Recognising Cyber Blockades as Crimes Against Humanity: Can International Criminal Law Keep Up?

Dora Vanda Velenczei
Monash University, Australia

dora.velenczei@monash.edu

Abstract: As a result of the heavily digitalised world on top of our increasing online presence and interconnectedness, states and civilian populations are becoming more and more vulnerable to cyber attacks. It is thus imperative to examine the dangers large scale cyber attacks pose with respect to their contribution to potential human suffering. As such, these large scale cyber attacks, especially a cyber blockade, may be able to constitute an international crime. The Prosecutor of the International Criminal Court announced at the Digital Front Lines conference that his office is willing to investigate cyber operations as potential war crimes given that they are capable of causing severe consequences akin to kinetic warfare. (Yoon Onn, 2023) This is the first significant step towards recognising the harmful effects of malicious cyber operations as international crimes. However, not only is the Rome Statute itself silent on cyber operations as potential international crimes, the ICC has not yet seen a case concerning malicious cyber activities as either a war crime or as a crime against humanity. As such, the central question the paper seeks to answer is whether the Rome Statute could potentially encompass cyber blockades as the crime against humanity of "other inhumane acts" under Article 7(1)(k) of the Rome Statute. The paper looks at crimes against humanity for three reasons: firstly, Karim Khan KC has already touched on cyber attacks potentially prosecuted as war crimes, as mentioned above, thus the knowledge gap is gradually being bridged with respect to war crimes. Secondly, there is an absence of any regulatory framework should a cyber blockade be unleashed in peacetime, where international humanitarian principles do not apply. Thirdly, establishing a cyber blockade as a crime against humanity would lead to greater individual criminal responsibility as opposed to a war crimes conviction. This, in turn, would send a strong deterrent message in both war and peace.

Keywords: Cyber blockades, Crimes against humanity, Rome Statute, Other inhumane acts, International criminal law

1. Introduction

The first instance of a cyber blockade can be traced back to the 19th century, though these resembled information blockades as opposed to cyber blockades. The Spanish-American War in 1898 has seen the first instance of submarine cables connecting neutral parties to territory controlled by belligerents frequently cut by US naval forces. (Hyde, 1922) This impaled the belligerents' capability to transmit intelligence and war strategy. Additionally, another information blockade emerged when the British forces blockaded Germany during World War I. While this primarily was a traditional blockade, Britain destroyed German communication cables and used Allied communication links to intercept and censor German military communication thereby adding the information blockade element to the traditional blockade. (Bruton, 2017) As such, information blockades have existed for an extended period of time.

The first occurrence of a cyber blockade was in 2007, when alleged Russian hackers brought down Estonia, as mentioned above. (Russell, 2014) As such, cyber blockades are unique to the 21st century. A cyber blockade can include a wide variety of activities ranging from distributed denial of service attacks (Landler and Markoff, 2007), through data breaches (Vojinovic, 2023), to malware and ransomware (Bhuiyan, 2023) to mention a few. As it will be seen, a cyber blockade can bring about several types of inhumane acts ranging from the deprivation of basic necessities through severe economic harm to injury or even death. Additional issues are encountered with the fact that contrary to a traditional blockade, a cyber blockade could exist in both war and peace. As a result, there is an impunity gap that international criminal law needs to be able to address that international humanitarian law cannot in peacetime. Thus, this paper discusses whether cyber blockades could be prosecuted as crimes against humanity under the Rome Statute.

2. What is a Cyber Blockade?

In the current, increasingly digital world, it is necessary to examine whether blockades are capable of being created in the cyberspace and whether there are adequate mechanisms to safeguard against a cyber blockade. The term cyber blockade does not yet enjoy a collectively accepted legal definition. There is one potential definition that was provided by Russell. According to her thesis, a cyber blockade includes "the act of preventing a state, through cyber attacks, from receiving or transmitting information beyond its borders for political reasons, with the intent of weakening the state, government institutions, economy, or society." (Russell, 2014)

According to this paper, a cyber blockade can be defined as a concerted and intentional effort to significantly disrupt or limit, or entirely deny digital communication, data retrieval, and information flow between states, organisations, and individuals, via the utilisation of cyber means. This can involve tactics aimed at impeding the state's access to online resources, services, or data physically or digitally, and directly or indirectly via its population.

