UNIVERSITY OF NAIROBI

SCHOOL OF LAW

BIT WARS: DATA PROTECTION AND DIGITAL IDENTITIES IN AN ERA OF GLOBAL CYBERWARFARE.

A THESIS SUBMITTED TO THE UNIVERSITY OF NAIROBI SCHOOL OF LAW IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF MASTER OF LAWS (LL. M)

BY

MANG'ARE GLENN ONG'UTI
G62/38286/2020

SUPERVISOR
DR. KENNETH MUTUMA

OCTOBER 2021

DECLARATION

I, **MANG'ARE GLENN ONG'UTI**, do hereby declare that this thesis is my original work and has not been submitted, and it is not currently being submitted in any other university.

MANG'ARE GLENN ONG'UTI

14th October 2021

This Research Paper has been submitted for examination with my approval as University Supervisor.

……

DR. KENNETH MUTUMA

Date **14th October 2021**

DEDICATION

To my little Zahlia,

Should I ever accuse you of ignoring me, just remind me that in 2021 you raucously yawped and bawled for my attention, but I needed 'just another 5 minutes' to finish this paper…

To Naomi…

May the God of Enoch, Elijah and Christ see you walk into heaven.

To the other ladies in my life

Ethel…
Nina…
Vera…
Tracy…

On whose backs I have been carried throughout my academic life. Of what strength is a man if he must be carried by a woman? I lay my achievements at your feet.

To Seth…

The total sum of all I want to be.

ACKNOWLEDGEMENTS

My Supervisor, Dr. Mutuma…

In a world full of people and things that I do not understand, I am glad to have met you who stands out for fitting the rare mould of being an incomprehensibly good guy…

May God bless you.

May everyone get the pleasure of working with you (or someone like you) at least once in their life.

TABLE OF CONTENTS

ACRONYMS

AP I	Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
AP II	Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
CoE	Council of Europe
eID	Electronic ID
EU	European Union
GDPR	General Data Protection Regulation
ICRC	International Committee of the Red Cross
IHL	International Humanitarian Law.
NSAs	Non-State Actors
OECD	Organisation for Economic Co-operation and Development.
OEWG	Open Ended Working Group
UDHR	Universal Declaration of Human rights
UN	United Nations
UNGA	United Nations General Assembly
UNGGE	United Nations Group of Governmental Experts.
WMD	Weapons of Mass Destruction

LIST OF CASES

Kenya

1. Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR

Spain

2. Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre

ECHR

3. Bărbulescu v. Romania (Application no. 61496/08)

LIST OF STATUTES

International

1. Geneva Conventions (1 to 4)
2. Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.
3. Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.
4. Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Convention 108)
5. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention)
6. Charter of Fundamental Rights of the European Union
7. Rome Statute
8. Hague Convention of 1899

Europe

9. The General Data Protection Regulation 2016/679 (GDPR)

Kenya

10. Constitution of Kenya, 2010
11. Data Protection Act, 2019
12. Registration of Persons (National Integrated Identity Management System) Rules, 2020.

1. BACKGROUND

Cyberwarfare has no globally accepted definition, especially in the perspective of IHL. Colloquially, it is used in very many different aspects, including cyber-attacks, cyber espionage and cyber aggression. It has been defined as 'an extension of policy by actions in cyberspace by state actors (or by non-state actors with significant state direction or support) that constitute a serious threat to another state's security, or an action of the same nature taken in response to a serious threat to a state's security (actual or perceived)'[1]. The devastation that can be caused during cyberwarfare is bound to compound as nation states become more and more reliant on technology and data to deliver critical services. We can presume that these nation states are consistently preparing offensive and defensive cyber-capabilities with this in mind.

This study is an exercise in a hypothetical question. It seeks to propose what the most destructive action in cyberwarfare would be. It then seeks to figure out whether cyberwarfare is overseen by the international community. It is an attempt to understand whether the importance of critical and personal data is known to the IHL community and whether there has been any attempt to guard against its abuse during the ubiquitous preparation for war, and during warfare itself.

1.1. Statement of Problem

In IHL, the principle of distinction is one of the major principles governing which objects can be attacked. This principle states that parties to a conflict must consistently distinguish combatants and military targets on the one hand from civilian persons and objects on the other.[2] It requires that militant combatants distinguish between civilian objects and military

[1] James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 2

[2] Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law* (Edward Elgar 2013) 70

objectives.[3] It is so well established that it is considered as one of the *jus cogens*.[4] The protection placed on non-combatants is meant to ensure that the adverse effects of warfare are not meted on them.

Advances in Information Technology have introduced changes in the way civilian and military resources may be viewed. More importantly, it has introduced a level of anonymity that has not yet been experienced in potential warfare. This severely complicates the traditional concepts of attribution and makes it extremely difficult to answer the question 'whodunit?'.[5] Conversations on cyberwarfare and its interaction with IHL have so far focused on how to best translate, transfer, and apply current *jus ad bellum* and *jus in bello* rules into cyberspace.[6] Consequently, it focuses on military command structures and critical civilian systems and the hardware and software in the cyber arena. So far, there has been little, if any, consideration given to the third component of computer systems. Data! This is despite data currently being the fuel that runs the modern economy and completely ignores the fact that it has both civilian and military applications.

The result is a massive gap that has not yet been properly considered, neither academically nor practically. The third, and most valuable limb of modern computer systems, might not have specific protection in times of cyberwarfare. As modern countries measure each other's military might in cyberspace, what would be the impact, on data protection, of an attack in this

[3] Article 52, AP I. Additionally, the principle of distinction is applied in the distinction between civilians and combatants. This is the main perspective of its application.

[4] Jean-Marie Henckaerts and others (eds), *Customary International Humanitarian Law* (Cambridge University Press 2005) 25

[5] Neil C. Rowe, 'The Attribution of Cyber Warfare' in James A. Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 61

[6] Michael N. Schmitt and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017) 375

sphere? Furthermore, what would be the impact should this attack happen on critical data, for example, digital identities?

1.2. Statement of Objective

The specific objectives of this study include:

1. To find out whether data protection during a situation of cyberwarfare has been regulated by IHL.
2. To examine the current IHL arguments and seek to understand whether the current transpositional approach of encompassing the traditional IHL mechanisms into cyberwarfare will suffice for data protection scenarios.
3. To propose potential solutions that can be utilized by the international community to design *sui generis* protective measures. Such measures should be modelled to fit the problem, rather than the problem being bent to fit into the current protections.
4. Make recommendations on what the IHL practitioners can consider as a potential solution for this lacuna.

On a general level, I hope to draw attention to the massive disruptive potential that exists in a situation where due to cyberwarfare, personal data is stolen and exploited by a belligerent nation state or those it sponsors. The recent dramatic focus on data protection within the civilian sphere should be an indicator of just how devastating the impact would be should military action be directed at achieving the same nefarious goals.

1.3. Research Questions

Nascent and growing fields always throw researchers curveballs. This is especially when they create lacunas that are capable of being answered only by asking more questions. This is one of those, as yet, practically untested international legal issues.

This research will attempt to get to the bottom of the following questions:

1. Is there any protection provided for ‘critical civilian data’ in cases of cyber armed conflict?
2. Is the current transpositional approach of expecting the same rules of armed conflict to apply to cyber armed conflict sufficient for data protection scenarios?
3. Does the world need a *sui generis* protection regime for cyber warfare, and in particular for the protection of data during cyber armed conflict?
4. As a result of the study, what recommendations would best address the identified gaps?

1.4. Hypothesis

Legal regulation of international cyberwarfare is in its embryotic stage. There are few scholars who are examining the manner in which it can be done. Most of them are however international law scholars who may not fully understand the most valuable aspects of computer networks and systems. They evaluate the dangers of cyberwarfare from a traditional *jus in bello* perspective and may, consequently, focus on similar principle approaches as in traditional military engagement.

Data protection is widely ignored in the conversation about cyberspace and IHL. In the consideration of their interaction, there are types of data that may be referred to as critical civilian data. Digital identities are an example of such kind of data. During cyberwarfare, such data will be the most valuable and the first to be targeted by belligerents. There is need to protect this critical civilian data from military targeting.

An additional protocol to the Geneva Convention that focuses on cyberspace is the best way to address what is emerging to be the most common form of belligerence in our times. This additional protocol would enable the regulation of the application of current and emergent technologies in warfare.

1.5. Justification of the Study

At around 0800 hours on the 7th of December 1941, one of modern history's greatest military surprise occurred when the Japanese army attacked the United States Naval Base at Pearl Harbor in Honolulu, Hawaii. The ensuing fallout resulted in the entry of the United States into World War II and the ever-debated question of, 'Was it a surprise?'

Cyberwarfare is currently the hottest military topic. The United States of America has the United States Cyber Command, the UK has the National Cyber Force, Russia has Military Unit 74455 (based within its Main Intelligence Directorate), and China has several units focused on cyber defence. It is an open secret that cyberattacks and cyber espionage are currently being undertaken by various countries. With the world's major military powers moving towards improving their capacities in cyberwarfare, the inevitable truth is that cyberwar is coming. Is the legal world prepared to deal with the inevitable resultant fallout? Is the International Humanitarian Law movement preparing for this or are they waiting for a surprise Pearl Harbor level event?

In the event that cyberwarfare occurs, one of the most sought-after prizes will be the digital data of a targeted country and the personal data that maintains law, order and access to digital services, including essential ones. In this inevitable digital arms race, the protections offered to the world's vulnerable are not merely adequate; they are non-existent.

1.6. Literature Review

Jus in bello. A well-researched and well covered area of international law; for the 20th century. We are however in the 21st century, and the computer first approach to almost everything has created a need for expansion of the understanding of *jus in bello* to include cyberspace. The IHL world has reacted and risen to the occasion. There is, however, a massive gap that has

remained unaddressed in this adjustment to modern digital warfare. This gap lies in the question of what role data, and therefore data protection, plays in IHL during cyberwarfare.

The 20th century boasted of a new slew of weapons that were designed for mass murder and destruction. There is no generalised definition of what weapons of mass destruction (WMD) are. Croddy and Wirtz classify WMDs into four types: biological, chemical, radiological, or nuclear.[7] WMDs can be thought of as weapons that can cause a hundred times the casualties of an equivalent mass of high explosive and severe contamination to an area.[8] They however do not touch on the potential destructive impact that cyberweapons can have when used on a massive scale, rather focusing on the idea of direct comparison to kinetic explosives.

Can data be a WMD? Cathy O'Neil thinks so and describes algorithms and data as Weapons of Math Destruction.[9] A clever play of words for a rather serious accusation. She however still manages to demonstrate the impact that data, and its manipulation, can have on not only an individual but also on a targeted society as a whole.[10] She closes the introductory chapter to her data science focused book with the sentence, 'Welcome to the Dark Side of Big Data.'[11] While her presentation of the potential impact of data is spot-on, she does not consider the issue

[7] Eric Croddy and James J Wirtz (eds), *Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology, and History* (ABC-CLIO 2005) 408

[8] ibid

[9] Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (First edition, Crown 2016)

[10] ibid. In Chapter 5, she discusses the curious case of crime prediction software where predictive policing software is used to predict crime patterns and therefore deploy scarce resources more efficiently. The resultant impact on communities is an unplanned for, but real, racial bias in policing.

[11] ibid 18.

from an IHL's legal protective scenario. Her focus is on the civilian aspect of data's massive disruptive potential.

