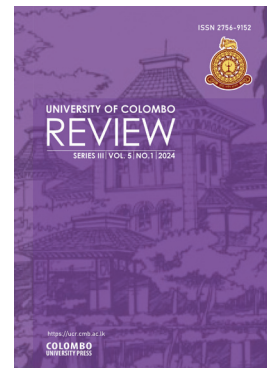


DOI: <https://doi.org/10.4038/ucr.v5i1.99>

University of Colombo Review (Series III),
Vol.5, No.1, 2024



“Big Data Breaches”, sovereignty of states and the challenges in attribution

Shannel Gunatileka

Independent Researcher

ABSTRACT

“Big data” refers to large sets of data, which are computationally analyzed to reveal patterns or trends in human behavior and interactions. At present, with the increased use of cyberspace for day-to-day activities, sensitive personal data is stored in computer servers. This massive number of data sets could be used to generate predictive models for a variety of uses such as policy-making and the prediction of societal changes. This has propelled nation-state adversaries to amass “big data” of another state through low-threshold data breaches. This article focuses on “big data breaches” committed by “state or state-sponsored groups”, involving a massive amount of data from victim states. For a cyber-attack to qualify as an “armed attack” or “use of force” under international law, it must satisfy the requirements of the “scale and effect” test. However, a big data breach would not satisfy this test and the attribution of the liability for lower-threshold cyber breaches has become a challenge. This is mainly because there is lack of consensus on the international law principles applicable to cyberspace. Nevertheless, big data breaches must be attributed, because it is an intrusion on state sovereignty, threatens security and results in economic loss. Qualitative research methodology was used to analyze state-sponsored big data breaches, the existing international legal framework, the drawbacks in attribution of such breaches and the need to push forth tailor-made laws for attribution of low-threshold big data breaches.


KEYWORDS:

Big data, State-sponsored data breaches, Low-threshold, Sovereignty, Attribution

Suggested Citation: Gunatileka, S. (2024). Big Data Breaches”, sovereignty of states and the challenges in attribution. *University of Colombo Review* (New Series III), 5(1), 104- 129

© 2024 The Author. This work is licenced under a Creative Commons Attribution 4.0 International Licence which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

✉ Corresponding author: shannelgunatileka@gmail.com

 <https://orcid.org/0009-0001-7832-9645>

Introduction: “Big data breaches” as a breach of personal data

Cyber-attacks such as the *Stuxnet* attack that disabled the Iranian nuclear program (Fruhlinger, 2022), the 2007 Estonian cyber-attacks on Estonia’s private and public sector organizations (International cyber law: interactive toolkit, 2021), the 2008 Georgian cyber-attacks on a series of websites during the Russo-Georgian War (International cyber law: interactive toolkit, 2021), and the 2013 Twitter Hack that affected the U.S. Stock Market (Moore & Roberts, 2017) are some examples of cyber-attacks on critical infrastructure, power grids, nuclear plants and attacks that malfunctioned computer networks. Apart from such cyberattacks, there is a global increase in big data breaches.

The COVID-19 pandemic shifted many sectors such as education and business to online platforms. To access online services, people provided their personal details. This resulted in a surge of data from the general public being released onto cyber-platforms. In addition, web-app companies enabled third-party applications to collect personal information of users and sell data relating to their internet activity to advertising agencies (Skelton, 2021). Thus, many records of sensitive personal information of the public citizenry were stored in remote computers with a risk of exposure to third parties.

“Big data” is a “combination of structured, semi-structured and unstructured data collected by organizations that can be mined for information and used in machine learning projects, predictive modeling and other advanced analytics applications” (Botelho & Bigelow, 2022).

Big data is often characterized by the three V’s: the large *volume* of data in many environments; the wide *variety* of data types frequently stored in big data systems; and the *velocity* at which much of the data is generated, collected and processed (Botelho & Bigelow, 2022).

Examples of sources of big data include customer databases, documents, emails, medical records, internet clickstream logs, mobile apps, and social networks. Big data is analyzed using data analytics technologies and techniques to harness new information and make strategic decisions. The following examples of this can be identified: Netflix stores information about subscribers including their most-viewed programs. This data can be used by Netflix to analyze what programs need to be newly introduced based on user preferences. Thus, marketing can be targeted. Similarly, banking data can be used to monitor the financial activity of customers. For this purpose, banks are in possession of sensitive data such as the biometrics of customers and other personal information. Healthcare databases contain medical records, patient histories, and other medical details. Such data can be used to track diseases, record patterns of diseases and associated factors and conduct research to develop remedies. In the education sector, educational details can be used to understand learning trends.

“Personal data” is defined as per Article 4 of the General Data Protection Regulation of the European Union (GDPR) as:

any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the *physical, physiological, genetic, mental, economic, cultural or social identity* [emphasis added] of that natural person” (Regulation (EU) 2016/679).

A “breach” is comprehensively defined under Section 2 of the Alabama Data Breach Notification Act of 2018:

The unauthorized acquisition of data in electronic form containing sensitive personally identifying information. Acquisition occurring over a period of time committed by the same entity constitutes one breach. The term does not include any of the following,

- a. Good faith acquisition of sensitive personally identifying information by an employee or agent of a covered entity, unless the information is used for a purpose unrelated to the business or subject to further unauthorized use.
- b. The release of a public record not otherwise subject to confidentiality or nondisclosure requirements.
- c. Any lawful investigative, protective, or intelligence activity of a law enforcement or intelligence agency of the state, or a political subdivision of the state (Ala. Code § 8-38-1 *et seq.*, 2018).

In essence, a data breach results in an “unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information”. (Wang & Wood, 2019). With most data breaches, cybercriminals steal names, email addresses, usernames, passwords, and credit card numbers, these “big data” breaches involve tampering with the personal data of the general public of victim states.

This article focuses on the breaches of big data by states or state-sponsored groups. On many occasions, data in databases of governmental authorities, social media apps, as well as private and public sector companies have been breached, compromising large amounts of people’s personal data records.

There are many examples of massive data breaches alleged to have been committed by states or state-sponsored groups. The Mariotte data theft involved millions of personal records of Chinese citizens (Sanger et al., 2018). The USA indicted four Chinese nationals who were later found to have been sponsored by the Chinese government to hack data of Covid patients’ from US computer systems (Office of Public Affairs, US Department of Justice, 2021) The exposure of personal data of 106 million international travelers to Thailand (Leesa-Nguansuk, 2021) and

the Yahoo breach (Chin, 2022) where over 3 billion records were exposed by alleged Russian hackers are further examples, What is noteworthy about these breaches is, firstly, the massive amount of data breached on a single occasion and secondly, the fact that it was committed by or on behalf of states.

Methodology

The research intends to explain the extent of big data breaches and assess the economic damage incurred by states as a result of big data breaches. The qualitative research method was used to interpret secondary data obtained from websites, journal articles, and reports to understand the current context of the big data breaches. These were used to assess the impact of big data breaches to states, the impact to the economies of these states, the reasons states breach data and the threshold of such big data breaches. The article analyzed primary data sources such as provisions in the Charter of the United Nations (1945), the Tallinn manual, and the EU General Data Protection Regulation (GDPR) to assess the adequacy of these laws in attributing liability for low-threshold data breaches by states or state-sponsored groups.