This paper posits that state weakening may be a central motive behind a cyber blockade, though this is not always the case. For example, if we take a look at the, allegedly, Russian cyber attack against Estonia, the central motive was indeed political weakening. (Russell, 2014) Estonia had decided to move a controversial Communist era statue, to which allegedly hackers sponsored by the Russian Federation responded with a comprehensive cyber attack that brought down the critical infrastructure and froze all digital data and communication of the civilian population of Estonia. (Russell, 2014) However, if we look at more recent cyber blockades, such as when the Costa Rican government and its state bodies were brought down by alleged Russian cyber attackers, the motive was simple extortion. (Datta and Acton, 2023) As a result, a definition must encompass all possible motives behind a cyber blockade.

As for data retrieval and information flow, the paper posits that data could be attacked. There is literature supporting this, although mostly focusing on armed conflict scenarios in the sense of whether data can be an object under international humanitarian law. (Pomson, 2023) This paper postulates that data can be attacked by a cyber blockade whether unleashed in peacetime too thereby significantly widening the scope of protection offered to a civilian population. The rationale to include data is because a state could be crippled via the partial or complete blockading of its civilian data, particularly if said data is publicly controlled, like tax data. This will be seen below especially from the Costa Rican ransomware attack in 2022.

As for victims, a cyber blockade could be unleashed on a civilian population and/or on a state and its organs. This paper suggests that a cyber blockade not per se focusing on a state and/or its organs could still be capable of weakening the state and/or targeting its weakness. This is suggested by the Colonial Pipeline ransomware attack of 2021, where Colonial Pipeline's servers had been brought down by the attackers. Had the company not paid the ransom worth of $4.4 million, hospitals, first responders, law enforcement, fire departments, airports, and traveling civilians could have been seriously compromised. This could have adversely affected the state and could have significantly weakened the state primarily economically and politically. (Associated Press, 2021) At the same time, the definition is not wide enough to encompass sporadic and rather disorganised instances of cyber attacks, which would most likely fall within the normative domestic law of cybercrime.

3. General Elements of Crimes Against Humanity under the Rome Statute

The below sections deal with whether Article 7 of the Rome Statute could offer a legal basis for the international prosecution of a cyber blockade as a crime against humanity. This section briefly outlines the legal landscape of crimes against humanity generally, then it moves onto discussing the specific crime against humanity of "other inhumane acts" as enunciated under Article 7(1)(k) of the Rome Statute. As a starting point, crimes against humanity comprise of inhumane acts that intentionally cause great suffering when committed part of a widespread or systematic attack directed against a civilian population with knowledge of the attack. (Article 7, Rome Statute) Crimes against humanity are more onerous crimes than war crimes, and encompass a wider range of crimes than genocide and aggression. However, they have been relatively overlooked with respect to large-scale cyber threats that are conducted outside the scope of an armed conflict.

3.1 Material Elements — Widespread or Systematic Attack against a Civilian Population

An attack must be either widespread or systematic. The definition takes a disjunctive approach rather than a conjunctive, which allows for the prosecution of crimes that may only be either widespread or systematic. Consequently, a miscarriage of justice can be better evaded. Widespread refers to the large-scale nature of the attack, while systematic refers to their organised nature and improbability of their random occurrence. (*Prosecutor v Akayesu*, 1998, *Prosecutor v Kunarac*, 2004) The *Akayesu* judgment further explains that such attack must happen pursuant to or in furtherance of a state or organisational policy to commit such an attack. This means that some minimal level of scale, multiplicity, and some collectivity is required. Though a single event may qualify as a crime against humanity, in practice that would likely not be categorised as such. The cases of *Stanišić and Simatović* further held that an attack is not limited to the use of force and it can include any mistreatment of the civilian population.

With respect to the meaning of "civilian population" in crimes against humanity comes from international jurisprudence. Conventionally, discussion about the meaning of civilian population was restricted to armed

conflict scenarios. However, given a crime against humanity can be committed in peace just as much as in war, the notion of civilian population must be understood in both war and peace. Thus the meaning of "civilian population" encompasses those of non-combatant status, and further stipulates that they must be a significant portion of the "civilian population" thereby outweighing those with combatant status. *Hors de combat* may be categorised as civilian. (*Prosecutor v Muthaura et al*, 2012)

3.2 Material Elements — State or Organisational Policy

The requirement that widespread or systematic attacks be carried out pursuant to or in furtherance of a state or organisational policy is unique to the Rome Statute. This element requires that a state or organisation has a plan or policy to commit the crime so as to distinguish attacks from isolated and sporadic attacks by random individuals. The policy need not be adopted at a high level, it does not have to be communicated according to any formality, and can be inferred from the circumstances, such as the way the crimes occur. It is satisfied when an individual actively promotes the state policy and when someone commits criminal acts envisaged by that policy. (*Prosecutor v Bemba*, 2016) It is not required that the policy be communicated in any specific way. There is no requirement that the policy be implemented by either action or inaction, and it can be inferred from the circumstances. (*Prosecutor v Katanga*, 2012)