I believe there is an even darker side that transcends the use of big data. It is to be found in the increasing reliance that societies, and of even greater concern, governments, place on data to organise and deliver critical services. The OECD explains that as societies transform into digital societies, there is an expectation that public services will move away from physical interactions to digitally enabled solutions.[12] It is expected that more and more governments will respond to this demand with the creation of digital identity schemes. Claire Sullivan explains that in order to support this new normal, transactional identities must be established, preferably using an official national identity database.[13] She does an excellent job in explaining digital identities as an important part of a nation state's digital infrastructure and, specifically in chapter 6, how its abuse can be harmful. However, she also focuses on the civilian nature of this abuse, with no mention as to its potential for exploitation by the various militaries.

According to Bertino and Takahashi, one can think of digital identity as the digital representation of the information known about a specific person or organisation.[14] Because different societies have different views of privacy, profiling, and identification, it can translate to vastly different ideas. It is, for example, not a scan of your passport or your identity card. However, your digital identity can comprise of your passport number, together with other

[12] OECD 'Digital Government in Chile - Digital Identity' (OECD Publishing 2019) 7. Available at < https://www.oecd-ilibrary.org/governance/digital-government-in-chile-digital-identity_9ecba35e-en >

[13] Clare Sullivan, *Digital Identity: An Emergent Legal Concept* (University of Adelaide) 4. Using the term transactional identity and comparing it to 'database identity', she discusses the differences between some of the various tenets of cyber-identities. She describes transactional data as that subset of database identity that is required to transact under a scheme.

[14] Elisa Bertino and Kenji Takahashi, *Identity Management: Concepts, Technologies, and Systems* (Artech House 2011) 11

unique data points compiled into a database. The ultimate digital identity would be the one that can completely replace your physical forms of identity. Also referred to as an electronic ID by the World Bank, it represents a government backed official identity.[15] It is this data that encompasses the various forms of digital identities that would provide sweet attraction to belligerents in case of war. Asking the question of how this data is protected is an excellent place to start.

Bygrave explains that data protection and related privacy rights have grown into a monolith.[16] This is directly related to the growth of the value and importance of data. In Forbes list of most valuable brands for 2020, the top five companies deal with data.[17] Of these five, three have data as their main product. Bygrave, a data protection veteran, explains that data protection refers to laws that regulate the gathering, registering, exploitation and dissemination of data.[18] He lists six core data privacy principles: fair and lawful processing, minimality, purpose limitation, data quality, data security and data subject influence. [19]

Bygrave recognises that due to this explosion of importance, data protection has transcended national boundaries and is a transnational issue. The transnational nature of the Internet, one of the main technologies that utilises data, has of course encouraged this international regulation. Europe and its institutions provide leadership in data protection. He identifies

[15] World Bank Group, *Digital Identity Toolkit: A Guide for Stakeholders in Africa* (World Bank Group 2014) viii. Available at < http://documents.worldbank.org/curated/en/147961468203357928/Digital-identity-toolkit-a-guide-for-stakeholders-in-Africa >

[16] Lee A Bygrave, *Data Privacy Law: An International Perspective* (First edition, Oxford University Press 2014) v.

[17] Marty Swant, 'The 2020 World's Most Valuable Brands' (*Forbes*) <https://www.forbes.com/the-worlds-most-valuable-brands/> accessed 25 January 2021.

[18] Bygrave (n 16) 1

[19] ibid

UNGA resolution 2450 of 19 December1968 (Doc E/CN.4/1025) as the first such international attempt at this regulation. This resolution resulted in a report calling for national data privacy legislation.[20] He explains that when Convention 108 was opened for signatures in January 1981, it was the first data protection multilateral treaty to be legally binding.[21] Other trans-national instruments include the OECD guidelines on privacy protection and transborder data flow and various privacy related United Nations General Assembly (UNGA) resolutions. In addition to these, he chronicles a history of the EU initiatives contained in its various directives, regulations, and other documents. His demonstration of the international nature of data protection, with a focus on public international law, demonstrates the appetite for the civilian regulation of data. He also exposes the lack of global unanimity on a way forward for such civilian protection. His work is however lacking when it comes to issues of data as critical infrastructure and does not show the potential massive possibility and impact of failure of data protection. It is regimented and segmented into the various individual aspects/principles in the various individual jurisdictional spheres of the civilian laws being discussed.

Makulilo's works indicate that Africa is also on the bandwagon. It seeks to leapfrog the long privacy developmental history. In 2014, the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) was adopted.[22] By June 2020, it was signed by 14 countries and ratified by 8. The idea that communal Africa does not value its privacy, and thereby its data protection, is debunked by Makulilo who explains that although the core values of the African society include those of community and dependence on one another, the

[20] Bygrave (n 16) 51

[21] 'Convention 108 and Protocols' (*Data Protection*) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 25 January 2021

[22] Can be accessed at < https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection >

interplay between modern technologies and globalisation have brought to the fore privacy and data protection issues.[23] As a representative of one of the world's least militarily powerful region, the potential exposure that Africa has to military adventurism by the more powerful cyber armies has not been considered. Cross-nation state sponsored breech of data protection, whether for military or other strategic purposes like business and espionage needs, has also not been considered. His works focus on the exotic nature of data protection laws and the state vs its population approach to data protection regulation is commendable but leaves a huge gap as indicated above.

Data Protection in itself is moving along fantastically for the civilian world. The main challenge is that it falls within what would be described as dual use technology. Seumas Miller explains that traditionally, the technical term 'dual use' can refer to technologies that can be put to both military and civilian use. He however expands what he calls a rather vague definition to include technologies whose ultimate function can be concurrently helpful and destructive, with the destructive harm being on a large-scale.[24] His expansion allows him to then include technology aspects like cyber-weapons, weaponised autonomous robots, various computer viruses and ransomwares as dual use technology.[25] He then proceeds to specifically exclude 'big data' from being considered a dual use technology.[26] One of the criteria he uses to exclude it is that it 'merely violates individual privacy rights' and does not result in serious enough harm.

[23] Alex B. Makulilo, 'The Context of Data Privacy in Africa' in Alex B. Makulilo (ed), *African Data Privacy Laws* (1st ed. Springer 2016) 16-17

[24] Seumas Miller, *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (1st edition, Springer 2018) 5-6

[25] ibid 91

[26] ibid 96. He opines that the 'mere violation of individual privacy rights' does not result in a sufficient harm to warrant bit data as a dual use technology.

However, the military use of data predates its civilian use and the concerns over data privacy have strong roots in the use of civilian data by the organised forces, civilian or military. It is this undervaluation of data, and its potential military exploitation, by the IHL community that has relegated the regulation of the most critical part of computer systems to the realm of purely civilian matters.

Experts do not disregard the importance of cyberspace and its weaponization. Arimatsu accepts that cyberspace presents unique challenges in IHL. This, according to her, is centred in its destruction of two primary IHL assumptions: territorial borders and identification of the adversary.[27] Her views are shared by several other experts on the subject matter. Subject to considerations of these two issues, most agree that IHL can be transposed to cyberspace. The preeminent texts on IHL in cyberspace, being the Tallin Manual and the Tallin Manual 2.0, do not make any reference to data protection.[28]

It is these massive gaps in the existing literature and research space that I aim to address. Like most WMDs, it will be a blast.

1.7. Theoretical Framework

The research being proposed is multi-disciplinary in nature. It is essentially a legal problem and has its roots in the operation of information technology war. This is directly through data protection and cyberwarfare. It is, additionally, also an issue that is heavily affected by

[27] Louise Arimatsu, 'Classifying Cyber warfare' in Nikolaos K Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015) 326

[28] Schmitt MN and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013); Schmitt MN and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017)

international law and, more specifically, international humanitarian law. Finally, international relations are what would determine the practicality of any proposed solutions.

This paper will utilise three theories as they apply to law and to international relations. The dabble into international relations is due to the very nature of the problem: how to get several states to work together and restrain each other in cyberspace. There are already various proofs that it can be done, but the theories behind the reasoning of the states as they cede sovereignty to international institutions and laws are to be found in international relations. The three theories are: Legal Transplant Theory, Liberalism, and Consequentialism.

Legal Transplant Theory

Legal transplant theory is a theory that has its roots in comparative legal study. The term is generally attributable to Alan Watson who described it as the 'most fertile source of [legal] development'.[29] The idea is that legal rules are borrowed from another legal system and then implemented in the destination legal system.[30] The general idea is that legal rules are taken from a different country and applied in another. It is more focused on geographical transfer and subsequent adoption of legal rules. A good example is what happened between colonizing powers and their colonial holdings.[31] The colonisers generally imported their laws into their colonial holdings and implemented them. Without doubt, this has mutated into a situation where there is some adoption of the rules which are then changed to fit the situation in the

[29] Michel Rosenfeld and András Sajó (eds), *The Oxford Handbook of Comparative Constitutional Law* (1st ed, Oxford University Press 2012) 1309.

[30] Francesca Fiorentini, 'Legal Transplants in the Law of Secured Transactions. Current Problems and Comparative Perspectives' in Francesca Fiorentini and Marta Infantino (eds), *Mentoring Comparative Lawyers: Methods, Times, and Places: Liber Discipulorum Mauro Bussani* (Springer 2020) 6.

[31] Toby S Goldbach, 'Why Legal Transplants?' (2019) 15 Annual Review of Law and Social Science 583. 586

receiving legal systems. Such adoption can be done to better align the transplanted laws with the culture or legal institutions in the receiving legal system

With globalisation, legal transplantation between different societies is becoming more and more common. Indeed, as new technologies are implemented in one society, subsequent societies that start to use these same technologies often borrow a lot from the experience of these initial implementations. Regionalisation and the corresponding increase of regional laws are having the same effect, for example, the legal regime of the European Union.[32]

While traditionally thought of as happening between two different legal systems, I propose to stretch this theory and apply it as between two different legal fields. In this case, IHL and Cyberlaw. I propose to recognise that the challenges facing the development of these two law-phenomenon are, on the surface, the same. In order to differentiate the two, I refer to the transfer between legal fields as transposition rather than transplantation.

Liberalism

Liberalism is an idea that focuses on the rights of the individual to life, liberty, and property.[33] Edmund Fawcett identifies four broad ideas that guide liberalism.[34] The first is the idea that conflict is inevitable. The second is a deep-rooted distrust of power and therefore a need to check it. The third is that human beings will always seek progress. The fourth is that of civic respect, especially by the government itself. The result is a societal setup where there is respect for the individual and a check on the powers of the government and state.

[32] ibid. 587

[33] Stephen McGlinchey and others, *International Relations Theory* (2017) 22. <https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=544> accessed 21 January 2021.

[34] Edmund Fawcett, *Liberalism: The Life of an Idea* (2nd edition, Princeton University Press 2018) 21

In international relations it is used to argue for the limitation of the state's global powers. The concern being that history has shown that states that built massive foreign power, often militarily, eventually turned this power inwards and abused it against their citizens. McGlinchey further summarises the works of Daniel Deudney and G. John Ikenberry into three reasons that explain global libertarian movement.[35] The first one is the creation of an international system that comprises of international law and international institutions. Secondly, free trade and capitalism have resulted in a market based international economy that encourages peaceful relationships. The third one is the creation of international norms most of which are based on liberal ideas of human rights, democracy, and the rule of law. As an aspect of Natural Law, liberalism focuses on the individual rather than the institutions that are used to govern society. Indeed, Mather identifies contemporary liberalism as an approach where power is used to check power.[36] Centralised power is a danger that both liberals and natural law proponents seem to be wary of.

In liberalism, we identify two basics that are of utmost importance to this research. The first is the idea that international cooperation amongst states is a good way of checking each other's powers and that international institutions help in this through their monitoring and reporting roles. The second is that the individual remains the primary concern of the state's international dealings and such individual's rights and liberties must be enhanced through all these dealings.