Limitations

The article excludes the breach of sensitive defense and military data. Instead, it focuses on big data breaches involving the personal data of members of the general public that are extracted from companies, hospitals, governmental authorities, and other institutes in possession of multiple records of data. Cyber-attacks on critical state infrastructure are also excluded. The article restricts itself to big data breaches while also excluding data breaches committed during an armed conflict. Furthermore, it excludes data breaches committed domestically by an individual or a group of individuals against other individuals, domestic state authorities or corporations, unless there are grounds to believe that such persons are acting on behalf of a state.

Analysis

Analysis of extent and purpose of big data breached by states

The battle for mass consumerism of personal data of victim states is propelled by two dominant states: China and the USA. The Chinese Shenzhen Zhenhua Data Information Technology Company, which has ties to the Chinese government, has been amassing a database of personal information on 2.4 million people, including prominent political figures such as Boris Johnson and Narendra Modi and their families, business leaders such as Ratan Tata, US military officials of all ranks, senior diplomats, academics, celebrities, ordinary members of the public, and even gangsters (Zhang, 2020). Furthermore, Table1 below provides an analysis of some examples of such breaches by states.

Table 1: Analysis of few prominent state-sponsored big data breaches, including their extent and purpose:

Example of a data breach incident	Analysis of the cyber data breaches
Equifax data breach 2017	<p>The USA consumer credit agency fell victim to a breach that exposed personal data such as names, social security numbers, dates of birth, addresses, and licenses of 143 million consumers. It was identified as the biggest cyber security disaster of the 21st century. (CRI Group, 2021).</p> <p>It is said that the Chinese government successfully acquired 80% of US adults’ data by 2021 by hacking healthcare companies, smart homes, sensors and 5G networks (Henriquez, 2021).</p>
China Microsoft hack 2021 (BBC News, 2021 July 19)	<p>The cyber-attack on Microsoft Exchange servers affected 30,000 organizations globally. For three months, intruders obtained data in emails, calendars and contacts as well as information from shops, schools, government organizations, etc. This was discovered in January 2021, and investigators initially assumed that the Chinese government merely wanted to steal information in emails. However, the true intention was discovered later. The Chinese Government intended to acquire this information to develop their Artificial Intelligence and to find patterns in human speech and facial recognition. (Temple-Raston, 2021)</p>
Zhenhua data leak by China	<p>Personal data from more than 2 million members of the public was collected by the Chinese big data harvesting company Zhenhua Data Information Technology on behalf of the Chinese government’s intelligence services. (Rahn, 2020)</p> <p>This is an example of a big data breach by a non-state entity on behalf of the state. This database was built to link individuals through network mapping, and in identifying the trends that influence the public.</p>

Big data breaches fail to reach the threshold of an ‘armed attack’ or ‘use of force’

Jus ad bellum (the right to wage war) refers to the instances where a state can resort to war, the use of armed forces, or the use of force in self-defense in accordance with the United Nations Charter of 1945. *Jus in bello* (right in war) relates to the conduct of the parties engaged in armed conflict and falls within the purview of international humanitarian law (International Committee of the Red Cross, 2015). This article is focused on situations falling outside the scope of *jus in bello*.

Murdoch Watney, in ‘Challenges pertaining to cyber war under international law’ (Watney, 2014), stated that international law does not clearly define when state-level cyber intrusion reaches the threshold of an armed attack. If the intrusion amounts to an armed attack, an armed conflict would exist and reaches the threshold for self-defense under Article 51 of the UN Charter (1945). Cyber-attacks on critical infrastructure may qualify as armed attacks and this would depend on case-by-case analysis.

However, Murdoch does not provide the requisites for a cyber-intrusion to qualify as an armed attack or use of force. Murdoch also does not discuss lower-threshold intrusions such as big data breaches. These are left unattributed because they would not reach the threshold of an ‘armed attack’ despite the grave consequences to the economy and sovereignty of victim states of such breaches.

The silence of the international community with regards to attribution of low-intensity attacks paves way for the domination of cyberspace by repeated lower-threshold attacks to amass millions of data of another state. Therefore, attribution and enforcement of stricter data privacy laws are required to uphold digital sovereignty.

Article 2(4) of the UN Charter imposes an obligation on member states to refrain from the use of force against other 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” (UN Charter, 1945).

Article 51 of the UN Charter (1945) provides for when self-defense can be exercised by states: “Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.”

An “armed attack” within the context of international law has been defined by the International Court of Justice (ICJ). “The International Court of Justice’s (ICJ’s) jurisprudence focuses on the “*scale and effects* [emphasis added]” of any particular hostile action directed at a state in order to determine whether it rises to the level of an armed attack” (Nicaragua v. United States of America, 1984[ICJ GL No 70]).

On the 22nd of December 2018, the United Nations General Assembly adopted G.A. Res. 73/266, referring to how international law applies to the use of information and communications technologies by states. Thereafter, an official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by states was submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266 (UN, General Assembly A/76/136). The following is a reference to two examples out of 15 of states that gave their voluntary contributions, in the official compendium in which they declared their stance on the Resolution. These two examples show how states can recognize varying thresholds of “scale and effect”: the USA has adopted a high maximum threshold for scale and effect, equivalent to a bomb attack, while Norway has adopted a broader scope to accommodate lower-threshold breaches.

In UN, General Assembly A/76/136 the statement made by Norway:

A cyber operation may constitute use of force or even an armed attack if its scale and effects are comparable to those of the use of force or an armed attack by conventional means. This must be determined based on a case-by-case assessment having regard to the specific circumstances. A number of factors may be taken into consideration, such as the severity of the consequences (the level of harm inflicted), *immediacy, directness, invasiveness, measurability, military character, State involvement, the nature of the target (such as critical infrastructure)* [emphasis added] and whether this category of action has generally been characterized as the use of force. This list is not exhaustive. (UN, General Assembly A/76/136, p. 70).

In UN, General Assembly A/76/136 the statement made by the United States of America:

Cyber activities may in certain circumstances constitute uses of force within the meaning of Article 2(4) of the UN Charter and customary international law. In determining whether a cyber-activity constitutes a use of force prohibited by Article 2(4) of the UN Charter and customary international law or an armed attack sufficient to trigger a State's inherent right of self-defense, States should consider *the nature and extent of injury or death to persons and the destruction of, or damage to, property* [emphasis added]. Although this is necessarily a case-by-case, fact-specific inquiry, *cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force / armed attack* [emphasis added]. If the physical consequences of a cyber activity result in the kind of *damage that dropping a bomb or firing a missile would* [emphasis added], that cyber activity should equally be considered a use of force / armed attack. (UN, General Assembly A/76/136, p. 70).