3.3 Mental Elements — Intent and Knowledge of the Attack

The perpetrator must know or intend for the conduct to be part of the widespread or systematic attack against a civilian population. Knowledge may be further inferred from relevant facts and circumstances. The perpetrator must engage in the conduct and they must intend for the consequences to occur in the ordinary course of events. (Rome Statute, 1998) With respect to this, the ICC developed a virtual certainty test to assess the foreseeability or the consequence that would normally follow in the circumstances where the acts were committed. (*Prosecutor v Bemba*, 2006) It is not required that the perpetrators fully understand the precise nature or scale of the attack. (Elements of Crimes, 2011)

4. Cyber Blockades as Crimes Against Humanity of "Other Inhumane Acts" under Article 7(1)(k) of Rome Statute

This section looks at whether a cyber blockade could be internationally prosecuted under the Rome Statute. There are specific requirements for a perpetrator to commit the crime against humanity of "other inhumane acts" under Article 7(1)(k). Firstly, the perpetrator must have inflicted great suffering, or serious injury to body or to mental or physical health by means of an inhumane act. The conduct must have been committed as part of a widespread or systematic attack directed against a civilian population. The perpetrator must have known that the conduct was part of or intended the conduct to be part of a widespread or systematic attack directed against a civilian population. (Elements of Crimes, 2011)

Perhaps the most contentious issue is the infliction of great suffering or serious injury via an inhumane act given that it is uncertain whether a cyber blockade would involve such harm or suffering. Consequently, the paper now turns to arguing that a cyber blockade can inflict such suffering or injury and so it can come within the scope of Article 7(1)(k). While jurisprudence is scarce on Article 7(1)(k), the starting point is the joint case of *Ngudjolo Chui and Katanga* before the Pre-Trial Chamber (PTC) of the International Criminal Court (ICC). The Chamber noted that the provision under Article 7(1)(k) operates as a '..."catch all provision" leaving a broad margin for the jurisprudence to determine its limits.' This is a particularly welcome article amongst the specified offenses under crimes against humanity for it keeps up with developments. In other words, Article 7(1)(k) acts as a *lex ferenda* provision. Thus novel forms of inhumane acts can be brought within its scope that the drafters in Rome may not have contemplated.

While this significantly widens the scope of Article 7(1)(k), previous jurisprudence seems to have been omitted by the PTC. The International Criminal Tribunal for the former Yugoslavia (ICTY) and International Criminal Tribunal for Rwanda (ICTR) described 'other inhumane acts 'as '...acts that deliberately cause serious mental or physical suffering or injury or constitute a serious attack on human dignity.' (*Prosecutor v Kayishema and Ruzindana*, 1999, *Prosecutor v Bagilishema*, 2001, *Prosecutor v Blaškić*, 2000) Indeed, if one follows the ICTY and ICTR's conclusions, unless an attack on human dignity can be shown, a cyber blockade may lay outside the scope of 'other inhumane acts'. Aspects of an attack on human dignity may include dehumanization, severe mental or bodily suffering, humiliation, the violation of human rights, and discrimination and stigmatization. (Renzo, 2012) It would be impetuous to posit that a cyber blockade is incapable of inflicting an attack on human dignity,

though it is conceded that the ICTR and ICTY standard involves a potentially higher threshold than that of the ICC.

In the case of a cyber blockade then, it could be argued alongside the PTC's reasoning that a cyber blockade may be caught by Article 7(1)(k). Indeed, the PTC held that 'other inhumane acts' '...are to be considered as serious violations of international customary law and the basic rights pertaining to human beings, drawn from the norms of international human rights law...'. (*Prosecutor v Katanga*, 2012) This would then allow the consideration of acts that would normally fall outside the scope of Article 7(1)(k). Below the paper examines specific situations that are capable of being created by a cyber blockade, which would be prosecutable inhumane acts under Article 7(1)(k).