Consequentialism

[35] McGlinchey (n 11) 24. <https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=544> accessed 21 January 2021. Here McGlinchey is speaking of their seminal paper 'The Nature and Sources of Liberal International Order' published in 1999.

[36] Henry Mather, 'Natural Law and Liberalism' (2001) 52 South Carolina Law Review 331, 354

Consequentialism is the view that whether an action is right or wrong depends on its outcome as compared to the outcomes of alternative actions.[37] It can be summarised in two principles:[38] First, to decide whether an action is right or wrong, one considers only the outcome of that act. Second, the best outcome is the one that produces the most good. Utilitarianism is one of the best known examples of consequentialism.

In the course of my argument, it will be necessary to evaluate whether there is any good to be got in the restriction of states' powers to collect and exploit critical data for purposes of cyberwarfare. This is then juxtaposed to the question of why unitary states should cede their power, and aspects of sovereignty, to the international system. I will be arguing that the international community needs to consider the repercussions of both taking and not taking any action. They should then take the action whose consequence will provide the best for the greatest number of people. I believe that focusing on people rather than the main actors in the international arena, being nation states, will drive the agenda forward and drive it towards a satisfactory end.

1.8. Research Methodology

I intend to make use of secondary data in completing this research. This will take the form of reviewing already written material in the relevant subject areas. The result will be a qualitative consideration of the research questions and an attempt to propose an amalgamation of different secondary data into a possible solution to the problem.

The main approach will be through desktop research. This will require me to make use of published materials, academic journals, reported interviews, publications by International

[37] Julia Driver, *Consequentialism* (Routledge 2012).

[38] 'BBC - Ethics - Introduction to Ethics: Consequentialism' <http://www.bbc.co.uk/ethics/introduction/consequentialism_1.shtml> accessed 28 January 2021.

NGOs, and government publications or training manuals. Equally important will be current promulgated laws and proposed laws. Where possible, the *ratio* and *obiter* views in case laws will also be incorporated. Data collected will be scrutinised and analysed in order to demonstrate best practices, potential problem areas and most importantly, the areas of confluence between these seemingly diverse fields. The results of the analysis will then be presented as a series of proposals on what the most likely reactions to certain actions and situations would be. The end-product will contain a brief introduction to the relevant subject areas, a demonstration of their confluence, a proposal of the importance of their confluence, and an examination of whether this importance should result in international efforts to proactively prepare for any negative consequences.

The reasons for selection of this method are mainly connected with the secrecy and abstract nature of the subject areas. Both data protection and cyberwarfare lend themselves to secretive ringfencing by the institutions that interact with them. The military nature of the interaction being considered by this paper makes it even harder to get first-hand primary data. Additionally, both fields carry with them huge reputational risks that may affect the perception of a potential source's information security and military preparedness. The potential for embarrassment is huge.

The cross-border considerations and legal grey areas also encourage secretiveness. Potential subject countries may find themselves in internationally embarrassing situations. They may be accused of cyber-belligerency and the information may, in turn, have real-world international relations implications. It would therefore be naïve to expect genuine primary data from the potential subject persons and institutions in the area. A good illustration of this is that there is not even one officially acknowledged admission by a country that it has engaged in cyberwarfare. Several accusations exist, but no acknowledgements.

The main potential pitfall of this methodology is that there is a constant danger in carrying forward undeclared or misunderstood assumptions from the secondary data. This is especially possible where there has been analysis done and the assumptions and parameters either not declared or lost in translation. I will remedy this by treating all analysis as biased and examining any conclusions or declarations from a neutral viewpoint, irrespective of their alignment with my hypothesis.

1.9. Limitations

The main limitations of this paper are inherent in the nature of the question being examined. Issues of military security, both defensive and offensive, are generally classified. Statements that are made in relation to these issues are often heavily considered and highly likely to be laced with the poisonous strain of propaganda and the deceptive use of diplomatic language. Perception management and international relations mind games are also an inherent part of this area. There are valid reasons to expect a lot of inaccurate data.

The availability of useful data is likely to be limited. As such, the sourcing of material and data has to be carefully considered and a lot of what I will come across will most likely not make it to this paper. The reasons being that it will be hard to countercheck and ensure validity of the data. This will compound the already expected dearth of material on the research questions.

An additional limitation is the theoretical consideration of the research question. This is also due to the aforementioned challenges of a lack of verifiable high volume data. This limitation is however countered by the very purpose of the paper, which is to make theoretical proposals on a subject that has not yet been widely examined.

This study will also have the limitation of several different contextual sources of data. It is unexpected to find research that will consider a single context (for example, country or

incident). This limitation is not expected to have a huge impact as the eventual goal of IHL is to cover the entire globe in a single agreement on the particular issue(s).

1.10. Chapter Breakdown

Chapter 1: Background and Outline

This chapter provides the structure and outline of the paper. It gives a background to the research, the justification for carrying it out and the methods used to carry it out. As such, it contains the research objectives, questions, methodologies, limitations, and hypothesis.

This chapter also contains the literature review. This attempts to illustrate the existence and content of other research in the constituent fields of this study.

Chapter 2: International data protection; the dearth of jus in bello.

This chapter will introduce the utility and importance of data in the modern world and the power its exploitation, legal or illegal, gives. It will then lay the background for the start of the journey that data protection has in IHL. Working on the hypothesis that there is currently no data protection envisioned in the realm of IHL, it will lay out the international data protection environment that would consequentially apply, even during war times. This is done from the position that even while the debate about application of data protection in IHL (an obviously better setting) continues, the rules of international data protection do not stand in abeyance. It is also premised on the idea that even with IHL, there were still rules prior to the codification of our current major rules.

Chapter 3: A primer on IHL and Cyberspace; is transposition enough in data protection?

This chapter will try and summarise what thought leaders in the field are proposing in terms of handling cyber armed warfare. It will focus and elucidate the transpositional approach being used with cyber warfare and hopefully demonstrate its adequacies and inadequacies. Given the multidisciplinary nature of the paper, it will also include a brief on IHL and two of its main

principles and an overview of whether international law, and therefore IHL, applies in cyberspace. It will also attempt to draw a distinction between cyber warfare and cyber espionage, cyber theft, cybercrime, information warfare and general cyber operations.

Chapter 4: Cyber warfare's inescapable evolution towards data.

Having seen that transposition is the main way in which IHL is currently being applied in cyberspace, this chapter will look at the unique nature of data and how this makes transposition an unsuitable approach for data protection in an IHL setting. We will then look at the international data protection principles that would have to be preserved in an IHL environment. Finally, we will look at electronic IDs and how they can be examples of critical civilian infrastructure that would need protection during times of belligerency.

Chapter 5: Conclusion

This chapter will conclude by summing up the relationship that I envision as being necessary to deal with what I view as an inevitable occurrence. It will attempt to demonstrate the potential effectiveness of the expansion of the Geneva Protocols with the inclusion of one which governs cyberspace in general and data protection in particular.

2. INTERNATIONAL DATA PROTECTION; THE DEARTH OF JUS IN BELLO

2.1. Introduction

In this Chapter, I will introduce the idea of personal data and the need for its protection. I will also demonstrate the importance of data to our current world and its primacy in almost all modern fields. I will also provide a historical and philosophical basis for data protection by linking it to the concept of privacy. Finally, I will provide an overview of the international data protection laws. By the end of the chapter, it will be evident that data and data protection are core issues in any modern society. The conclusion of the chapter will be an invitation to consider these issues from a warfare perspective.

2.2. Is Data (Protection) that Important?

So, what is data and why does it need protection? When did it become something worth writing books about? Maybe it is a simple consequence of the information age. Maybe it is a reckoning between fears of the growing corporate strength of data-centric corporations on one hand and the regulators and citizens from whom they extract this digital gold on the other hand. The idea that our data needs to be protected immediately raises the question of 'from who?' The obvious targets become these corporations and institutions that we deal with every day. The players that are consistently in our news cycles, hitting unforgettable highs that include tremendous personal wealth. Out of the top ten richest individuals in the world, eight are directly working with information technology.[61] Of the remaining two, one is a significant investor in

[61] Dorothy Neufeld, 'The Richest People in the World in 2021' (*Visual Capitalist*, 9 March 2021) <https://www.visualcapitalist.com/richest-people-in-the-world-2021/> accessed 15 April 2021.

information technology companies (including USD 119 Billion dollars in Apple Inc)[62] and the other is in the fashion industry.[63] Data is unarguably the world's most valuable commodity.

Data has been defined as the physical representation of information in a manner suitable for communication, interpretation, or processing by human beings or by automatic means.[64] This word-for-word definition covers most aspects of what data is. However, the data that will be generally referred to in this paper is personal data. Personal data is described as 'any information relating to an identified or identifiable natural person'.[65] It is this personal data that has the potential to make up a country's critical infrastructure and of which digital identity is a good example.

For data protection purposes, there is a restriction to 'identifiable natural persons'. Kenya's Data Protection Act, 2019 describes an identifiable natural person as 'a person who can be identified directly or indirectly, 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.' This restriction holds true, with slight variations in the types of identifiers, with most data protection legal regimes.

However, for the purpose of this paper, the discussion of data protection in a cyberwar scenario will include hypothetical scenarios of possible references to juridical persons. This is because

---

[62] 'Berkshire Hathaway Portfolio Tracker' (*CNBC*, 16 May 2019) <https://www.cnbc.com/berkshire-hathaway-portfolio/> accessed 15 April 2021.

[63] 'Forbes Billionaires 2021: The Richest People in the World' (*Forbes*) <https://www.forbes.com/billionaires/> accessed 15 April 2021.

[64] Organisation for Economic Co-operation and Development and Source OECD (Online service) (eds), *OECD Glossary of Statistical Terms* (OECD 2008). 119

[65] ibid 404. This simplified definition also aligns with what most data protection instruments define personal data as. For example, the GDPR is a word-for-word copy of the same. Kenya's Data Protection Act, 2019 is an exact replica of the two referenced sources.

the field of digital identities is still nascent and there may be instances, now or in future, of digital identities being linked to juridical persons.

2.3. Age of Data

We are living in an age of data. Data analysis, data scientist, data security, data this and data that. The information age is considered as part of the industrial revolution. The first industrial revolution was identified by mechanisation. It revolved around iron, coal, and textiles.[66] The second industrial revolution was identified by automation and mass production. It revolved around the use of steel, chemicals, and electricity.[67] The third industrial revolution is also referred to as the digital revolution. It is identified by digital electronics. It revolves around computers, the internet, and their enabling technologies. It was pioneered by the transistor. It led to the information revolution and the exploitation of these two revolutions has had a huge impact on the world.

Computers are considered to be a general-purpose technology and they are at the core of both revolutions. Shimizu describes general-purpose technology as a technology that can be used for various products and processes.[68] However, it becomes extremely important when it can transform an entire economy.[69] Common examples given as general-purpose technologies include the wheel, steam engine, electricity and of course the Internet. It is this uneven impact

[66] 'Industrial Revolution | Definition, History, Dates, Summary, & Facts' (*Encyclopedia Britannica*) <https://www.britannica.com/event/Industrial-Revolution> accessed 16 April 2021.

[67] Eric Niiler, 'How the Second Industrial Revolution Changed Americans' Lives' (*HISTORY*) <https://www.history.com/news/second-industrial-revolution-advances> accessed 16 April 2021.

[68] Hiroshi Shimizu, *General Purpose Technology, Spin-Out, and Innovation: Technological Development of Laser Diodes in the United States and Japan* (Springer Singapore Imprint,Springer 2019). 16

[69] Richard G Lipsey, Kenneth Carlaw and Clifford Bekar, *Economic Transformations: General Purpose Technologies and Long-Term Economic Growth* (Oxford University Press 2005). 97

of general-purpose technologies that cascades into almost every sector of life, making their impact, and thus their dangers, ginormous.