Norway adopted “immediacy, directness, invasiveness, measurability, military character, State involvement, the nature of the target (such as critical infrastructure)” as the criteria to decide whether the cyber operation was an armed attack. This means that the ‘scale and effect’ of the attack must be determined through a case-by-case analysis to decide whether an attack qualifies as an armed attack. Similarly, the USA adopted its criteria as “the nature and extent of injury or death to persons and the destruction of, or damage to, property...[or] damage that dropping a bomb or firing a missile would” to decide whether the cyber activity was an armed attack. Thus, I opine that if the scale and effect test is adopted for “big data breaches” it may not be able to satisfy these requirements since a big data breach, by its very nature, does not cause injury, death and destruction to life and property in a manner equivalent to that of dropping of a bomb as opined above by the USA.

This is why Lucas Kello proposed the concept of “unpeace”, denoting highly damaging cyber actions whose non-violent effects do not rise to the level of traditional war and therefore exist in a state of neither war nor peace in other terms a gray zone). Despite being non-violent and not considered acts of war in the traditional sense, the damaging effects on the economy and society at large may be even greater than certain armed attacks. (Kello, 2017).

I agree that a gray zone exists and that big data breaches compromising large amounts of personal data, which is a cyber-intrusion, may not reach the threshold of an armed attack in accordance with the scale and effects theory. However, attribution is needed, firstly because of the economic consequences and secondly because it violates the sovereignty of states.

Analysis of big data breaches and the related economic consequences

This article focuses on state-sponsored big data breaches, excluding those on critical infrastructure or related to an armed conflict. However, irrespective of whether a big data breach is state-sponsored or not, it is first essential to establish whether there is a significant economic impact resulting from a big data breach.

According to the latest data retrieved on the 3rd of March 2024 from Privacy Rights Clearinghouse (PRC), within the time period from 31st December 2021 to 28th September 2023 they received 6,370 data breach notifications and reported that 5,367,033,911 records had been breached (Privacy Rights Clearinghouse, 2020). The Data Breach Report 2023 by the IBM Security and Ponemon Institute (IBM, 2023) stated that the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.

The report analyzed the effect of big data breaches that compromised 11 companies within two years (IBM, 2018). First, the average cost of a data breach of 1 million compromised records is nearly \$40 million dollars; at 50 million records, the estimated total cost of a breach is \$350 million dollars. Second, the average time to detect and contain a mega-breach was 365 days.

The study also compared the cost of data breaches in different industries and regions, finding that data breaches are the costliest in the U.S. (average cost of \$7.91 million) and the Middle East (average cost of \$5.31 million), and least costly in Brazil (average cost of \$1.24 million) and India (average cost of \$1.77 million) (IBM, 2018.).

With regards to the most common type of breach, the report stated that, as of 2018, healthcare organizations had the highest costs associated with data breaches costing them \$408 per lost or stolen record, nearly three times higher than the cross-industry average of \$148 (IBM, 2018.).

It must be noted that there is difficulty in analyzing the exact harm and consequences of a data breach. First, there are hidden costs such as loss of business,

negative impact on business reputation, and employee time spent on recovery, which increase business expenses as well as the difficulty of managing the business. The cost of lost business alone accounted for one-third of the total cost of mega data breaches (IBM, 2018). Secondly, there is no specific data that solely estimates the economic impact of the state-sponsored big data breaches because they are not prosecuted against or labeled as being committed by a state in most cases. Thirdly, there is no consensus on the cost factors for measurement of data breaches, and it generally results in various types of harms and impacts including monetary and economic harm, psychological harm, and social harm as well as indirect and hidden costs. Therefore, it is important to identify to what extent the costs are monetarily assessed. For example, the 'Equifax data breach' cost the company hundreds of millions of dollars but also impacted hundreds of millions of consumers in the US for decades (Soergel. A, 2017).

Big data breaches involve a large amount of data, which is often a consequence of multiple breaches. As shown above, it results in the loss of businesses and economic loss to states. These intrusions may not reach the required threshold of a physical 'armed attack' committed by states under international law. However, repeated breaches by cyber-dominant states make cyberspace vulnerable. It results in damage to business, coupled with other continuing losses. Therefore, I opine that it is necessary to investigate these repeated breaches and formulate mechanisms for attribution.

Big data breaches are a violation of 'state sovereignty'

The land, sea and sky are spaces visible to the naked eye. These regions are demarcated as areas where states exercise their sovereign jurisdiction, and thus a state will have its own defined territory as provided in Article 1 of the Montevideo Convention on the Rights and Duties of States. However, cyberspace is not visible to the human eye but hidden within a system of multiple computer networks.

An intrusion into the territorial water and land of another state may amount to a violation of the sovereignty of the victim state. On the other hand, cyberspace cannot be demarcated into areas subjected to the control of individual states. However, the data stored on servers belonging to a particular state or data owned by a state cannot be tampered with or intruded upon by any other state. I suggest that such an intrusion must also be considered an intrusion upon the sovereign space of the relevant state. Moreover, cyberspace must be considered as a *sui generis* space subject to the principle of sovereign equality of states in Article 2(1) of the UN Charter.

At present, the European Union Agency for Cybersecurity ranks data breaches 8th in the top 15 threats in cyberspace (ENISA, 2020.). States such as China, Russia, North Korea and Iran aspire to dominate this new space (CISA, n.d.). These states

are collecting and compiling the data of citizens in other states to pursue objectives that have not been made clear yet, which is a form of mass consumerism (Geltzer, 2020). The most probable reason may be that amassing this massive amount of personal data assists in analyzing information and trends of states related to both the geopolitical and economic vims of the citizens. This poses a threat to security and impedes the exercise of state sovereignty in cyberspace.

Therefore, I consider it necessary to extend the existing international law concepts such as sovereign equality to cyberspace, while also extending existing legal provisions such as those in the UN Charter, articles on the responsibility of states, and the Tallinn Manual.

Extension of existing legal provisions and principles to the cyber space

The principles of international law and the UN Charter

The state, as a person recognized under international law, should possess the following qualifications: a permanent population; a defined territory; a government; and the capacity to enter into relations with other states as per Article 1 of the Montevideo Convention. This territory may encompass land, air and the sea. In international law, sovereignty is a concept that permits a government to exercise full control over affairs within a territorial or geographical area or limit. As per the 1928 Island of Palmas arbitral award, it defined sovereignty as “the independence in regard to a portion of the globe, it is the right to exercise therein, to the exclusion of any other State, the functions of a State” (II RIAA 829, p. 838). This concept provides the basis for a state to exercise control over its territory. The air, land, and sea of a state are visible, and hence it is easier to ensure that these spaces are within state control. Similarly, I suggest that the cyberspace of a state must also be protected to ensure that no other state can breach the data of its citizenry.

The application of international law, and the UN Charter in particular, to maintain peace and security in cyberspace and to regulate state conduct was accepted in the Resolution adopted by the UN General Assembly on the 23rd of December 2015:

Welcoming the conclusion of the Group of Governmental Experts in its 2013 report that international law, and in particular the Charter of the United Nations, is applicable and essential to *maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful information and communications technology* [emphasis added] environment, that voluntary and non-binding norms, rules and principles of *responsible behavior of States* [emphasis added] in the use of information and communications technologies can reduce risks to international peace, security and stability [emphasis added] and that given the unique attributes of such technologies, additional norms can

be developed over time. (UN Doc. S/RES/2396).

Thus, the principles of sovereignty and sovereign equality as enshrined in Article 2(1) of the UN Charter could be extended to the realm of cyberspace.

