansip, asked media to explain to him the difference between a naval blockade of sovereign states and the blockade of government institutions and newspaper websites. Well, there is no degree of equivalence between blocking websites and naval blockade. Blocking websites does not cause violence and certainly cannot be categorized as use of force, according to the ambiguous yet widely accepted legal interpretation.

Defense Industrial Base attacks occurred in 2007 were an attack on military weaponry. The objective of the attack was to steal highly sensitive information related to under production advanced weapons, such as designs and weapon specs of F-35 Joint Strike Fighter, Patriot Missiles, and Anti-Ballistic Missile Defense system now known as 'THAAD", 'Terminal High Altitude Area Defense'.

Subversion

Sony Hack in 2014 was widely attributed to North Korean regime. In response to a movie, North Korean perceived insulting to Kim Jong Un, North Korean hackers stole sensitive content and communication material from North American Movie studio.

In the midst of the Russian-Georgian war in 2008, Russian origin cyber forces initiated a massive cyber-attack against Georgian government and banking networks. The aim was to create confusion by cutting communication bridge between government, public and International community. This cyber-attack can be considered complementary in nature with-in the midst of conventional attack.

Use of Force and International Law

The primary treaties that deal with war and conduct of war are; United Nations Charter, Geneva Convention of 1949, its Additional protocols of 1977, and Hague conventions of 1899, and 1907. To understand this legal quagmire, one must start with 'Article 2(4)' that prohibits the use of force in international politics. It states, "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".[23] Concept of force is again very important in context of war, and in the absence of exclusive treaty underlining cyber warfare, one must rely on Martens clause in Additional Protocol 1 of 1977, which state;

"in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience".[24]

What International Law Says About Cyber Warfare

We find no treaty that exclusively addresses cyber conduct, except a cybercrime treaty, under the framework of Council of Europe, signed in 2001.[25] Budapest Convention on cybercrime dealt with criminalization of certain cyber offences. It also called upon treaty members to extend mutual jurisdiction and assistance to each other. This treaty primarily deals with transnational cyber-crimes. It is targeted towards cyber criminals, as compared to the cyber conduct of nation states.

In the absence of customary International Law, it becomes rather difficult to examine the conduct of states in cyberspace but just as Judge Simma concluded that "the absence of a legal prohibition however does not constitute the presence of a legal permission."[26] Moreover, International Court of Justice (ICJ) concluded that "an international instrument has to be interpreted and applied within the framework of the entire legal system prevailing at the time of the interpretation."[27]

Use of force to achieve political gains is defined as a violation of another state's sovereignty. International Law, does not classify all cyber operations as use of force, because of the inherent technical difficulties in attribution, and effects of operation. However, certain cyber operations, whose impact can be compared with that of kinetic attacks, could be administered under the customary international law.

A conflict between two nation-states is called an International Armed Conflict. Legal precedence and customary international law is rather clear in its interpretation that any action that results in fatalities or destruction of critical infrastructure can be considered an armed attack. Any such attack will be dealt under Article 2(4) of the United Nations charter. The conduct of war is treated under the provisions of International Humanitarian Law (IHL).

There are few remedies available for a state that suffers fatalities or an attack on its critical infrastructure. Under the ambit of international law, the victim state reserves the right to exercise self – defense, if it perceives that the cyber operation in its impact or scale has reached the threshold of a conventional or kinetic attack. The right to respond will not be limited to cyber operation. It can be kinetic in nature. The state that believes it to be the victim of the cyber-attack can also resort to United Nations Security Council. However, it might be bit of a problem if the belligerent is member of the Security Council.

In light of the above mentioned legal framework, not every cyber-attack or cyber-operation can be classified as use of force. Espionage, coercion, and sabotage are old techniques. These activities cannot be termed as use of force if they do not cause above mentioned destruction. These activities act as an auxiliary instrument in grand strategy.[28]

Cyber Warfare in South Asia

India and Pakistan have been in conflict since independence. The hostilities between the two neighbours, who also happen to possess nuclear weapons are a cause of great concern for international community. Addition of cyber space brings another dimension to their adversarial relations. As mentioned above, there are multiple types of cyber operations, designed for different outcomes. Both states have employed whole range of cyber operations against each other.[29] And these operations will only get complex with time. There is a need to study how would cyber warfare impact strategic stability of South Asia, especially between India and Pakistan.

Pakistan and 5th Generation War

Pakistan's strategic circles recognize the importance of cyber space and the need to secure it. It believes India is waging 5th generation warfare against Pakistan,[30] and cyber space is the key component of hybrid nature of 5th generation warfare.

An important element of 5th generation warfare is disinformation campaign. Its key facet is to destabilize socio-political structure of the targeted state by disseminating disinformation. The purpose of disinformation campaign is to create anarchy in the society. Anarchy is sought to ensure state's resources are diverted to combatting internal instability while the adversary utilize its resources to strengthen itself.