Computer systems are generally recognised to comprise of three components: Input devices, Central Processing Unit (CPU), and Output devices.[70] There is however a string running through these components that is traditionally not mentioned. Data! Input devices enable data to be entered into the computer system, the CPU processes this data, and the output devices display the processed data. As data flows through these components, the true value of computer systems is realised. In the computing world, data can be simply defined as 'raw facts and figures that are processed into information'.[71] It is this transformative aspect, from data to information, that has defined the information age.

The importance of data cannot be understated, and it cannot be summarised. It requires an extra volume of books. Suffice it that I recommend Bruce Schneier's book, 'Data and Goliath'. The perversive nature of data in the various aspects of our modern lives, and that it is, individually and collectively, being collected and utilised are well discussed. From its use in mass surveillance by both the government and the multi-national corporations,[72] to the impact on web surveillance. He uses the phrase 'We don't lie to our search engine' to put it in perspective.[73] Does Google really know more about us than we do? Yes, because it remembers everything we search, perfectly and forever.[74] He also delves into the impact that data has on

[70] Brian K Williams and Stacey C Sawyer, *Using Information Technology: A Practical Introduction to Computers & Communications* (Eleventh edition, McGraw Hill Education 2015). 27. Storage can also be considered as a component but it is not as critical as the basic ones listed.

[71] ibid 27.

[72] Bruce Schneier, *Data and Goliath* (WW Norton & Company 2015) Chapter 2

[73] ibid

[74] ibid

our relationship with governments, business, and society as a whole. And yet this scary seminal book from the year 2015 still undersells the importance of data, in my opinion. Six years later, data is even more important. An interesting demonstration of the importance of data is the elevation of data by the Chinese government to a factor of production.[75] In their fourteenth 5-year plan, data has been equated to land, labour, capital, and technology.[76] This acknowledgement of data by the world's second biggest economy, which is projected to become the largest economy by 2028, is most accurate.[77]

Oil and data can both leak. The dangers of oil leaks are well documented and have been a companion of the transportation and use of oil since the beginning. They are generally referred to as oil spills and the biggest ones are memorable. Their impact on the environment is widely reported and it is accompanied with pictures of volunteers in bio-hazard suits, marine life covered in oil, and spoilt beaches. The largest reported oil spill was the Gulf War Oil Spill. It is estimated that about 11 million barrels of crude oil were purposefully released by the Iraq Army as it prepared to fight the combined UN forces mandated to liberate Kuwait.[78] Like the

[75] 'China Is Laying the Groundwork to Nationalize Private Companies' Data' (*protocol*) <https://www.protocol.com/china/china-national-security-data-exchange> accessed 17 June 2021.

[76] A translated version of the 5 year plan is available at https://cset.georgetown.edu/wp-content/uploads/t0237_5th_Plenum_Proposal_EN-1.pdf.

[77] Evelyn Cheng Lee Yen Nee, 'New Chart Shows China Could Overtake the U.S. as the World's Largest Economy Earlier than Expected' (*CNBC*, 1 February 2021) <https://www.cnbc.com/2021/02/01/new-chart-shows-china-gdp-could-overtake-us-sooner-as-covid-took-its-toll.html> accessed 17 June 2021.

[78] Nick Barber, '1991 Gulf War Oil Spill' (23 November 2018) <http://large.stanford.edu/courses/2018/ph240/barber1/> accessed 3 May 2021.

situation being contemplated in this paper, it revolved around the weaponization of a hitherto civilian-application focused resource.[79]

When data leaks, the effects can be as dangerous, if not more so, as that of oil leaks. Data protection is the world's risk mitigation strategy. It has become what allows the age of data to flourish.

2.4. Historical Development of Data protection from Privacy.

The main objective of data protection is to afford some type of protection to data subjects when third-parties access and process their persona data. Simple! This does not, however, then provide the reasons for why it is done, and therefore, underline its importance to the greater scheme of societal balance of interests.

A historical understanding of data protection is then needed to better appreciate its importance. This paper is not the right place for an in-depth look, however, a summary of the same starts with the understanding that what we refer to as data protection is the logical decades-long product of hard labour by privacy activists. Indeed, the idea that identity, privacy, personal information, and data protection are intricately linked is a basic conclusion in this field.[80] Therefore, the basic reasons that data protection exists is to be found in the same basic reasons that privacy exists. Reasons that have been extrapolated into the modern world of massive data collection and processing.

[79] Dagmar Schmidt-Etkin. 'Spill Occurrences: A World Overview' in Mervin F Fingas (ed), *Oil Spill Science and Technology: Prevention, Response, and Cleanup* (Elsevier/Gulf Professional Pub 2011) 13-15. Out of the top 5 oil spills, it lists three as being 'war-related intentional spillage'.

[80] Eleni Costa and others, 'Regulating Identity Management' in Jan Camenisch (ed), *Digital Privacy: PRIME - Privacy and Identity Management for Europe* (Springer 2011).

Privacy is an old concept. Socrates and Aristotle mentioned it in their writings. Aristotle draws a distinction between the private family life and the public life.[81] The adage 'a man's house is his castle' gives a hint of the idea of privacy.[82] It was espoused in the US Constitution's fourth amendment by the words 'right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures'. This was back in 1791.

In retro-modern times it has been described as the 'right to be left alone'. This is modern in the grand scheme of the right to privacy, but it is a vestige of the state of the issue in 1890 when Samuel Warren and Louis Brandeis had their seminal work, A Right to Privacy, published in the Harvard Law Review.[83] This article is mentioned as the 'invention' of this right and indeed is one of the first times the idea was concisely expressed.[84] Over time, the right to privacy has been highly debated, controversially applied, and loudly opposed and adopted in various measures.

The modern idea of privacy now encompasses many constituent rights.[85] The importance placed on these rights vary from time to time and also between societies. A loose listing of

---

[81] Judith DeCew, 'Privacy' in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2018, Metaphysics Research Lab, Stanford University 2018) <https://plato.stanford.edu/archives/spr2018/entries/privacy/> accessed 20 May 2021.

[82] In the 1928 US Supreme Court case of *Olmstead v United States* [277 US 438 (1928)], the court referred to privacy laws as providing 'protection against such invasion of "the sanctity of a man's home and the privacies of life."'

[83] Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 Harvard Law Review 193.

[84] Irwin R Kramer, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' 39 Catholic University Law Review 703. While it is to be noted that the attribution of this 'invention' is widely cited by several authors, Krawer does an excellent four paragraph summary introduction on the impact the article had on the field of privacy and the law in general.

[85] Leslie Francis and John G Francis, *Privacy: What Everyone Needs to Know*® (Oxford University Press 2017). 1

some of these constituent rights will include information privacy, anonymity, bodily security, right to be forgotten, confidentiality rights, rights to secrecy, spatial privacy, do-not-track, right to autonomy, de-identification, and of course data protection.

Simultaneously, the international scene for privacy protections has been active. What can be considered its main underpinning would be Article 12 of the Universal Declaration of Human rights: ***No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks***. Another instrument in the International Bill of Rights that mentions privacy is the International Covenant on Civil and Political Rights. The UN Convention on the Rights of the Child, United Nations Convention on Migrant Workers, African Charter on the Rights and Welfare of the Child, American Convention on Human Rights, European Convention on Human Rights, and the Arab Charter on Human Rights all mention issues on privacy.[86]

2.5. International Data Protection Scene

It is important to start this conversation about IHL and data-protection with a review of the current international data protection framework. This is because, in my opinion, should it be concluded that there is no data protection in IHL, then it is these rules of international data protection that will form international law's rear-guard protection. As such, even during belligerency, there will be no lacuna, except for those that occur within the laws of international data protection itself. The suitability and enforceability of the same will be highly doubtful, but that is a debate for another day.

[86] 'What Is Privacy?' (*Privacy International*) <http://privacyinternational.org/fr/node/56> accessed 20 May 2021. This contains a listing of the various specific articles in these instruments as well as in others.

That said, data protection is not something that has quickly drawn the attention of the international law-making efforts. This is probably because it has not been at the front of the thoughts, of the masses or the intellects, which form the ostensible reasons for what are often political and international power plays. It is however becoming more and more important. Regional and indeed international efforts have been put in place and more continues to be done.

A key issue is the differences between the cultural viewpoints of the major movers of international collaborative efforts. Seen from a regional viewpoint, the North American and European viewpoints are based on different cultural and philosophical approaches. The former is more concerned with protecting privacy, and by extension data, from their government and the later are more unsettled about private corporations and corporate access to data.[87] Further to this, the Russians and the Chinese have strong communist backgrounds and have traditionally favoured strong government. They are also seemingly sensitive about state sovereignty and are generally loath to giving away power, actual or supervisory, to international treaty bodies. [88]

However, the efforts that have been put in are summarised below. Note should be taken that these are not international in respect to availability/applicability to the entire globe but rather constitute of regional and international efforts to regulate data protection at a multi-state level. Additionally, there is a lot of mention of transborder data flow in the international instruments, especially the earlier ones. There was a bifold basis for this. First, there was a fear that privacy protection laws would be used to restrict data flows with an adverse effect on trans-border trade and innovation, and secondly, there was an equally important concern that private actors would

[87] Francis (n 66) 45,46.

[88] Isaac Porche, *Cyberwarfare: An Introduction to Information-Age Conflict* (Artech House 2020). 3

move data processing out of national jurisdictions to avoid national laws.[89] While modern international, and indeed national, efforts also contain references to transborder flow of data, they can be said to be more focused on the human right perspective of data privacy.

2.5.1. UNGA Resolution 2450 of 19 December 1968 (Doc E/CN.4/1025)

This represents one of the first attempts at the international stage to address the issue of data protection. It was also the first attempt by the United Nations.[90]

United Nations General Assembly (UNGA) is a forum of all the member states of the United Nations. It is a creature of Article 7 of the United Nations Charter, and its principal powers and functions are set up by Chapter IV of the same instrument.[91] In 1968, the UNGA passed a resolution titled '*Human Rights and Scientific and Technological Developments*'.[92] It required the Secretary General to 'examine the impact of technological developments on human rights including considerations of individuals' right to privacy 'In light of advances in recording and other techniques''.[93]

UNGA resolutions do not have any legal effect. Indeed, the only body that, contemporarily, would seem to religiously respect them are the organs of the UN. As such, nation states, the main protagonists in the data protection arena during the time of this resolution, were in no

[89] Brendan Van Alsenoy, *Data Protection Law in the EU Roles, Responsibilities and Liability* (Intersentia 2019). 207

[90] Bygrave (n 29) 51

[91] See Articles 9 – 22.

[92] General Assembly Resolution 2450 (XXIII) of 19 December 1968. See 'Kirby, Michael --- "Privacy Today: Something Old, Something New, Something Borrowed, Something Blue" [2017] JlLawInfoSci 1; (2017) 25(1) Journal of Law, Information and Science 1' <https://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html#fn39> accessed 1 June 2021.

[93] As quoted from: Lee A. Bygrave in 'International Agreements to Protect Personal Data', James B Rule and GW Greenleaf (eds), *Global Privacy Protection: The First Generation* (E Elgar 2008). 29

way obligated to pay this resolution any heed. However, there was a publication by the UN Secretary-General titled 'Points for Possible Inclusion in Draft International Standards for the Protection of the Rights of the Individual against Threats Arising from the Use of Computerized Personal Data Systems'. This encouraged nations to legislate on this topic and provided for minimum standards for such legislation.[94]

As such, this initiative did not, by itself, go very far. However, the 1990 Guidelines Concerning Computerised Personal Data Files, which I discuss below, quoted it as the beginning of the journey to its creation.