Furthermore, Article 2(4) of the UN Charter provides that, states shall refrain 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 Nation and states must not intervene in the realm of state sovereignty in violation of the rules enshrined in the UN Charter. This is also reiterated in customary international law through the principle of non-intervention. In the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in Accordance with the Charter of the United Nations (A/RES/2625(XXV)), the principle of non-intervention is defined as, “No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State.” (UNGA Resolution 2625 (XXV) 1970).

The principles of the Articles on Responsibility of States for Internationally Wrongful Acts 2001

Article 1 of the Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter Articles on State Responsibility) provides that “[e]very internationally wrongful act of a State entails the international responsibility of that State”. Thus, a state is internationally responsible for an intentional wrongful act, which constitutes conduct attributable to the state under international law. If the international law on the principle of state sovereignty is violated, then it could be argued as an internationally wrongful act in breach of state responsibility.

Furthermore, according to Article 2, a breach of international obligation is an internationally wrongful act of a state when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State.” The consequence of such conduct, as per Articles 31 and 34, is the responsible state is required to provide reparation for injury and damage through restitution, compensation and satisfaction.

According to Article 8, “the conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct”. Thus, the acts committed by persons under state control can be considered acts of that particular state and state-sponsored acts committed on behalf of states amount to conduct controlled by states.

Wrongfulness is, however, precluded under Chapter V in cases of consent, self-defense, countermeasure, force majeure, distress, and necessity. Chapter II provides that countermeasures can be taken so long as they are not in violation of human rights or preemptory norms and are proportional to the end perceived.

As a general rule, states must respect the exercise of sovereignty by any state. However, there is no uniform agreement regarding the application of international law to cyberspace, and there are diverse applications of the “scale and effects” test. A cyber operation that satisfies the scale and effects test could be considered a use of force against state sovereignty.

The research paper, ‘Cyber attribution: technical and legal approaches and challenges’ (Tsagourias & Farrell, 2020), advocated for the attribution of cyber-attacks committed against states. This included attacks on critical infrastructure, such as power grids, but failed to address what ought to be done for crimes that do not qualify as an armed attack or a use of force.

However, a cyber-data breach fails to reach the threshold of an armed attack under international law and is excluded from liability. This means that there would not be any state responsibility. That is why I suggest big data breaches by states should be regulated by a tailor-made law.

The Tallinn Manual on the International Law Applicable to Cyber Warfare

The Tallinn Manual on the International Law Applicable to Cyber Warfare (hereinafter the ‘Tallinn Manual’) is a non-binding document that lays out the international law, primarily the *jus ad bellum*, relating to cyber activities. The Tallinn Manual is divided into four parts: Part I deals with general international law and cyberspace. Part II covers specialized regimes of international law and cyberspace. Part III concerns international peace and security and cyber activities, which are mostly drawn from Tallinn 1.0., while Part IV is the rest of Tallinn 1.0, which was the first manual and applies to the law of cyber armed conflict.

As per Rule 1 of the Tallinn Manual 2.0, states may exercise control over cyber infrastructure and activities within its sovereign territory and Rule 2 requires such control to be exercised without prejudice to international obligations. Furthermore, Rule 4 provides that a state must conduct cyber operations in a manner that does not violate the sovereignty of another state. Sovereignty is a principle of customary international law and Article 2(4) of the UN charter recognizes the principle of sovereign equality between states. It can also be said that territorial sovereignty is violated even if the state or the state-sponsored hackers are present in one state and conduct cyber operations against another state. For example, this may include the introduction of malware into the cyber infrastructure of another state. However, low-threshold big data breaches can be considered a violation of sovereignty. Cyber-attacks such as the 2007 Estonian cyber-attacks that reached the threshold of an “armed attack” did not result in Russia being held accountable before the International Court of Justice due to insufficient evidence (McGuinness, 2017). Consequently, it is reasonable to assume that lower-threshold attacks, such as a big data breach, will almost certainly be left unattributed.

Rule 6 imposes the obligation to exercise due diligence. Therefore, when there are adverse consequences to other states, a state must exercise due diligence in not allowing its territory, or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other states. There is a possibility that not all crimes will be subject to this Rule since they need to have “adverse consequences”. It is necessary to prove that a big data breach had “adverse consequences” to establish a state’s failure to uphold its responsibility of due diligence. However, a definition is not provided for the nature of “adverse consequences”.

Attribution of states for breach of international obligations is provided by Rule 14 and a state bears international responsibility for a cyber-related act that is attributable to that state and constitutes a breach of an international legal obligation. Furthermore, Rule 17 provides that actions of non-state actors, such as the CIA or NSA in the United States, who serve on behalf of the state, will be attributable to the state. If cyberagents of a state committed the big data breach, that act will be considered a breach of data by that particular state. In the case of attribution of states for the acts of non-state actors who acted on behalf of the state, the element of “effective control” by the state must be established as per international law. In this regard, mere support or encouragement is insufficient. A party asserting that a state is responsible must satisfy the “effective control” test adopted by the International Court of Justice in *Nicaragua v United States of America*, 1984 (ICJ GL No 70) or, at least, “overall control” as defined by the International Criminal Tribunal for the Former Yugoslavia in *Prosecutor v Tadić*, 1999 (IT-94-1-AR72). This control test is included in Rule 17 of the Tallinn manual. In the cyber realm, it can be considered that non-state actors are acting on behalf of a state when the state provides the cyber tools, identifies the targets, selects the date for the cyber operation etc. However, the fact that the individual/s were state-sponsored will be challenging to prove and the perpetrator state may be discharged of liability as the rules require a high threshold of proof. For example, if the Chinese government deploys private companies to amass big data for the state, that connection to the state and the state’s effective control over the private companies require proof. Cyber breaches committed by private groups under state sponsorship is difficult to establish because the threshold requirement is to prove “control” by the state.

In Rule 19, wrongfulness of the act is precluded in instances of self-defense, countermeasures, consent, necessity, force-majeure, and distress. A state can respond to a non-cyber violation with a cyber-countermeasure, and to a cyber-violation with a non-cyber countermeasure.

Rule 34 provides for the applicability of international human rights law and, therefore, the principles of customary international human rights law are applicable. With regards to the right to privacy, there is consensus among experts that individuals’

private communication should not be inspected by another human, but there is no consensus regarding whether it can be inspected by non-human entities (Jensen, 2017, p.759). There is consensus that the right to privacy also includes the protection of an individual's personal data. However, "personal data" is not well-defined in law. Metadata is considered personal data if it is linked to an individual and life (Jensen, 2017, p.759). As per Rule 36, in cyber activities, states must respect international human rights of individuals and protect individuals from abuse by third parties. Thus, the protection of the data subjects is a duty imposed on states.

However, to date, there is no agreement among experts as to whether cyber operations that do not cause physical consequences or a loss of functionality would qualify as a violation of sovereignty. This lack of consensus poses a challenge to attribution, especially for the big data breaches that tend not to satisfy the "scale and effect" test to assess whether the attack surpassed the requisite threshold for an armed attack or to constitute a use of force.