4.1 Denial of Critical Services and Disruption of Critical Infrastructure

If a cyber blockade disrupts critical services, especially those services that are necessary to sustain life, such as healthcare, electricity, water supply, or emergency response systems, it can lead to severe suffering and even loss of life. This is particularly the case in situations, where people rely on these services for their basic needs. There is no evidence that a cyber blockade has ever resulted in death. However, should hospitals and emergency services go down as a direct result of the cyber blockade and result in loss of life, the cyber blockade may fall within the scope of the crime against humanity of "other inhumane acts". (Russell, 2014)

Additionally, cyber blockades that target critical infrastructure, in other words, those assets, systems, and networks that provide services necessary to carry on with daily life and even sustain life. For example, with the increasing digitalisation of power grids, they are becoming more and more vulnerable to a cyber blockade. (Krause et al, 2021) By blockading a power grid, perpetrators could block civilians from accessing necessary services, and even cause harm or death to individuals should a blackout occur at a hospital within its coverage.

For example, there has been evidence of a sophisticated attack on the University of Manchester in 2023, which involved a paralysis on NHS medical records and patient data. (Bateson, 2023) While this event cannot be classified as a cyber blockade, attacks like this within the scope of a cyber blockade could in turn bring the attack within the scope of Article 7(1)(k). Consequently, a cyber blockade targeting critical services or infrastructure could be characterised as "other inhumane acts".

4.2 Economic Impact

Cyber blockades that target financial institutions or disrupt the economy can cause a potential market crash, and even job loss with potential increase in poverty. This in turn could lead to significant suffering among the affected population. As technology currently stands, there appears to be no systemic cyber risk that would be capable of significantly impacting the economy, this is not proof of an absence of risk. (Warren, Kaivanto, and Prince, 2018) While Warren et al's article does not contemplate a cyber blockade, the piece rightfully concedes that their speculations are not risk free. Indeed, a cyber blockade could, theoretically, contribute to a significant economic downturn should its primary or sole aim be to paralyze the state economy. This, in turn, could have a detrimental effect on the respective civilian population to the extent that it may come within the scope of Article 7(1)(k).

This was the case, when the government of Costa Rica was compromised by a ransomware attack in 2022. Twenty-seven public institutions were targeted, which included the Ministries of Finance, Labour and Social Security, and the Science, Innovation, Technology and Telecommunications, the National Meteorological Institute, and the Social Security Fund. (Murry and Srivastava, 2022) The attack began with the crippling of the servers of the Finance Ministry, which disabled the Virtual Tax Administration and the Customs Information System. Then the websites of the Science Ministry and Meteorological Institution were disabled. The latter also saw information theft via an attack on the email server. A secondary attack, supposedly by a different actor, shut down the critical systems of the Social Security Fund, including the Single Digital Health Record. The only purpose was to extort money from the Costa Rican government. (Datta and Acton, 2023)

The government refused to pay the ransom, and as a result, the cyber blockade remained operational for several months until the end of June 2022. The government was forced to temporarily shut down the computer systems that are normally used for declaring taxes and for the control and management of imports and exports. This caused an economic loss of approximately US$ 125 million in the first two days after the cyber blockade was unleashed. (Chamber of Foreign Trade of Costa Rica, 2022) On 8 May 2022, the president of Costa Rica issued an executive order proclaiming a national emergency due to the cyberattacks against the country's public sector and stated that the country was in a "state of war". (Collier, 2022)

As the above example demonstrates, a cyber blockade could disable a state's financial sector and economy to a degree that it could be categorised as "other inhumane acts". Since this most likely would happen within the context of a widespread or systematic attack, the cyber blockade could be characterised as a crime against humanity.

4.3 Humanitarian Impact

Under international humanitarian legal rules, once an offer of aid by an impartial humanitarian organisation is accepted by interested parties, they must '…allow and facilitate rapid and unimpeded passage of humanitarian relief for civilians in need…' (Additional Protocol I, Article 70(2), which broadened previously adopted position in Geneva Convention IV, Article 23. See also ICRC Customary International Humanitarian Law Study 2005, Rule 55.) While there is academic support for the contention that blocking humanitarian aid may potentially constitute a crime against humanity, it is largely restricted to kinetic means, in other words, the physical interference or blocking of such aid. (Kraemer, Bhattacharya, and Dhrubajyoti, 2012)

In a cyber scenario, if the cyber blockade interferes with the delivery and administration of humanitarian aid, medicine, and other basic necessities to ensure survival, it can result in severe suffering and harm to those who depend on such assistance for their survival. (Tallinn Manual 2.0, 2017) The obligation not to interfere includes the obligation to ensure personnel are respected and protected: a cyber blockade must not be utilised to block the delivery of humanitarian aid and to cut off personnel from accessing aid to deliver. (Gisel, Rodenhauser, and Doermann, 2020) As such, blockading humanitarian assistance via cyber means could cross the threshold of Article 7(1)(k).