2.5.2. Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data

I will refer to these guidelines as the OECD Privacy Guidelines for purposes of this paper.

The Organisation for Economic Co-operation and Development (OECD) describes itself as an international organisation that works to build better policies for better lives. It currently consists of 38 member countries and 5 key partners.[95] Its member countries (including the 5 key partners) are representative of every continent, and it claims to represent about 80% of world trade and investment.[96]

The OECD privacy guidelines were a result of almost two decades of studies and efforts by the OECD that begun in the 1960s and culminated with the adoption of these guidelines on the 23rd of September 1980. In 2013, there was an update to these guidelines in order to bring them up

[94] Bygrave (n 29) 51.

[95] 'About the OECD - OECD' <https://www.oecd.org/about/> accessed 28 May 2021.

[96] 'Discover the OECD' available at 'About the OECD - OECD' <https://www.oecd.org/about/> accessed 28 May 2021.

to date with the myriad of societal and technological changes that have happened since 1980.[97] As such, the current document is the 2013 privacy guidelines.

They are exactly what they claim to be, guidelines! They are legally non-binding.[98] They do not represent a treaty or a convention or any form of instrument known to international law. From the ordinary functioning of the OECD, they have had a heavy impact on the national laws developed, both statutory and case law. This is because member states modelled their national data protection and privacy laws around these guidelines. Courts have also variously referred to them as they went about their business of interpreting data protection laws. These principles have such notoriety as to be cited in non-member states including here at home in Kenya. The Kenyan High Court, sitting in a three-judge bench in the Huduma Number case, stated as follows:[99]

> In considering this issue, we take the view, and will be guided by the principles developed by the Organisation for Economic Co-operation and Development (OECD) namely the OECD Privacy Principles, which is in our view a more comprehensive and internationally recognized data privacy and protection framework that we deem most appropriate for our purposes. We also note that the said principles have been replicated in the African Union Convention on Cyber Security and Personal Data Protection.

One of their key lasting impacts has been the eight basic principles of data privacy referred to in the above Huduma case. Listed, these are: collection limitation principle, data quality

[97] 'OECD Work on Privacy - OECD' <https://www.oecd.org/sti/ieconomy/privacy.htm> accessed 30 May 2021.

[98] Johann Čas, 'Ubiquitous Computing, Privacy and Data Protection: Options and Limitations to Reconcile the Unprecedented Contradictions' in Serge Gutwirth (ed), *Computers, Privacy and Data Protection: An Element of Choice* (Springer 2011) 149

[99] Nubian Rights Forum & 2 others v Attorney General & 6 others; Child Welfare Society & 9 others (Interested Parties) [2020] eKLR

principle, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle, and the accountability principle.[100]

2.5.3. Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data

This convention was opened for ratification on 28th January 1981. In honour of this, from 2006, January 28 has been celebrated as Data Protection/Privacy Day.[101] The convention is also referred to as Convention 108 and it came into force in 1985 after being ratified by five countries and it currently has 55 ratifications.[102] In 2018, it underwent 'modernisation' through amendment by the 'Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data'. References to Convention 108 in this document will be to this 'modernised' version that contains the amendments.[103] The Convention also has one Additional Protocol.[104]

It was negotiated under the auspices of the Council of Europe (CoE). The CoE is an international multi-nation organisation that was formed in 1949 with an aim to protect democracy and human rights while fostering European unity. Membership is limited to

[100] As reflected in PART 2 (Articles 7 - 14) of the Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013).

[101] '28 January - Data Protection Day' <https://www.coe.int/en/web/portal/28-january-data-protection-day> accessed 30 May 2021.

[102] 'Chart of Signatures and Ratifications of Treaty 108' (*Treaty Office*) <https://www.coe.int/en/web/conventions/search-on-treaties> accessed 24 May 2021.

[103] Available from 'Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (*Treaty Office*) <https://www.coe.int/en/web/conventions/full-list> accessed 27 May 2021. The main purpose of the amendments was to update it to the modern context.

[104] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows.

European states, and this has been translated to mean the continent of Europe, rather than the European Union, and indeed has allowed states like Cyprus to join.[105]

It might be from this loose approach to the definition of Europe by the CoE that partly contributed to the provision in Convention 108 that CoE non-member countries can accede to the Convention.[106] Therefore what may have seemed like a European endeavour became a global one with wider ramifications. Currently eight non-CoE member states have ratified Convention 108.[107] The first was Uruguay in 2013, and the list includes Senegal, Mauritius, and Argentina.

Its importance has less to do with its open welcoming nature, given the low numbers of non-CoE members that have ratified it, and more to do with its historical place in data protection at the international level. It was the first international instrument concerning data protection. This means that it has had an impact on several data protection regimes, including what may be arguably the most impactful regime, the EU's General Data Protection Regulation (GDPR).[108] Several authors refer to it as the only multilateral treaty that concerns data protection.[109]

---

[105] Stefanie Schmahl and Marten Breuer (eds), *The Council of Europe: Its Law and Policies* (First edition, Oxford University Press 2017). 44-45

[106] Article 23. Treaty is available at 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data' (*Treaty Office*) <https://www.coe.int/en/web/conventions/full-list> accessed 24 May 2021.

[107] 'Chart of Signatures and Ratifications of Treaty 108' (*Treaty Office*) <https://www.coe.int/en/web/conventions/search-on-treaties> accessed 24 May 2021.

[108] Bart Custers and others, *EU Personal Data Protection in Policy and Practice* (1st ed. 2019, TMC Asser Press : Imprint: TMC Asser Press 2019). 217. There is a direct line drawn from Convention 108 to the GDPR, through the EU's 1995 Data protection Directive (Directive 95/46/EC)

[109] Bygrave (n 29) 31; See also Europäische Union and Europarat (eds), *Handbook on European Data Protection Law* (2018 edition, Publications Office of the European Union 2018). 24. Take note that these references refer to Convention 108 as the only international multilateral treaty on data protection.

In the relevant jurisdictions, this Convention applies to data processing by both public and private actors. Where ratified, it forms binding law.[110] This means that where there is no national legislation, the Convention will apply. However, should national legislation be created, then it should, as per Article 4, conform to Convention 108. Any derogations must be in conformity with reservations done vis-à-vis Convention 108.

2.5.4. Guidelines Concerning Computerized Personal Data Files

UNGA Resolution 45/95 of 14 December 1990 gave birth to the 'Guidelines Concerning Computerized Personal Data Files'. The challenges facing UNGA resolutions have been alluded to above in the discussions about UNGA's 1968 resolution. These guidelines essentially listed some principles of data protection that member states were spurred to implement within their national data protection laws. Of peculiar interest is the inclusion of 'Part B' that required 'Governmental International Organisations' to adhere to the guidelines.[111]

The challenges that faced this attempt were the same as that of UNGA Resolution 2450 discussed above. The soft law nature of the resultant guidelines made for a good document but nothing more. At the same time, there were several other international initiatives that were more 'business' focused, as opposed to this one which was more focused on human rights. Multilateralism was thus focused on these other initiatives, some of which matured into legally binding 'hard law'.

[110] Europäische Union and Europarat (eds), *Handbook on European Data Protection Law* (2018 edition, Publications Office of the European Union 2018). 25

[111] Guidelines for the Regulation of Computerised Personal Data Files.

This is not to suggest that they have had zero impact. Soft law persuades and Yilma has identified two cases in different jurisdictions that referenced these guidelines.[112] The Spanish Constitutional Court in the case 'Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre' references them,[113] as well as the European Court of Human Rights in the case of Bărbulescu v. Romania.[114]

2.5.5. African Union Convention on Cyber Security and Personal Data Protection

This document is a product of the African Union and was adopted on June 27, 2014.[115] As of July 2020, it had 14 signatures and 8 ratifications. It is also known as the Malabo Convention. It is divided into the following thematic areas. The first is electronic transactions, and it is followed by data protection and the last theme is cybercrime. Data protection is covered, specifically, in its second chapter.

Article 36 of this convention requires that it shall enter into force '30 days after the date of the receipt by the Chairperson of the Commission of the African Union of the 15th instrument of ratification'. As previously mentioned, the convention currently has only 8 ratifications. It is as such not yet in force but continues to play an important role in the data protection conversation on what is the world's 2nd most populous continent.

---

[112] Kinfe Micheal Yilma, 'The United Nations Data Privacy System and Its Limits' (2019) 33 International Review of Law, Computers & Technology 224.

[113] Available (in Spanish) at 'Sistema HJ - Resolución: SENTENCIA 292/2000' <http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276> accessed 1 June 2021. In particular, see para 8.

[114] Application no. 61496/08 available at 'BĂRBULESCU v. ROMANIA' <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}> accessed 1 June 2021.

[115] 'African Union Convention on Cyber Security and Personal Data Protection | African Union' <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 1 June 2021.

2.5.6. Summary on International Data Protection

There have been other developments in the international data protection scene. However, there is no global concerted effort to develop data protection instruments that might have a larger than geo-regional sectoral impact at the international level.

There are some provisions that deserve honourable mentions despite the fact that they do not meet the threshold of the above listed instruments, especially that of multilateralism and international applicability. Article 8 of the Charter of Fundamental Rights of the European Union is titled 'Protection of personal data' and provides binding law for the nations of the European Union. There is also ECOWAS' Supplementary Act A/SA.1/01/10 that is titled Act on Personal Data Protection within ECOWAS. This ECOWAS Act was adopted in 2010 and applies, as binding law, to its member states. The Asia-Pacific Economic Cooperation (APEC) also has a Privacy Framework.[116] This framework aims to increase information privacy protection while at the same time reduce potential barriers to transborder data flow.

It should also be considered that the changing nature of globalisation and increased reliance on data and, consequently, transborder flow of data, has caused a knock-on effect of national and regional laws in the international data protection scene. For example, as a rather important international market, the EU's restriction, through the GDPR, on transfer of data to territories that do not offer guarantees of data protection, has driven an increase in the passage of national data protection law, many of which are modelled after those in this all-important market.[117]

[116] Available at 'APEC Privacy Framework' (*APEC*) <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> accessed 17 June 2021.

[117] Alex B Makulilo (ed), *African Data Privacy Laws* (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016) 18

2.6. Conclusion

The idea that data protection is necessary is, nowadays, a forgone legal conclusion. This is based on the wider fact that there is a lot of data generated, its economic value is almost unmatched, and its exploitation is something that is increasingly differentiating societies. Various nation states are in the process of enacting or improving on their data protection regimes. International data protection is probably one of those areas of international law that a disproportionate number of us interact with on a daily basis. From the global but unadopted requirements, to the regional and better enforced, international data protection will grow into an even bigger area. This will be especially true once the USA gets on the bandwagon. At the same time, the use of eIDs will increase and the personal data being associated with these IDs will be used in more places, and countries, and for more purposes.

The underlying veneer of military action in all sectors of society will have an impact on both personal data and its usage. Formal and informal military action is ongoing in the information age. The secrecy that is a staple of peacetime military action and preparation is compounded with the relative ease, anonymity, low cost, and high value returns of cyber warfare. Is it possible that there are critical areas of national information management systems whose vulnerability, real or imagined, would severely impact non-combatants in a cyber warfare scenario?

The traditional response to the protection on non-combatants is through IHL and its laws. As such, IHL has been immediately applied to this field by well-meaning practitioners. They have not had to apply their minds as to the choice of application tool to use, having obviously settled on transposition as the tried and tested one. They have however found that the very nature of cyberspace has demanded they apply their minds in creative ways to align IHL and its principles with this virtual world.