A coordinated campaign to damage Pakistan's image in international media was uncovered by Brussels based EU Disinfo Lab.[31] The report published by EU Disinfo Lab details 15 years of disinformation campaign designed to isolate Pakistan. Over 750 dubious and fake media organizations spread over 120 countries have been promoting Indian interests while discrediting Pakistan.

We identify four important components that could be target of cyber operations between Pakistan and India. Unless cyber-operations cause considerable physical or monetary damage, it won't escalate to kinetic conflict. The four components are as followed;

a. **Military Infrastructure.** Modern militaries rely on real time data to formulate strategic and tactical plans. Their access to real time data is based on digital infrastructure. This makes military's cyber

infrastructure highly sensitive. India and Pakistan both recognize the need to engage in penetrating others digital infrastructure.

In operation Outside the Box, Israeli Air Force first took out Syrian air defense system before aerial attack on nuclear reactor. It should be noted that without successful cyber-attack, such a clean operation would not have been possible.

Similar is the case with India and Pakistan. In military engagements achieving surprise factor is of considerable importance and its achievement becomes hander when the target is in close geographical proximity. The only way either side could achieve the shock factor is by engaging in cyber-attacks that can render the opponent's digital infrastructure unresponsive.

India and Pakistan possess nuclear weapons. Any miscommunication or confusion with regards to cyber-operations between them can be devastating not just for the region but for world at large.

b. **Critical Infrastructure.** In the 21st century, every aspect of human life is dependent on cyber space. National critical infrastructure is defined as a network of assets that are deemed necessary for maintaining normal life.[32] Every state has its own criterion of what constitutes critical infrastructure but usually include energy sector, transportation system, communication sector, and financial sector.
An American cyber security firm in its recently published report claimed that Mumbai's electric grid was targeted with cyber-attack.[33] This kind of cyber operation has the capacity to adversely impact millions of lives. These kinds of attacks on utility providers blur the lines of warfare.

c. **Economy.** Banking industry and financial markets are backbone of national economies. Our banking industry and financial markets depend on digital infrastructure to operate. This makes them vulnerable to cyber-attacks. A single day of suspension of trading in stock markets can cause billions of rupees of loss and shatter the confidence in the market. Similarly, a coordinated attack on banking network can cause immense socio-political damage. Cyber-attacks have an inherent problem of attribution. Deciding who is responsible for a cyber-attack is finding needle in a haystack. This confusion in attribution only benefits non-state actors.

Legal and Technological Implications in South Asia

In conclusion, some recommendations are derived as to how Pakistan can ensure its cyber security.

Formulate National Cyber Strategy. This is 2021 and Pakistan has not yet published its cyber strategy. The first order of business for Pakistani strategists should be to conduct a comprehensive consultation and prepare a cyber-strategy. It must define Pakistan's critical infrastructure. It needs to be an inclusive policy that ensures adequate security while safeguarding fundamental rights of the citizens.

Auditing Infrastructure Procurement. Trump administration issued an executive order to stop Huawei from building 5G communication network in the United States. It was feared that, Huawei will provide access to Chinese state that would then have the capability to piggyback through backdoor and collect massive amount of intelligence.[34]

Pakistan imports most of computing equipment it requires both for its commercial as well as military use. It must devise a mechanism to ensure that every bit of infrastructure that is procured is thoroughly audited. A dedicated organization should be created with sole purpose of ensuring that the cyber infrastructures (hardware + software components) are secure from foreign interference.

Centralized Data Centers Regime. Government of Pakistan deals with massive amount of data. This data is stored in multiple data centers operated by various agencies. There is a need to create a centralized command that can be mandated to ensure security of data as well as data centers. Similarly, data protection act needs to be upgraded. Role based access mechanism needs to be introduced to protect privacy and establish accountability of officials.

How can a regional or bilateral cyber security framework be established?

It is very necessary for strategic stability of the region that India-Pakistan establish a bilateral cyber security framework. The complex intersectional nature of cyber space requires both states to establish some ground rules.

In 1988, India and Pakistan signed an agreement on prohibition of attack against nuclear installations and facilities. Since then, both states share a list of their nuclear installations every year. There is need to establish similar mechanism. Both states should clearly define their critical infrastructure and agree not to attack those installations.

If India and Pakistan can find a mutually acceptable solution, it can decrease the chances of an accidental skirmish. As is the case with Indo-Pak history, accidental skirmishes can lead to full fledge war.

If it is impossible for India and Pakistan to cooperate bilaterally, a multilateral forum might offer more conducive environment for engagement. Pakistan and India can work together to establish a regional cyber security framework and create a pathway for other states to follow.

Endnotes

[1] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," *Comparative Strategy* 12, no. 2, (1993): 145.

[2] Richard A Clarke, and Robert K. Knake, *Cyber war* (New York: Tantor Media Incorporated, 2014), 10.

[3] Paulo Shakarian, Jana Shakarian, and Andrew Ruef, *Introduction to cyber-warfare: A multidisciplinary approach* (Waltham: Syngress, 2013), 57.

[4] Duncan Hodges and Sadie Creese, "Understanding Cyber-attacks," in *Cyber warfare: a multidisciplinary analysis*, ed. James A Green, (New York: Routledge, 2015), 34.