4.4 Psychological Impact

Prolonged cyber blockades, especially those that cut off communication or access to information, can lead to psychological distress, anxiety, and other forms of mental suffering among individuals who are isolated or unable to connect with loved ones.

Cyber blockades may trigger emotional trauma responses for there may be a sense of helplessness with respect to the extreme complexity of the cyberspace. (Kostyuk and Wayne, 2021) The amount of new technology put out on an almost daily basis makes it increasingly burdensome for lay civilians to keep up to date. Thus, this sense of rapid novelty potentially mixed with anxiety and dread may be the main driving force behind public responses. (McDermott, 2019)

Secondly, the ubiquity of cyberspace and digital interconnectedness, and the transnational reliance on the digital architecture mean that the civilian population may feel constantly threatened. Indeed, there are accounts of this from the 2007 Estonian Distributed Denial of Service attack. The editor of the Estonian daily newspaper Eesti Paevaleht, commented that 'You couldn't get information; you couldn't do your job. You couldn't reach the bank; you couldn't check the bus schedule anymore. It was just confusing and frightening.' (Mite, 2007)

Thirdly, the fact that there is increasing difficulty around deciphering who is behind a cyber blockade may cause additional negative psychological impact, which in turn can exacerbate the perceived risk. (Egloff 2020, Kaminska 2021) A sophisticated, high level cyber perpetrator would have little difficulty concealing their digital footprint, and could even make a cyber blockade look like as though it originated from somewhere else than in actuality. For example, should a cyber blockade have taken place, and the governmental and national security authorities are unable to trace the attack back to a perpetrator and make a confident attribution, this sense of uncertainty can exacerbate the psychological impact of the cyber blockade. As a result, given the potential emotional trauma, a cyber blockade may be characterised as "other inhumane acts" under Article 7(1)(k) of the Rome Statute.

5. Conclusion

Cyber blockades have evolved from the traditional law of blockades into the cyber sphere. Given a cyber blockade can be released in both war and peace, academia ought to examine its capabilities from a holistic perspective in the absence of a comprehensive regulatory framework. The most robust international legal framework that has a peacetime applicability is international criminal law, more specifically crimes against humanity. In contrast to war crimes, crimes against humanity can be committed during peacetime; unlike genocide, crimes against humanity is legally easier to establish for it does not require a special intent to kill based on group status.

However, as shown, the Rome Statute and its accompanying Elements of Crimes are becoming increasingly outdated for a cyber blockade would likely fall outside the scope of crimes against humanity. The only possible legal basis for international prosecution is Article 7(1)(k), which is designed to capture "other inhumane acts". Though, the International Criminal Court is yet to clarify its arguments for there is a discrepancy in jurisprudence from the ICTY and ICTR with reference to what is required to be established in order to successfully prosecute "other inhumane acts".

Thus, with the rapid emergence of new technologies that can be utilised in an offensive way whether in war or peace, international criminal law is increasingly becoming obsolete. A cyber blockade poses one of the greatest challenges to the existing framework of international criminal law given its destructive capabilities with respect to a civilian population and its respective state. Consequently, international criminal law must stay up-to-date with respect to unique cyber threats, such as cyber blockades. While theoretically these could be prosecuted internationally under Article 7(1)(k) of the Rome Statute, the International Criminal Court is yet to hear a case of this nature.

References

Associated Press, (2021) 'Colonial Pipeline confirms it paid $4.4m ransom to hacker gang after attack', The Guardian, 19 May.

Bateson S, (2023) 'NHS cyber attack follows rising numbers of data breaches in global healthcare sector' *Verdict*, 29 June.

Bhuiyan J, (2023) 'Cyberattack disrupts hospital computer systems across US, hindering services' *The Guardian*, 04 August.

Chan Yoon Onn K, (2023), 'The Prosecutor's New Policy on 'Cyber Operations' before the International Criminal Court (and its Implications for Ukraine): Some Preliminary Reflections' *EJIL Talk!* (15 September).

Chincilla D, (2022), '$125 millones en pérdidas estima Cámara de Comercio Exterior tras ciberataque que afectó aduanas' *Amelia Rueda*, 19 April.

Collier K, (2022) 'Costa Rica declares state of emergency over ransomware attack' *ABC News*, 11 May.