3. A PRIMER ON IHL AND CYBERSPACE; IS TRANSPOSITION ENOUGH IN DATA PROTECTION?

3.1. Introduction

In this chapter, I will introduce IHL and give examples of its major principles, namely principles of discrimination/distinction and proportionality. These principles will be briefly discussed and then extended into the idea of how IHL treats civilian infrastructure. I will also consider the question of whether privacy, being the root source of data protection is currently protected by IHL. Subsequently, I will then give a short introduction to what cyberspace is and some of the terms that are used in the field with relation to cyber operations. I hope that a by-product of this second discussion is to demonstrate that while the terminology may differ, there is little change between these operations in peacetime and in wartime. These two discussions should ensure that we are on the same page as I then provide an introductory discussion on the current arguments on applicability of IHL in cyberspace. Hints of the complexity of the situation, the impact of the proliferation of Non-State Actors (NSAs) and the idea of declarations of war will be touched on. At this point, I will introduce the concept of transposition and demonstrate its applicability in cyberspace, with the overarching questions of whether this concept suffices with regard to cyberspace, and more precisely, whether it can also be applied with regard to international data protection during belligerency.

3.2. An Elemental Concept of International Humanitarian Law

International Humanitarian Law (IHL), also referred to as *jus in bello*, is a well understood topic in International Law. It governs the conduct of war and has been described as 'humanity in times of war'.[118] It is an ever-evolving conversation about how civilised nations conduct war

[118] Jean-Marie Henckaerts, 'History and sources' in Ben Saul and Dapo Akande (eds), *The Oxford Guide to International Humanitarian Law* (First edition, Oxford University Press 2020). 1

and an increasingly frustrating attempt to balance the war machine and the civilian population's welfare. This ever-evolving nature is because men, and the states they have formed to protect each other, are continuously finding novel ways to kill each other. Where killing fails, then great harm must be inflicted.

Due to this continuous development, the world of IHL is now considered to compose of two types of weapons: kinetic and non-kinetic. The key differentiator being the type of the energy that is used to do the intended damage. Porche provides a simple definition of kinetic weapons as the traditional weapons that cause 'physical, kinetic effects'.[119] While simplified, it might be too simplified as it is possible to cause physical effects with non-kinetic weapons. Porche does further distinguish it by saying that it is a weapon that 'causes destruction of a target by application of a physical force'.[120] Conversely, non-kinetic weapons can be thought of as those weapons that use the transmission of electricity, the diffusion of chemical substances or biological agents or sound.[121] This is a very broad definition that may cause confusion as some of them do require/utilise kinetics e.g. application of biological agents. A better explanation, and the one often used, is that which seems to distinguish them from kinetic weapons. As such, these weapons are often contrasted as kinetic or cyber weapons.[122]

---

[119] Isaac Porche, *Cyberwarfare: An Introduction to Information-Age Conflict* (Artech House 2020) 4.

[120] ibid 22.

[121] Stuart Casey-Maslen, 'Non-Kinetic-Energy Weapons Termed "Non-Lethal": A Preliminary Assessment under International Humanitarian Law and International Human Rights Law' [2010] Geneva Academy of International Humanitariam Law and Human Rights <https://www.geneva-academy.ch/joomlatools-files/docman-files/Non-Kinetic-Energy%20Weapons.pdf> accessed 22 August 2021. 5

[122] There are legitimate arguments for including information warfare and other means of electronic warfare as non-kinetic weapons. See, for example, Martti Lehto, and Gerhard Henselmann, 'Non-Kinetic Warfare: The New Game Changer in the Battle Space' in Brian K Payne and Hongyi Wu (eds), *The proceedings of the 15th international conference on cyber warfare and security* (Academic Conferences International 2020).

Many civilian technologies have a history of starting as military research before being utilised for civilian uses.[123] International humanitarians must then come up from behind and try to plug the emergent resultant holes in IHL. The basic rules of international humanitarian law are accepted as *jus cogens*.[124] These basic rules provide the foundation for keeping military innovations under check. In order to benefit from this god-like status that is already accorded IHL in international law, there is an understandable allure to associate emerging issues with these established basic principles. It does not always make for a fitting glove.

Jus in bello traces its origins to ancient times. For a long period of time, here have been, in one form or another, rules that govern the conduct of war. This field of humanitarianism began its codification as far back as Plato's time, when they included the prohibition of robbing corpses and the destruction of property.[125]

Modern roots of IHL can be traced to the 1860s and two Swiss gentlemen: Henry Dunant and Guillaume-Henri Dufour. After witnessing the horrors of war, they founded, together with three others, the 'Committee of Five' which later became the International Committee of the Red Cross (ICRC). This Committee of Five then organised for a conference in 1864 where the Convention for the Amelioration of the Condition of the Wounded in Armies in the Field was adopted.[126]

Jus in bello has a close associate in *jus ad bellum*. *Jus ad bellum* refers to the law that governs the conditions when a state can resort to war. It therefore, technically, also covers when a state

[123] Alex Roland, *War and Technology: A Very Short Introduction* (Oxford University Press 2016) 90.

[124] Carlo Focarelli, *International Law* (Edward Elgar Publishing 2019). 231

[125] Jonathan Crowe and Kylie Weston-Scheuber, *Principles of International Humanitarian Law* (Edward Elgar 2013). 3

[126] 'What Are the Origins of International Humanitarian Law? | The ICRC in Israel, Golan, West Bank, Gaza' <https://blogs.icrc.org/ilot/2017/08/07/origins-international-humanitarian-law/> accessed 6 July 2021.

cannot resort to war. Both *jus in bello* and *jus ad bellum* are relevant when cyberwarfare is to be considered but the focus of this paper remains *jus in bello*.

3.2.1. Principles of Distinction and Proportionality

It is necessary to understand, in brief, what some of the major principles of IHL are. This is because I seek to illustrate the idea of transposition of IHL into cyberwarfare by referring to them. A fitting listing of the main principles are to be found in Heinsch's work that conveniently focuses on the cyberspace aspect of IHL. In it he lists five main principles, these are: Principle of distinction; Principle of proportionality, Principle of necessity, Precautions in attack, and Prohibition against unnecessary suffering.[127] To these, and based on a higher-level breakdown, Kolb adds the principle of humanity, and principle of limitation.[128] I happily recommend Kolb's work for a deeper look at these principles and their background and relationship. I will proceed to briefly elucidate on the principle of distinction and the principle of proportionality.

The **principle of distinction** can apply in two different scenarios. The first considers persons and applies such that there should be a distinction between combatants and civilians. The second considers objects and applies such that there should be a distinction between civilian objects and military objectives. While seemingly straightforward, these two perspectives can get complicated as war is increasingly fought in areas where this distinction is not immediately clear or, more likely, is purposefully obfuscated. The principle of distinction is firmly set in

[127] Robert Heinsch, 'Methodology of Law-Making: Customary International Law and New Military Technologies' in Dan Saxon (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff Publishers 2013). 17

[128] Robert Kolb, *Advanced Introduction to International Humanitarian Law* (Edward Elgar 2014). 78

IHL and is considered as one of the *jus cogens*.[129] It is regarded as the first among equals. It may be the reason why conversations on distinction are innumerable and indefatigable.

In international armed conflict, this principle of distinction is to be found in Article 48 of the Additional Protocol I (AP I). This clearly states the principle and differentiates between the above mentioned two perspectives of persons and objects. The principle is then buttressed by Articles 52(1) and 52(2) of the AP I which focus on the application of the principle to civilian objects.

The **principle of proportionality** is intricately tied to the idea of the minimisation of civilian death and injury. It demands the consideration of non-combatants in all military decisions being made, with the objective that such consideration will result in decisions that will reduce the harm to these non-combatants. Proportionality, like distinction, also applies to both persons and objects. With reference to objects, there should be a proportional pay-out to military attacks that minimises damage to civilian objects vis-à-vis the legitimate military objective/advantage of the attack or defence.

In international armed conflict, this principle of distinction is to be found in Article 51 (5)(b) which provides the main statutory basis for this principle. The proportionality here is referred to as a balance of 'excessive in relation to concrete and direct military advantage'. This provision is also buttressed by Article 57 (2)(b) which governs the considerations where a military objective is to be attacked.

3.2.2. IHL's Treatment of Civilian Infrastructure

The idea that there is infrastructure that is purely of a civilian nature and from which there is no tangible benefit to attacking it militarily is another bedrock of IHL. This is an extension, or

[129] Heinsch (n 108) 38.

indeed, an expression, of the principle of distinction that has just been discussed. In this previous mention, I drew attention to the existence of two limbs of this protection: persons and objects. The discussion of persons, while relevant to IHL, is not within our purview. We shall instead focus on the issue of objects. However, for context, the protection of these two are premised on largely the same IHL laws.

Article 52(1) of AP I states that 'Civilian objects shall not be the object of attack or reprisal'. The rest of Article 52 of AP I then proceeds to attempt to contextualise the prohibition of attack and reprisal. It applies a restrictive definition of what a military object is while designating a wider residual definition of civilian objects.[130] This serves the purpose of future-proofing the definition of civilian objects. As previously mentioned, a look at Article 48, AP I, will provide the basis of Article 52. Similar protection is offered by Article 8 (2)(b)(ii) of the Rome Statute. This designates intentional attacking of civilian objects as a 'war crime'. The Statute however requires that there be a 'serious violation'. There are several cases in which the principle of protection of civilian objects has been applied. These include the south African Case of Boeremag case. .[131] In this case, the judge reiterated that 'only the targeting of military objectives is permissible'

In order to understand the principle of distinction, it is necessary to be able to clearly identify the differences between a military object and a civilian object, and therefore civilian infrastructure. The aforementioned idea of residual definition comes into play to allow for a wider range of not only civilian infrastructure, but more interestingly, in which instances military objects can, and indeed should, be treated as civilian objects. Article 52 (2) of the AP I introduces the two additional criteria of 'contribution to military action' and 'military

[130] Kolb (n 109) 157.

[131] Judgement delivered by the North Guateng High Court on 26th August 2010 pp. 70

advantage'. The expectation is that context plays the greatest role in determining what civilian infrastructure is.[132] Some experts prefer to summarise it thus: Where there is doubt, then assume it is civilian infrastructure.[133] Makes it easy on paper, but not any easier in practice.

Confusing? Yes it is, and so it shall remain. The main reason for this is the everchanging nature of war and the tools used for warfare. It should be expected that the intangible components of computer networks will bring even greater confusion when put to this triple-test of not being a civilian object, not contributing to military action, and whose attack would offer a military advantage.

3.2.3. IHL and Privacy

As indicated in this chapter's introduction and in Chapter 2, there is an accepted relationship between data protection and privacy, with the former being considered as being an offshoot or derivative of the latter. Given that I have also posited, and it is indeed the situation, that IHL does not stretch itself into the real of data protection, it would be necessary to consider the question of whether the traditional right to privacy, in itself, is accorded respect in IHL.

Should there be an expectation of privacy under the current accepted IHL rules, then the question of extending or transposing these protections to data protection would be much easier to argue.

By itself, privacy is not considered as an issue protected by IHL. The various aspects of privacy may however be protected, not necessarily as privacy issues, but as single issues to be handled. A good example is that to be found in how Article 25 of the fourth Geneva Convention provides for a right to family correspondence of a strictly personal nature. Personal correspondence, and indeed family correspondence, is considered to be an aspect of privacy as exemplified by article

[132] Kolb (n 109) 159-160.