In the article titled "International Criminal Tribunal for Cyberspace" (ICTC) by Judge Stein Schjolberg (2012), the judge proposed establishing a new tribunal for cyberspace, an international charter, and a new enforcement mechanism such as a Global Virtual Taskforce. I too consider that it is vital for states to reach a consensus in the application of international law and the regulation of state conduct in cyberspace.

Data breaches and the right of self-defense of states

Article 51 of the UN Charter provides that "Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs". This means that self-defense is an available option if there is an armed attack. Moreover, threatened states can exercise force in the case of an imminent attack so long as the military action taken is proportionate (UN peacebuilding, 2004).

A big data breach does not generally qualify as an armed attack because a cyber data breach does not *per se* have violent consequences like a bomb explosion. Therefore, an attack against critical infrastructure might qualify under this category, but not the crime of big data breach. This means that the right to self-defense is not available in the absence of an armed attack. This is because espionage and other low-threshold cyber operations, such as installing malware to obtain information or monitoring, do not reach the above stated threshold or constitute a use of force in violation of Article 2(4) of the Charter. Thus, the existing laws do not sufficiently address cybercrimes.

Another issue is that it refers to an attack committed by one state against another state. Therefore, if a country deploys private individuals to commit the crime and the victim state fails to establish "effective control" by the controlling state, then, that state would be barred from an act of self-defense. This gap in international law

paves way for states to use cyberspace for intelligence and surveillance.

The right to spy recognized in Chapter VII of Resolution 2396 adopted by UN Security Council (UN Doc. S/RES/2396) guides member states to “intensify and accelerate” peacetime intelligence collection, and “to develop systems to collect biometric data, which include fingerprints, photographs, facial recognition, and other relevant identifying biometric data”. It also provided guidelines for states to collect and process passenger information, develop databases on suspected groups, and increase cooperation with information and communication technology companies to collect digital records and share them through bilateral and multilateral arrangements. Does this signify that surveillance and spying are rights of states? Spying has been performed since ancient times to observe the behavior of the enemy in the interests of national security. However, spying for the private ends of rulers for dictatorship or commissioning an internationally wrongful act is an abuse of that right (Lubin, 2018). This will be a violation of the right to privacy as stated in Rule 34 and Rule 36 of the Tallinn Manual, which provide that states have the duty to protect the rights of its people. Therefore, the use of personal data for such other purposes may not qualify as an act committed in the national interest. For example, the use of big data by China to improve Artificial Intelligence or a breach of data by app companies to 3rd party states may not be for national security but rather an act for political domination.

Yet can a state defend its act of peacetime information collection from another state in response to an imminent threat? In such an instance, states that collected personal data must prove that it was a defense against imminent threats and must also establish that the act of intrusion was proportional. Data breaches and mass consumerism of personal data may not satisfy these requirements, because of the inability to prove imminence and proportionality. This is why I opine that an international law on cyberspace must be formulated to ensure regulated state conduct in cyberspace.

Challenges in the application of existing international law

The lack of hard law for regulation of the international law in cyberspace

International law governing international cyberspace are soft laws. *Despite the existence of principles such as state sovereignty, and due diligence, there is an inability to extend the existing international law for the attribution of big data breaches. This is because laws such as the Tallinn Manual and the 2001 Articles on State Responsibility are soft laws.*

Apart from the UN Charter (1945), general principles of law and state practice, the laws in the Tallinn Manual and the Articles for the Responsibility of States for Internationally Wrongful Conduct are not binding. Thus, attribution is challenging

since the existing intensity threshold for an armed attack may not be reached by most attacks that are nevertheless of great impact on the victim states' economy, citizens, and sovereignty, and may be left unattributed. Regulation would then depend on the domestic law frameworks but those are also fragmented and not uniform. Thus, international regulation is truly challenging due to the lack of hard law, specifically for cybercrimes.

The ambiguities and the lack of consensus in the law

Harmonized laws will assist evidence-gathering and enforcement. The Tallinn manual is non-binding, but there is a lack of consensus. The existing laws have ambiguities as pointed out under Table 2 of the article and must be clarified to ensure the proper regulation of states' conduct in cyberspace. This can be initiated by the UN which has the ability to attract state cooperation in promoting peace in cyberspace.

The *sui generis* nature of cyberspace and crimes such as intrusion for big data breaches must be attributed despite ambiguities and, in the absence of laws for attribution, because breaches intrude on sovereignty, the economies of victim states are affected and the attacks may be repeatedly committed upon the victim state.

Lack of sufficient expertise, funding and calls for global mutual assistance efforts

Technical capabilities are important for law enforcement because investigators seated behind computer devices would be investigating and tracing criminals. Thus, for the effective application of a global data protection regime, all states need capacity for technology expertise and funds. This is because when tracing criminals who are intercepted via computer networks in a different state, the chain of law enforcement will break if some states lack sufficient technology to quickly retrieve and collect cyber data traces left by criminals in these networks. Therefore, developing and underdeveloped states require international assistance.

A cyber data breach is a transnational crime, and data is transmitted via multiple computer networks and intercepted by computers from different jurisdictions. When locating criminals, law enforcement would require assistance from several states. Thus, it is a transnational crime where the crime occurs in one state and the criminal may be residing in another state. Therefore, a breach of data of one state by another state involves multiple national data protection regulations.

The perpetrator of cybercrimes is difficult to locate

Relative to other spaces, one of the major challenges in cyberspace is in locating the perpetrator, and it requires joint expertise from different states to locate the crime and the perpetrator. The computer may be found, but identifying the criminal who was controlling that computer requires another investigation. Alternatively,

they may have used fake identification. Thus, crime investigation in cyberspace is challenging since criminals can attack computers in one state while residing in another. The Internet Protocol (IP) address is used for identification, but the use of proxy servers and other methods to hide the identity makes attribution challenging. This is why Article 25 of the Council of Europe Convention on Cybercrime, the Budapest Convention (Council of Europe, 2001), encourages domestic cybercrime laws to incorporate mutual assistance laws and extradition laws.

Difficulty in valuing the consequences of a data breach

Article 31 of the 2001 Articles on Responsibility of States for Internationally Wrongful Acts provides guidelines to make full reparations for injury, including any damage, whether material or moral, for acts in violation of international obligations. This can be in the form of restitution (Article 35), compensation (Article 36) or, if the two aforementioned remedies fail, by satisfaction (Article 37). Yet it is difficult to quantify the damages because there may have been breaches of data regulation laws in several states prior to the final target state being reached and because there are no cost factors for measuring data breaches due to the monetary and economic harm, psychological harm, and hidden costs and other issues under the preceding topic on economic consequences.

Recommendations for attribution under international law

Global cooperation and the common but differentiated principle

The controlling, collection and retention of personal data, is insufficient to protect personal privacy because “big data enables new, non-obvious, unexpectedly powerful uses of data” (Executive Office of the President, 2014, p. 54). The USA claimed that it has the capacity to locate its cyber adversaries and hold them accountable (Macak, 2016, p. 138). Canada noted that it has systems to localize cyber intrusions, including state-sponsored breaches (Macak, 2016, p. 138).