[5] Michael Glenn Mullen, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership* (Washington D.C: Joint Chiefs of Staff, 2011), 5.

[6] ICRC, "International Humanitarian Law and the Challenges of Contemporary Armed Conflicts," *ICRC Doc 31IC/11/5*, no.12 *(*2011): 36.

[7] US DoD, *Dictionary of Military and Associated Terms* (Washington D.C: DOD, 2011), 70.

[8] Michael N. Schmitt, ed. *Tallinn manual on the international law applicable to cyber warfare* (Cambridge: Cambridge University Press, 2013), 258.

[9] U.S DOD, *US National Military Strategy for Cyberspace Operations,* (Washington D.C: DOD, 2011), GL–1.

[10] NATO's Glossary of Terms and Definitions, p 2–C–11.

[11] U.S DOD, *Joint Terminology for Cyberspace Operations* (Washington D.C: DOD, 2011), 3.

[12] U.S DOD, *Joint Terminology,* 8.

[13] Joshua Davis, "HACKERS TAKE DOWN THE MOST WIRED COUNTRY IN EUROPE," *The Wired*, July 2007, https://www.wired.com/2007/08/ff-estonia/

[14] David Sanger, "Obama orders speed up wave of cyberattacks against Iran," *The New York Time*, June 01, 2012, https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

[15] Harel, Amos and Benn, Aluf, "No longer a secret:How Israel Destroyed Syria's Nuclear Reactor," *Haaretz*, 2018, https://www.haaretz.com/israel-news/MAGAZINE-no-longer-a-secret-how-israel-destroyed-syria-s-nuclear-reactor1.5914407

[16] Yaakoz Katz, "And they struck them with blindness," *Jerusalem Post*, 2010, https://www.jpost. Israel.com/Magazine/Features/And-theystruck-them-with-blindness

[17] Kim Zeter, "Meet Flame, The massive spy malware Infiltrating Iranian Computers," *The* Wired, May, 2012, https://www.wired.com/2012/05/flame/

[18] Thomas Erdbrink, "Iran Confirms Attack by Virus that collects Information," *The New York Times*, May 30, 2012, https://www.nytimes.com/2012/05/30/world/middleeast/iran-confirms-cyber-attack-by-new-virus-called-flame.html

[19] Nathan Thornburgh, "Inside the Chinese Hack Attack," *Time.com*, 2005, http://content.time.com/time/nation/article/0,8599,1098371,00.html

[20] BBC.com, "Major cyber spy network uncovered," *BBC.com*, 2009, http://news.bbc.co.uk/2/hi/americas/7970471.stm

[21] Kim Zetter, "Google Hack Attack was Ultra Sophisticated," *New Details show,* January, 2010, https://www.wired.com/2010/01/operation-aurora/

[22] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2012): 15.

[23] U.N charter, Article 2(4), http://www.un.org/en/sections/un-charter/chapter-i/index.html.

[24] Article 1(2) of Protocol I Additional to the 1949 Geneva Conventions on the Protection of Victims of International Armed Conflicts, text in UNTS, Vol 1125, pp 3 ff.

[25] For further understanding of Budapest convention, consult https://www.coe.int/en/web/cybercrime/the-budapest-convention. PDF version of the treaty can be downloaded at: https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

[26] Marco Roscini, *Cyber operations and the use of force in international law* (New York: Oxford University Press, 2014), 19.

[27] ICJ, "Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) notwithstanding Security Council Resolution 276 (1970)," *Advisory Opinion, 21 June 1971*, (The Hague: ICJ Reports, 1971), para 53.

[28] Roscini, Cyber operations, 161.

[29] For a detailed list of cyber operations, visit marie beazner, *Regional rivalry between India-Pakistan: tit-for-tat in cyberspace*, (Zurich, CSS, 2018). https://doi.org/10.3929/ethz-b-000314582

[30] Dawn.com, "Pakistan being subjected to 5th-generation warfare in 'massive way' but we are aware of threats: DG ISPR," *dawn*, Dec 2020, https://www.dawn.com/news/1593804

[31] Gary Machado, Alexandre Alaphilipppe, Roman Adamczyk, and Antoine Gregoire, *Indian Chronicles: Deep Dive Into a 15-year Operation Targeting the EU and UN To Serve Indian Interests*, (Brussels: EU DisinfoLab, 2020). https://www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests/

[32] "Critical Infrastructure," Department of Homeland Security, https://www.dhs.gov/science-and-technology/critical-infrastructure

[33] David Sanger, Emily Schmall, "China Appears to Warn India: Push Too Hard and the Lights Could Go Out," *The New York Times*, Feb 2021, https://www.nytimes.com/2021/02/28/us/politics/china-india-hacking-electricity.html

[34] Kadri Kaska, Henrik Beckvard and Tomáš Minárik, *Huawei, 5G and China as a Security Threat,* (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2019) https://www.ccdcoe.org/uploads/2019/03/CCDCOE-Huawei-2019-03-28-FINAL.pdf