[133] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012). 196

31 of Kenya's constitution. However, the provided protection is not geared towards the right to privacy but rather the right to communicate. Concerning protected persons, article 27 of the fourth Geneva Convention provides for the respect for their persons, their honour, their family rights, their religious convictions and practices, and their manners and customs. This protection, and the additional ones highlighted in this article, contain aspects of privacy but again without highlighting privacy by itself. On the other hand, Article 16 of the first Geneva Convention mandates the compulsory recording of personal data, including medical information. This is an obvious breach of traditional (civilian) data protection laws.

Privacy is by itself not directly protected by IHL and that a situational consideration of each situation ought to be done should a scenario come up. It would however be a fallacy to equate privacy and data protection, for whatever purpose. As indicated in chapter 2.4, the historical development of data protection from privacy and its continued consideration as a component of privacy is set in stone. They are however not synonymous, and care should be taken to not presume that a lack of coherent protection of privacy in IHL indicates that data protection is not deserving of IHL's consideration. Data, due to its dual use nature, goes beyond individual's privacy and into many more innumerable implications.

3.3. Is International Cyberspace regulated?

In August 1949, the most recent Geneva Conventions were adopted. There were additional protocols adopted in 1977.[134] It goes without saying that this was way before computers were thought of as the tools they have become today. Indeed, the use of the word 'cyber' was first

[134] The third additional protocol was adopted in 2005 but is not substantive in regards to IHL as it mainly covers the emblems that are used within IHL.

noted in the Oxford English dictionary in 1961, and it did not translate to what is thought of as cyber today.[135]

Cyberspace, according to the United States' Department of Defence, refers to 'a domain that consists of the interdependent networks of information technology infrastructures and resident data, including the internet, telecommunications network, computer systems, and embedded processors and controllers'.[136] Pretty long definition for something most of us will presume to know. However, it does play an important role of demonstrating the various aspects of digital infrastructure that are relevant to military minds. Amongst them, is data; here it is referred to as 'resident data'.

One of the main challenges of cyberspace is trying to classify what is going on in regard to the types of cyber events. This classification would play a very important role in IHL as it would help to predetermine whether an event even meets the minimum criteria for IHL to apply. Cyber operations are defined by the UK Ministry of Defence as 'the planning and synchronisation of activities in and through cyberspace to enable freedom of manoeuvre and to achieve military objectives'.[137] Cybersecurity is the protection and defending of cyberspace.[138] Of note is that it does not refer to the physical protection of these assets despite the fact that physical security is very important in the greater scheme of things.

A cyberattack can be defined as 'An electronic attack to a system, enterprise or individual that intends to disrupt, steal or corrupt assets where those assets might be digital, digital services or

[135] 'The Bizarre Evolution of the Word "Cyber"' (*Gizmodo*) <https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487> accessed 18 July 2021.

[136] Porche (n 100) 11-12. Page 13 of this book has a clear illustration of the space that cyberspace occupies in the larger information space and their different components.

[137] ibid 18.

[138] ibid 15.

physical assets with a cyber component.'[139] This is a broad definition and, as we see in a bit, is not to be confused with the idea of an attack in IHL. Therefore, for purposes of IHL, there are some cyberattacks that would not reach the threshold of an attack. Cyberwar has been defined as 'An extension of policy by actions taken in cyberspace by state or nonstate actors that either constitute a serious threat to a nation's security or are conducted in response to a perceived threat against a nation's security.'[140]

A key characteristic of cyberspace conflict is that there is little difference between the behaviour of belligerents before and during a conflict. The low cost of entry coupled with the easy anonymity that is an intrinsic character of this type of war means that attribution to nation states is complex, if not impossible. Consequently, nations have little incentive to declare war in cyberspace. Indeed, even in the traditional spheres of war, nations have been increasingly reluctant to declare war. Fazal explains that this disincentive is directly related to the increase in codified *jus in bello*.[141] According to him, it has become too 'expensive' to formally declare war and cyberspace presents rather strong attributes to support acts of war without declarations of war.

A direct answer to the question of whether international cyberspace is regulated is yes.[142] Most regulations are considered to apply to cyberspace as well as they do in the physical world. This

[139] Duncan Hodges and Sadie Creese, 'Understanding cyber- attacks' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 34.

[140] Paulo Shakarian, Jana Shakarian and Andrew Ruef, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress 2013).

[141] Tanisha M Fazal, 'Why States No Longer Declare War' (2012) 21 Security Studies 557. 557

[142] François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 1. See also Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013). 13

includes public international law. The entire body of public international law is huge and there are obviously sections of it that will not apply, mainly due to the nature of the laws themselves. However, where there is a confluence, it may be necessary to then apply such sections. For example, the United Nations Convention on the Law of the Sea (UNCLOS) will obviously have little to do with cyberspace. However, UNCLOS has huge impact on sovereignty. and it may be necessary to determine sovereignty in relation to acts that have impacted cyberspace. It also has an impact on the nationality of ships which may in turn impact attribution of acts done in cyberspace from such ships.

Tsagourias notes that the application of law in cyberspace is deeply political.[143] This is especially so in international law where there is neither a central body to create rules, nor is there one to enforce any existing laws. This is a major source of the frustration with the international regulation of cyberspace. Nations states have become politically savvy and are less eager to enter into binding international treaties, especially in areas that are not yet of great concern to their domestic audiences. Areas like international cyberspace.[144] Further below, I give a brief of the United Nations Group of Governmental Experts (UNGGE) process, which process faced several challenges at a basic level such as the attempt to answer the key question, 'Does international law apply to cyberspace?'[145]

[143] Nicholas Tsagourias, 'The Legal Status of Cyberspace' in Njcholas K Tsagourias and Russell Buchan (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015). 14

[144] Marco Sassòli and Patrick Nagler, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019). See 10.116

[145] ibid. See 10.110. Here the authors lay blame squarely on China and Russia and their unwillingness to clarify the relationship between IHL and cyberspace.

The Tallinn Manual describes the applicability of international law to cyberspace as 'unsettled'.[146] It then proceeds to set the mood for a 282-page treatise on the applicability of international law to cyberspace. Their main take is that the space is regulated and that the various already existing laws do apply to it. Of course, as mentioned earlier, it is easier for experts to try and squeeze the existing laws by stretching them into new areas like cyberspace than it is for them to wait around for politicians to agree on new ways to restrict their own sovereignty.

In the Tallinn Manual 2.0, the author group of experts considers issues like sovereignty, jurisdiction, state responsibility, application of IHL and a host of other interesting subjects. These topical areas are then looked into in detail and where there is consensus, the manual declares the international law that applies and how it applies. For example, under the aforementioned issue of civilian objects/infrastructures, the manual clearly points out that Article 52(1) will apply but only where such cyberoperation qualifies as an attack. Then it delves into scenarios where a cyberattack would be considered to have occured. Case-by-case is the operative phrase.

In this case-by-case attempt to check on the applicability of international law, a lot of attention is paid to the fact that while cyberspace is talked of as a separate area to be regulated, it practically consists of already regulated domains. There is then an academic attempt to apply the various rules from these regulated domains into cyberspace. With the Tallinn manual, the authors were able to agree on a lot and decided to then shelf the portions that were not agreed on for future debate.

[146] Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013). 3

Of note in this area are the efforts to get consensus, at an international law level, on the question. The United Nations Group of Governmental Experts (UNGGE) in the Field of Information and Telecommunications in the Context of International Security gave reports in 2013 and 2015 that essentially concluded that international law does apply in cyberspace. The UNGGE is comprised of a geographically and regionally balanced group of experts, appointed by their governments. They however work in their personal capacities.[147] This group debates the subject matter and issues a report. In the case of the above-mentioned group, one of the matters they looked at is how international law applies in the ICT field with respect to States. Like the Tallinn group of experts, they are also divided on the manner in which different aspect apply when it comes to the practical side of the law.

The UNGGE's work is supplemented by the Open Ended Working Group (OEWG). The OEWD was established in 2018 as a way to include more states in the conversation that was initially led by the UNGGE. While the UNGGE consists, at any point, of 25 states that have been invited to join, the OEWG is comprised of any UN member state that is largely interested in the ongoing work of the OEWG. However, the two have similar mandates in terms of the areas of work and this includes the relationship between international law and cyberspace. The phraseology used by both groups is 'advancing responsible State behaviour in cyberspace'.

In their 2021 report, the OEWG also reiterated 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 ICT environment'[148] They

[147] 'Group of Governmental Experts – UNODA' <https://www.un.org/disarmament/group-of-governmental-experts/> accessed 20 July 2021.

[148] UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security, 'Final Substantive Report' (10 March 2021) A/AC.290/2021/CRP.2. See paragraph 34.

however, also had the rider that 'further common understandings need to be developed on how international law applies to State use of ICTs'.[149]

As such, there is an ongoing challenge in regard to the legal regulation of cyberspace.[150] If the debate so far is to be summarised, we can state that international law does apply in cyberspace, and it does govern cyber operations. However, we are not sure how it applies, and neither are we sure if all of its relevant portions apply. The fact that it has not yet been tested in decision-making bodies might have a lot to do with this vague lacuna.

3.4. Mutatis Mutandis: Does Transposition Suffice?

It is clear that international law applies. It is also clear that its application needs to be reviewed on a case-by-case basis in order to decide if the situation being considered is covered by the law being proposed. What I have not touched on is the methodology employed once this applicability decision is made.

Mutatis mutandis is an alliteration that makes most new law students smile. It rolls off the tongue and is pretty easy to remember in a year full of new Latin phrases. It means 'all necessary changes having been made'.[151] It however literally translates to 'things having been changed that have to be changed'.[152] Its application is along the lines of analogy, in that when given two situations, the second one would be treated in the same way with only the necessary

[149] UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security, 'Final Substantive Report' (10 March 2021) A/AC.290/2021/CRP.2. See paragraph 34.

[150] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017).

[151] Bryan A Garner and Henry Campbell Black (eds), *Black's Law Dictionary* (9th ed, West 2009). 1115

[152] 'Definition of MUTATIS MUTANDIS' <https://www.merriam-webster.com/dictionary/mutatis+mutandis> accessed 20 July 2021.

changes being done to allow it to be treated in that manner. For example, If I say that provisions of the first contract with supplier A should apply *mutatis mutandis* to a second one with supplier B, then we might change the title of the second one, update its validity dates, or update its parties. However, the rest will, by and large, remain the same.

For simplicity, I shall refer to this phenomenon as transposition. Yet in doing so, I shall not be the first one to call it so. In his paper title 'Law as Transposition', Esin Örücü argues that transposition is a more apt term to the more common term 'legal transplant'.[153] He explains it as a phenomenon where a legal rule is used in a recipient legal system as it was in a donor legal system and that transposition is then done to suit the particular socio-legal culture in the recipient legal system.

A ridiculous example will hopefully make things clearer. Let us say Country A has a law that requires all dogs to be fed at exactly 09:15 p.m. and by a person dressed in trousers and a white shirt. Country B is a neighbouring country where trousers are culturally discouraged, and dogs viewed as religiously unacceptable as pets. They therefore have more cats as pets and would like to adopt this law. They would then transpose it such that their law would require that all cats be fed at exactly 09:15 p.m. and by a person dressed in a robe and a white shirt. The law from country A will apply to country B, *mutatis mutandis*. It will have been transposed to allow for the required socio-legal culture in country B.