States that are advanced in cyber activities may have the necessary technology to localize the perpetrators, but global cooperation is required for the purpose of investigation. This is because data breaches occur through multiple servers and may originate from computers in any state. Developing states and states that lack frameworks for data protection will require the assistance of other states in locating criminals. Countries should consider the implications of their actions and ensure that laws and policies are not made in a manner that hinders the mutual assistance in investigation and law enforcement.

Extending the existing legal framework

States have international obligations and must not use their territories to commit crimes against another state. In the absence of a codified law such as the United Nations Convention on the Law of Sea (UNCLOS) adopted in 1982, cyberspace can nevertheless be governed, to a certain extent, by international law by modification of the existing international law to suit cyberspace. There are certain principles that can be extended to apply in cyberspace as well and can be used to attribute states.

Customary international law and the sliding scale theory

“The sliding scale theory” introduced by Professor Frederic Kirgis provides that the “requirement for *opinio juris* increases as the evidence of State practice decreases” (Shackelford et al., 2016, p. 5). Strong state practice or *opinio juris* can give rise to international obligations. Since technologies develop rapidly before widespread state practice can emerge, *opinio juris* can create international obligations. This is evident from the increase in domestic legislation concerning cyberspace for data protection or even from international conventions such as the Budapest Convention, and regional treaties such as the EU General Data Protection Regulation (GDPR), African Union Convention on Cybersecurity and personal Data Protection.

Due diligence norms

Principles in existing case law such as the duty to warn, the no-harm principle, and the principle of non-intervention (Shackelford et al., 2016, p. 8) can be used since there is no hard law applicable to these lower-threshold crimes. These are accepted principles applicable to crimes of big data breaches because they have widespread usage in state practice.

The Corfu Channel Case or United Kingdom v Albania 1949, (ICJ GL No. 1) established that a state has a duty to warn other states of known or foreseeable harms. Therefore, it is necessary to prove that a state had knowledge of the crimes committed within that particular state; for example, that the computer labs used to perpetrate the crime were sponsored by the state.

The Trail Smelter Arbitration Case between the USA and Canada (U.N. Rep. Int'l Arb. Awards 1941)) introduced the due diligence norm of ‘no-harm’. The Tallinn Manual also adopts the no-harm principle. The state has the duty to ensure that there is no threat to other states from the cyber activities conducted within their territories, and this principle is relevant to big data breaches carried out by states or those sponsored by states.

States must not intervene in the affairs of other states. The Tallinn Manual and the Articles on Responsibility of States for Internationally Wrongful Acts,

encompass the concepts of sovereignty and non-intervention as established in the Nicaragua case (1984).

Thus, it is high time that cyber-sovereignty is ensured to attribute those that use cyberattacks in the form of a lower-threshold intervention into another state's database with intent to obtain data. These result in economic downfall, influence state policies and threaten the free use of cyberspace by victim states. Thus, a regime to govern these lower-threshold attacks is needed.

A big data breach does not amount to a use of force or armed attack but it is still an intervention upon the territory of another state resulting in adverse economic consequences and theft of data. This data can be manipulated to victimize the state and exert political pressure to influence domestic matters. Therefore, the states through which the cyber data breach occurred or was transmitted have a duty to exercise due diligence and inform or warn the victim-state.

The enactment of a tailor-made treaty and courts

The president of Microsoft, Brad Smith, proposed enacting a Digital Geneva Convention (Smith, 2018). Judge Stein Schjolberg proposed establishing a new tribunal for cyberspace, a new Charter, and a new enforcement mechanism such as a Global Virtual Taskforce (Schjolberg, 2012).

Building on the foundation of the Tallinn Manual, a set of binding laws for cybercrimes would be a perfect solution. However, it is challenging to harness global participation, and especially difficult to ensure the compliance of superpowers. For example, to date, the USA has refused to ratify the Rome Statute of the International Criminal Court. Thus, attribution for lower-threshold interventions in cyberspace by data theft is challenging.

A tailor-made law will, however, serve as a model law for all states. This model law can include the laws for cyberspace governance in times of peace, such as the theft of personal data. A treaty similar to the UNCLOS, which is the result of international consensus and preferably without reservations, can resolve the interpretative ambiguities identified previously.

The International Court of Justice can serve as the court with jurisdiction and can consist of judges specializing in cyber law. A UN-led initiative to frame laws is required for attribution in this space. Such an initiative can be justified as an ideal mechanism to tailor a law because of the success in formulating the UNCLOS for the regulation of state conduct relating to the seas. The UN formulated the UNCLOS, a convention that, despite taking several years to formulate, enshrined core principles of state practice, was widely accepted by many states, and to date is the core law that is adopted in matters relating to the sea. Therefore, the UN must take the initiative to regulate cyberspace and ensure peace and harmony by formulating a law that can be widely accepted internationally.

Creation of a domestic mechanisms in line with international standards

Create public awareness regarding safe use of computer and online platforms and the associated rights and remedies

Sufficient public awareness is needed on how to assert one's rights to data protection and privacy. For this purpose, the use of popular media such as newspapers, TV, and social media, as well as education through school ICT curricula, is necessary. ICT and cybersecurity must be included, at least as auxiliary components, in university curricula.

Data breach notification adopting the USA model

In the event of a data breach, the USA has data breach notification laws where notice must be provided to the affected individuals. For the purposes of breach notification, personal information includes a person's name, credit card number, financial information, license, biometric data, and medical information (World Law Group, 2013). USA Companies in Insurance are also subject to data breach notification requirements for breaches of data in their possession. For example, the State Insurance Departments have regulations imposing breach notification requirements and are required to provide notice to the state in the event of a breach as per the Financial Services Modernization Act of 1999 or the Gramm-Leach-Bliley Act (15 U.S.C. § 6801).

The notice has to be given "as soon as practicable and without unreasonable delay following discovery of the breach" (world law group, 2013, p. 181). Florida Information Protection Act of 2014 requires notification to be made within 30 days of discovering the breach. If not, the possessor of the information has to incur a fine and pay damages (Fla. Stat. § 501.171).

Civil action against companies that fail to maintain adequate data security systems can be instituted as in Fed. Trade Comm'n v. Wyndham Worldwide Corp. (799 F.3d 236 (3d Cir. 2015)). States also need to include this mechanism for all companies, businesses, and state authorities in possession of public personal data.

Recruiting and training experts to reduce dependence on foreign expertise

Retaining technology, computer science, and IT graduates by providing attractive salaries enhances local expertise. Employment and career opportunities in cybersecurity and data protection must be increased, especially in police, ICT-related departments, and other regulatory bodies, to assist data protection efforts.

Data protection response teams

Each department and entity in possession of public data, such as hotels, businesses, airports, hospitals, government authorities etc., must ensure sufficient precautions have been taken by their IT departments. For this, cybersecurity officers must be recruited to analyze security breaches and perform computer audits.

Adopting EU General Data Protection Regulation (GDPR) standards through law

Having different compliance requirements across different nations makes enforcement of the law against transboundary crime challenging. In the USA, each state has a different data protection law and in the absence of standardized law within a particular state it is difficult to enforce the law.