Datta, P. M., & Acton, T. (2023), "Ransomware and Costa Rica's National Emergency: A Defense Framework and Teaching Case" *Journal of Information Technology* Vol 0, No 0.

Drew P, (2017) *The Law of Maritime Blockade: Past, Present, and Future*, Oxford University Press.

Egloff F, (2020), "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* Vol 6 No 1.

Gisel L, Rodenhauser T, Doermann K, (2020) "Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts" (2020) *International Review of the Red Cross* Vol 102, No 913.

Henckaerts J-M and Doswald-Beck L, (2005) *Customary International Humanitarian Law Rules Vol 1*. Cambridge University Press.

Hyde C, (1922) *International Law Chiefly as Interpreted and Applied by the United States,* Little Brown.

Kaminska M, (2021), "Restraint under Conditions of Uncertainty: Why the United States Tolerates Cyberattacks." *Journal of Cybersecurity* Vol 7 No 1.

Kostyuk N, Wayne C, (2021), "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* Vol 6 No 2.

Kraemer J, Bhattacharya, Dhrubajyoti, (2012) "Blocking Humanitarian Assistance: A Crime Against Humanity?" *Leibnitz Information Centre for Economics*.

Krause T, Ernst R, Klaer B, Hacker I, Henze M, (2021) "Cybersecurity in Power Grids: Challenges and Opportunities" Special Issue Security and Trustworthiness in Industrial IoT Vol 21 No. 18.

Landler M and Markoff J, (2023) 'Digital Fears Emerge After Data Siege in Estonia' *The New York Times*, 29 May.

Marklund, Andreas, and Rüdiger, (2017) *Historicizing Infrastructure.* Aalborg University Press.

McDermott R, (2019), "Some Emotional Considerations in Cyber Conflict." *Journal of Cyber Policy* Vol 4, No (3), pp 309–25.

Mite V, (2007) Estonia: Attacks Seen As First Case Of 'Cyberwar' *Radio Free Europe*, 30 May.

Murry C, and Srivastava M, (2022) 'How Continue Ransomware Group Crippled Costa Rica - Then Fell Apart' *Financial Times*, 9 July.

Pomson O, (2023) ""Objects? 'The Legal Status of Computer Data under International Humanitarian Law", *Journal of Conflict and Security Law*, Vol 28, No 2, pp 349-387.

Renzo M, (2012) "Crimes Against Humanity and The Limits of International Criminal Law", *Law and Philosophy* Vol 31, No 4, pp 443-476.

Russel AL, (2014) *Cyber Blockades*, Georgetown University Press.

Schmidt M N et al, (2017) *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, Cambridge University Press.

Shandler R, Gross ML, Canetti D, (2023) "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis", *Journal of Global Security Studies* Vol 8 No 1.

Vojinovic I, (2023), '10 of the Biggest Data Breaches in History' *DataProt*, 14 July.
Warren P, Kaivanto K, Prince D, (2018) "Could a Cyber Attack Cause a Systemic Impact in the Financial Sector?" Bank of England Quarterly Bulletin Q4.
Legislation
Elements of Crimes 2011. Available at: https://www.icc-cpi.int/sites/default/files/Publications/Elements-of-Crimes.pdf (Accessed 18 October 2023).
Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) 1977. Available at: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 (Accessed 18 October 2023).
Rome Statute of the International Criminal Court 1998, c. 2. Available at: https://www.icc-cpi.int/sites/default/files/RS-Eng.pdf (Accessed 18 October 2023).
Cases
Prosecutor v Akayesu (1998) ICTR-96-4-T.
Prosecutor v Bagilishema (2001) ICTR-95-1A-T.
Prosecutor v Bemba (2009)ICC-01/05-01/08.
Prosecutor v Bemba (2016) ICC-01/05-01/08
Prosecutor v Blaškić (2000) IT-95-14-T.
Prosecutor v Gbagbo and Blé Goudé (2012) ICC-02/11-01/15.
Prosecutor v Katanga (2012) ICC-01/04-01/07.
Prosecutor v Katanga and Ngudjolo Chui (2009) ICC-01/04-01/07 OA 8.
Prosecutor v Kayishema and Ruzindana (1999) ICTR-95-1- T.
Prosecutor v Kunarac et al (2004) IT-96-23-T & IT-96-23/1-T.
Prosecutor v Muthaura et al (2012) ICC-01/09-02/11.
Prosecutor v Tadić, (1997) IT-94-1-T.
Prosecutor v Stanišić (Jovica) and Simatović (Franko) (2017) MICT-15-96-PT, ICL 1099.