While international courts and laws must regulate state conduct internationally, as argued under Section 9, states must also adopt uniform standards domestically to regulate cyberspace. At present, many states are adopting the standards set by the GDPR to enact domestic data protection laws.

The GDPR includes key areas such as establishing lawful purposes for data processing (Articles 5 and 6), need for data subjects' voluntarily consent (Article 7), right to erase (Article 17), right of access (Article 15), right to rectification (Article 16), and the right to object (Article 21). In addition, automated messages must be provided according to the new law. The data controller has a duty to give information to the data subject and appoint a data protection body.

Auditing computer databases and performing impact assessments

New regulations must be enacted for the protection of critical information infrastructure, such as hospitals, businesses, and government authorities. In the USA, insurance companies are regulated by regulations to protect healthcare and other customers, and these entities must submit their audits and impact reports of security checks, details on threat information, responses for mitigation and report imposition of liabilities for inaction as provided in the Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) and Gramm-Leach-Bliley Act.

Structuring a regulatory mechanism with new authorities and agencies

For the purpose of regulation, I suggest that states formulate a national cyber security strategy and cyber security agency. An example of a model I prepared is provided in Figure 1. The cyber-security agency can be established as the main control center. This agency must be empowered with an adequate workforce. To increase its efficiency, its powers can be delegated to new authorities, as proposed in the organizational map depicted in figure 1. Chosen centers that have a massive amount of public data, such as hospitals supermarkets, departments of state authorities, companies etc., must be regulated by a critical infrastructure regulator. National cyber security operation centers should be established to act in cases of data breaches and act as data breach notification centers. Subsequently, to ensure efficiency, regional bodies can be established in each district for the above units to detect and regulate the tasks at a regional level.

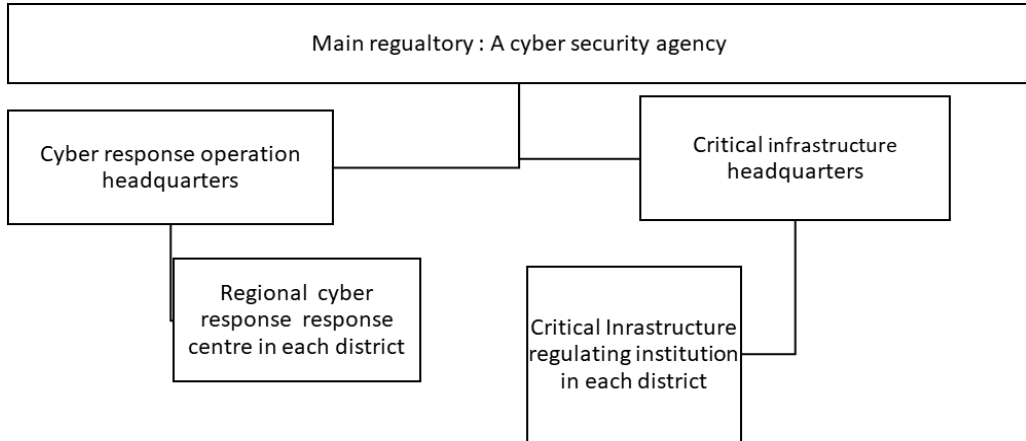


Figure 1: Conceptual framework to delegate tasks to regional centers

Conclusion

States exercise control within their demarcated territories in accordance with international law. Respect for the sovereign equality of states is accepted internationally, and from it spring the principle on the prohibition of the use of force and the principle of non-intervention. The principle of sovereignty must be extended to cyberspace. A big data breach must be considered a wrongful act that gives rise to state responsibility. The issue with cyber data breaches of big data is that they are not considered to constitute a use of force according to the generally accepted “scale and effect” test and would not be attributed internationally. However, this results in many lower-threshold crimes being repeatedly committed by states without attribution. Thus, tailor-made laws with broad state acceptance must be enacted to govern this space.

Conflict of Interest

The author has no conflict of interest to declare.

References

- BBC News. (2021, July 19). China accused of cyber-attack on Microsoft Exchange servers. *BBC News*. <https://www.bbc.co.uk/news/world-asia-china-57889981>.amp
- Botelho, B., & Bigelow, S. J. (2022, January). What is Big Data and Why is it Important? *SearchDataManagement*.<https://www.techtarget.com/searchdatamanagement/definition/big-data>
- Chin, K. (2022, August 5). Biggest Data Breaches in US History. *UpGuard*. <https://www.upguard.com/blog/biggest-data-breaches-us>

- CISA, (n.d.). Nation state cyber actors, *Cybersecurity and Infrastructure Security Agency*. <https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors>
- Council of Europe, Convention on Cybercrime, Council of Europe, 23 November 2001, <https://www.refworld.org/legal/agreements/coe/2001/en/90189>
- Corfu Channel, United Kingdom v Albania, ICJ GL No 1, [1949] ICJ Rep 4, ICGJ 199 (ICJ 1949), United Nations International Court of Justice 9th April 1949,
- CRI Group, (2021). Equifax data breach is a security disaster: the biggest security disaster of the 21st century. *Lexology*. <https://www.lexology.com/library/detail.aspx?g=3953cae4-2ec4-4278-9b07f904ccc3f9f2>
- Data Breach Notification Act of 2018, § 8-38-1 et seq, (2018).
- ENISA. (2020). Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. *ENISA*. <https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020>
- Executive Office of the President of the United States. (May 2014). Big Data: Seizing Opportunities, Preserving Values, *Whitehouse government* www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
- Financial Services Modernization Act of 1999 (15 U.S.C. § 6801) 1999
- Florida Information Protection Act of 2014(Fla. Stat. § 501.171). 2014
- Fruhlinger, J. (2022, August 31). Stuxnet explained: The first known cyberweapon. *CSO Online*. <https://www.csoononline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html>
- FTC v. Wyndham Worldwide Corp 799 F.3d 236 (3d Cir. 2015) US Court of Appeal, 24th August 2015
- Geltzer, J. (2020, April 29). Weapons of Mass Consumerism: Why China Wants Your Personal Information. *Just Security*. <https://www.justsecurity.org/62187/weapons-mass-consumerism-china-personal-information>
- Henriquez M. (2021, February 2) China has stolen the personal data of 80% of American adults. *securitymagazine*. <https://www.securitymagazine.com/articles/94493-china-has-stolen-the-personal-data-of-80-of-american-adults>
- Health Insurance Portability and Accountability Act of 1996 (Pub. L. 104-191) 1996
- IBM. (2023). Cost of a data breach 2023. *IBM*. <https://www.ibm.com/reports/data-breach>
- IBM. (2018.). IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses. *IBM*. <https://www.prnewswire.com/news-releases/ibm-study-hidden-costs-of-data-breaches-increase-expenses-for-businesses-300679124.html>
- International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, Supplement No. 10 (A/56/10), chp.IV.E.1, November 2001, <https://www.refworld.org/legal/otherinstr/ilc/2001/en/20951>,

- International cyber law: interactive toolkit. (2021, September 17). Cyberattacks against Estonia (2007) - International cyber law: interactive toolkit. *International Cyber Law: Interactive Toolkit*. [https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_\(2007\)](https://cyberlaw.ccdcoe.org/wiki/Cyber_attacks_against_Estonia_(2007))
- International Committee of the Red Cross. (2015, January 22). What are jus ad bellum and jus in bello?. International Committee of the Red Cross. <https://www.icrc.org/en/document/what-are-jus-ad-bellum-and-jus-bello0%EF%BB%BF>
- International cyber law: interactive toolkit. (2021, September 17). Georgia-Russia conflict (2008). *International cyber law: interactive toolkit*. [https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_\(2008\)](https://cyberlaw.ccdcoe.org/wiki/Georgia-Russia_conflict_(2008))
- Island of Palmas Case (or Miangas), United States v Netherlands, Award, (1928) II RIAA 829, ICGJ 392 Permanent Court of Arbitration, 4th April 1928,
- Jensen, E. T. (2017, March 13). The Tallinn Manual 2.0: Highlights and Insights. *SSRN*. <https://ssrn.com/abstract=2932110>
- Kello, L. (2017). The Virtual Weapon and International Order. *Yale University Press*. <https://yalebooks.yale.edu/9780300234497/the-virtual-weapon-and-international-order>
- Leesa-Nguansuk, S. (2021, September 22). Personal data of 106m travelers exposed online. *bangkokpost*. <https://www.bangkokpost.com/business/2185963/personal-data-of-106m-travellers-exposed-online/>
- Lubin, A. (2018). Cyber law and espionage law as communicating vessels. *2018 10th International Conference on Cyber Conflict* <https://doi.org/10.23919/cycon.2018.8405018>
- Macak, K. (2016, May 1). Is the international law of cyber security in crisis? *IEEE Conference Publication*. <https://ieeexplore.ieee.org/document/7529431/>
- McGuinness, D. (2017, April 27). How a cyber attack transformed Estonia. *BBC News*. <https://www.bbc.com/news/39655415>
- Military and Paramilitary Activities in and against Nicaragua, Nicaragua v United States, ICJ GL No 70, [1984] ICJ Rep 392, ICGJ 111 (ICJ 1984), United Nations International Court of Justice 26th November 1984
- Montevideo convention on the rights and duties of states. 1933
- Moore, H., & Roberts, D. (2017, July 14). AP Twitter hack causes panic on Wall Street and sends Dow plunging. *The Guardian*. <https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall>
- Office of Public Affairs, US Department of Justice (2021, July 19) Four Chinese Nationals Working with the Ministry of State Security. *US Department of Justice* <https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion>
- Prosecutor v. Dusko Tadic (Appeal Judgement), IT-94-1-A, International Criminal Tribunal for the former Yugoslavia (ICTY), 15 July 1999

- Privacy Rights Clearinghouse. (2020). Data Breaches *Privacy Rights Clearinghouse*. <https://privacyrights.org/data-breaches>
- Rahn, W. (2020, September 29). Data leak exposes China's new "hybrid warfare. *dw.com*. <https://www.dw.com/en/zhenhua-data-leak-exposes-chinas-new-hybrid-warfare/a-55083540>
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (OJ L 119 04.05.2016, p. 1, ELI: <http://data.europa.eu/eli/reg/2016/679/oj>)
- Schjolberg, S. (2012). Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes An International Criminal Tribunal for Cyberspace (ICTC) Prosecution for the Tribunal Police investigation for the Tribunal. EastWest Institute (EWI) Cybercrime Legal Working Group. <https://www.cybercrimelaw.net/documents/ICTC.pdf>
- Sanger, D. E., Perlroth, N., Thrush, G., & Rappeport, A. (2018, December 12). Marriott Data Breach is traced to Chinese hackers as U.S. readies crackdown on Beijing. *The New York Times*. <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html>
- Shackelford, S., Russell, S. D., & Kuehn, A. (2016). Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors. *Chicago Journal of International Law*, 17(1), 1. <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil>
- Skelton, S. K. (2021, February 9). Facebook sued for data-sharing practices with third parties. *ComputerWeekly*., <https://www.computerweekly.com/news/252496091/Facebook-sued-for-data-sharing-practices-with-thirdparties#:~:text=Jukes%20claims%20that%20between%20November>.
- Smith, B. (2018, May 15). The need for a Digital Geneva Convention. *Microsoft*. <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/>
- Soergel, A. (2017, September 8). Equifax breach could have 'decades of impact'. *US news*. <https://www.usnews.com/news/articles/2017-09-08/equifax-breach-could-have-decades-of-impact-onconsumers>
- Tallinn Manual on the International Law Applicable to Cyber Warfare <https://lib.ugent.be/en/catalog/rug01:002327127>
- Temple-Raston, D. (2021b, August 26). China's Microsoft Hack May Have Had A Bigger Purpose Than Just Spying. *NPR*. <https://www.npr.org/2021/08/26/1013501080/chinas-microsoft-hack-may-have-had-a-bigger-purpose-than-just-spying>

- Trail Smelter Arbitration Case (United States Vs Canada) 1941, U.N. Rep. Int'l Arb. Awards 1905 (1941) https://legal.un.org/riaa/cases/vol_III/1905-1982.pdf
- Tsagourias, N., & Farrell, M. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law*, 31(3). <https://doi.org/10.1093/ejil/chaa057>
- UN peacebuilding, (2004.). A more secure world Our shared responsibility Report of the High-level Panel on Threats, Challenges and Change, *UN Peacebuilding*. <https://www.un.org/peacebuilding/content/more-secure-world-our-shared-responsibility-%E2%80%93-report-high-level-panel-threats-challenges-and>
- UN Security Council Resolution 2396, Threats to International Peace and Security Caused by Terrorist Acts, UN Doc. S/RES/2396. 21 December 2017.
- UN Security Council Resolution 2396, Threats to International Peace and Security Caused by Terrorist Acts, UN Doc. S/RES/2396. 21 December 2017.
- 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, A/RES/2625(XXV), 24 October 1970, <https://www.refworld.org/legal/resolution/unga/1970/en/19494>
- United Nations. (1945, June 26). UN Charter. United Nations. <https://www.un.org/en/about-us/un-charter>
- UN General Assembly. Resolution 73/266. Advancing responsible State behaviour in cyberspace in the context of international security A/RES/73/266. 18 December 2013
- UN, General Assembly Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security established pursuant to General Assembly resolution 73/266. A/76/136 13th July 2021 <https://digitallibrary.un.org/record/3933543?ln=en>
- Wang, P., & Wood, D. (2019). Economic Costs and Impacts of Business Data Breaches. *Issues in Information Systems*, 20(2), 162–171. https://iacis.org/iis/2019/2_iis_2019_162-171.pdf
- Watney M (2014, April 1) Challenges pertaining to cyber war under international law. *IEEE Conference Publication* <https://ieeexplore.ieee.org/iel7/6908325/6913961/06913962.pdf>
- World law group.(2013).Global Guide to Data Breach Notifications. world law group. <https://www.theworldlawgroup.com/news/2016-global-data-breach-guide>
- Zhang, A. (2020, September 18). China Data Leak Points to Massive Global Collection Effort. *VOA*. <https://www.voanews.com/east-asia-pacific/voa-news-china/china-data-leak-points-massive-global-collection-effort>