The phenomenon, in itself, can be found in comparative law, where it is referred to as a 'legal transplant'. Legal transplants are studied in comparative law as a method by which legal norms

[153] Esin Örücü, 'Law as Transposition' (2002) 51 International and Comparative Law Quarterly 205.

are transferred from one legal system to another.[154] It is mainly associated with Alan Watson who premised that a society's laws are often borrowed from other societies rather than being a development of that society.[155]

Away from the country perspective of a legal system, the idea of transposition is being applied as between different legal fields. It is such attempts that have seen the main principles of IHL being transposed into cyberspace, and as set out by Jan Smits, the importance of imitation and transplants in the legal field is already well established.[156] Despite Örücü according similar explanations to both transplants and transpositions, I prefer to use the term transposition so as to avoid this long established idea in comparative law of legal transplants being done across societies.

3.4.1. Transposition of IHL into the regulation of cyberspace

The idea of cyberwar excites the mind. How to impact the enemy from thousands of miles away, anonymously, seated next to a gorgeous person, on the beach, and with a drink in hand. The premise has been overplayed in movies but in the world of IHL, it is a relatively new prospect. This is hinted at by what can be considered to be the ultimate bible on the interaction between these two otherwise disparate fields; the Tallinn Manual and the Tallinn Manual 2.0.[157] The first manual was exclusively based on cyber warfare (and therefore IHL) while the second

[154] Claudio Corradetti, 'Can human rights be exported? On the very idea of human rights transplantability' in Antonina Bakardjieva Engelbrekt and Joakim Nergelius (eds), *New Directions in Comparative Law* (Edward Elgar 2009). 40

[155] Alan Watson, *Legal Transplants: An Approach to Comparative Law* (University Press of Virginia 1974).

[156] Jan M. Smits, 'Rethinking Methods in European Private Law' in Maurice Adams and J Bomhoff (eds), *Practice and Theory in Comparative Law* (Cambridge University Press 2012). 182

[157] There are currently two Tallinn Manuals: Tallin Manual and the inspiringly named Tallinn Manual 2.0. The premise behind the two manuals is that unaligned experts were asked to discuss and agree on how cyberwarfare is regulated. They put down the issues they agreed on but left out those they disagreed on. Thus, the issues agreed on ought to form a starting point on the discussion and push the conversation forward.

one is more general with discussions about cyber operations (and therefore includes peace times).

In the introduction to the Tallinn Manual, the project director sets the main question of the Manual as being 'whether the existing law applies to cyber issues at all, and, if so, how'.[158] This introduction then proceeds to give a detailed explanation of the pains the Manual's group of experts went to in order to simply apply the existing IHL principles to this field of cyberwarfare.

The idea that the introduction of new technologies provides opportunity for circumvention of current extant protections in IHL is a no-brainer. A general outline of the steps that would be taken by the IHL community whenever there is an emerging threat to the already established wars would like something like this:

(1) Understand the (potential) use and impact of the new technologies in war.

(2) Debate the applicability of current IHL laws to these technologies.

(3) Identify gaps that do not seem properly covered by current IHL.

(4) Lobby for alternative laws to cover the gaps.

(5) Incorporate the entirety of the new field into the conversation on alternative laws.

Robert McLaughlin and Hitoshi Nasu hint to this in the historical context by explaining that the initial shock and awe of new technologies being employed in war would act as a 'midwife' that would trigger re-evaluation of what was considered fair, chivalrous, or honourable on the

[158] Schmitt, '*Tallinn Manual*' (n 127) 3.

battlefield.[159] Their contention, to which I fully subscribe, is that this is no longer applicable to the rapid nature of advancement that current technologies are undergoing.

As previously mentioned in this paper, it is the combination of the slow-moving nature of the creation of international law and the secretive nature of cyberwarfare that form a tag team to prevent quick movement through these listed steps. Above all these, is the reluctance by modern nations to be encumbered by regulations in these new frontiers.

It is at such junctures of the interaction with new technologies, in particular, those of the dual-application nature that transposition then plays a key role. For transposition to properly apply, it is necessary for there to exist irrefutable principles in the source field of law. In our case, these would include the two principles of IHL as I have earlier mentioned and given examples of. The two principles of distinction and proportionality are irrefutable in IHL. In addition to these two, the idea of civilian infrastructure also provides little room for argument in the application of these principles. Secondly, there also needs to be what seems like a lacuna in the target legal field.

3.4.1.1. Transposition's resultant conundrum.

A key example of the pitfalls of transposition when it comes to cyberspace and the application of IHL is the definition of what an 'attack' is.

Article 49 of AP I sets out what the standard understanding of an attack is: 'acts of violence against the adversary, whether in offence or in defence.' The importance of what the definition of an attack is in IHL cannot be underestimated. While the law of armed conflict delves into

[159] Robert McLaughlin and Hitoshi Nasu, 'Conundrum of New Technologies in the Law of Armed Conflict' in Robert McLaughlin and Hitoshi Nasu (eds), *New Technologies and the Law of Armed Conflict* (1st ed. 2014, TMC Asser Press : Imprint: TMC Asser Press 2014).

the issue at a more fundamental level, IHL also provides important restrictions that can be triggered by whether an attack has happened or if it is imminent.

The Tallinn Manual responds to this using their typical transpositional approach.[160] Rule 30 of the Tallin Manual attempts to define what a 'cyber-attack' is. It clearly states that 'non-violent operations, such as psychological cyber operations or cyber espionage, do not qualify as attacks'.[161] In response to the ethereal nature of cyberspace, the experts make the 'effect' or 'consequence' argument.[162] The consequences of a cyber operation will determine whether or not it shall be considered as an attack, for purposes of application of the IHL rules.[163] As such, a violent attack is one in which there are violent effects/consequences. So far, this makes good sense and seems to be not only easily transposed, but also arguably defensible amongst those who understand IHL.

However, the departure comes in when the issue of data is considered. To be clear, the Tallinn Manual explains that data-targeting operations can rise to the threshold of an attack if there is a consequential injury or death of individuals or the damage/destruction of objects.[164] On the other hand, data in itself does present challenges by its very nature. [165] For example, data is capable of replication without diminishing the original. In civilian data protection, the principle

[160] Sassòli (n 125) 59. The authors of this book explain it as 'it applies the existing rules to this new domain'.

[161] Schmitt, '*Tallinn Manual*' (n 127) 107

[162] Seumas Miller, 'Cyberattacks and "Dirty Hands": Cyberwar, Cybercrime, or Covert Political Action?' in Fritz Allhoff, Adam Henschke and Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press 2016) 231-232

[163] Heather A. Harrison Dinniss, 'The regulation of cyber warfare under the jus in bello' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 129.

[164] Schmitt, '*Tallinn Manual*' (n 127) 108.

[165] Sassòli (n 125) 532. Here the authors state that even the mere deletion of data can be considered as damage and destruction.

of accountability takes care of this nature by placing responsibility on a person legally identified as the data controller. Replication, by itself, is prima facie evidence of breach of this responsibility.

Indeed, Seumas Miller identifies four types of consequential harm that may result from cyberattacks.[166] Physical/Psychological harm that is experienced by human beings, destruction of physical objects and the environment; cyberharm that destroys software and data; and institutional harm that undermines confidence in institutions. He recognises that the first two have a different threshold of the consequence/effect at which they can be considered an attack for purposes of war, when compared to the last two. How then does one apply transposition where the source seemingly requires a violent effect or consequence? The glove does not fit.

A transpositional approach is difficult to maintain where there is no effectual damage. Where the data is stolen by a belligerent but there is neither harm nor violence used or effected, is the offending nation state (the one that carried out the operation) free from both responsibility and countermeasure? Should the victim state wait for harm or violence to consequentially occur before the right to self-defence or countermeasures can be triggered? Indeed, Sassòli and Nagler criticise this attempt to consider the quantum or extent of damage as being 'difficult to reconcile' with the Geneva laws which talk of 'violence'.[167]

A different scenario that resists transposition has to do with the persistence of data. A belligerent nation can target military combatants, or civilians supporting military operations, under the rules of proportionate response and distinction. This can, without stretching the imagination or commenting on legality, include the collection of personal data of such combatants. This imagination needs even less further stretching when the use of asymmetrical

[166] Miller (n 143) 232.

[167] Sassòli (n 125) 536.

warfare and non-state actors in cyberwarfare is considered. For purposes of this argument, a more benign source of this data might be, for example, data collected on prisoners of war.

The persistence of data means that this data continues to be available to the collecting nation even after such combatants become civilians. Is it then justified to continue keeping this data? Should IHL even care whether or where this data exists? Does the dual nature of data (civilian and military) then require that active combatants be simultaneously recognised as civilians for purposes of protection of their personal data even while they are still combatants? Is the disruption of the personal lives of combatants, where such disruption would provide a military advantage, through the use of their personal data, a legitimate response in belligerency? For example, can the purchase history of an effective commander be 'leaked' in order to make their continued leadership untenable and reduce support for the army?

In international data protection, such issues can be taken care of through the principles of purpose limitation and storage limitation. The first will require that only necessary data be collected and that collected personal data be utilised for the specific purpose it was collected. The second will require that data be retained only for as long as is necessary to complete the purpose for which it was collected. These concepts are, obviously, unknown to IHL and, more crucially, there is nothing to then transpose them from.

Transposition gets even more complex when the unstated but obviously evident fact that cyber espionage is a continuous activity that is done before, during and after belligerency is considered. Given that data is the consistent target of this espionage, the general conclusion that data is outside the ambit of IHL leaves the key question of 'in which field of law does it lie?'

3.5. Conclusion

The idea that there is a lacuna is, at this time in the development of regulation of cyberspace, unarguable. The key question remains which laws apply when and where, especially when IHL is being considered. The main principles of IHL apply. They apply through obvious consideration of the main purpose of IHL, the humanisation of war. Declaration of application is however not enough. Any average legal mind will see as many loopholes in that declaration as there are full stops. As such, transposition has been the greatest weapon that IHL practitioners have had in expanding the reach of IHL into cyberspace.

A most excellent summary of the problem is done by Taddeo and Glorioso who describe the challenge as being deeper than a simple question of interpreting cyber into current IHL [what I refer to as transposition]. To them it is whether IHL at its most basic, normative, and conceptual framework level can satisfactorily and adequately handle the medium and long-term changes prompted by cyber.[168] I further ask whether it can handle even the short-term changes prompted by data.

In the case of the Legality of the Threat or Use of Nuclear Weapons, the ICJ got a chance to address the issue of applicability of already established IHL rules to what was a new domain of law.[169] They recognised that nuclear weapons were not a consideration in the IHL rules as the main principles pre-exist them and the rules put in place after the codification of the Geneva laws simply left them out. However, the idea that IHL would consequently not apply was wrong

[168] Ludovica Glorioso and Mariarosaria Taddeo (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017) x.

[169] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996, available at: https://www.refworld.org/cases,ICJ,4b2913d62.html [accessed 2 August 2021]

because ‘such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present, and those of the future.’[170]

The question of whether transposition suffices with data protection scenarios during belligerency is best answered by looking at the nature of data and the effectual honey pot this nature causes it to be.

[170] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226. Paragraph 82.

4. CYBER WARFARE'S INESCAPABLE EVOLUTION TOWARDS DATA.

4.1. Introduction

In this chapter, I will focus on data and why it is the next frontier for cyberwarfare. While IHL is still treating cyberwarfare itself as being a new arena, the allure of data is such that it is already a sought-after commodity in cyberwarfare. I will begin by proposing reasons why data is altogether a different concept when it comes to warfare, and therefore IHL. Some of its unique characteristics will be explored, accompanied by illustrations of the exploitation of some of these characteristics in previous cyber-attacks. I will then touch on the international data principles as they currently exist. These principles offer a conversational starting point for incorporation of data protection into IHL without the necessary use of transposition. I will finally explain that digital identities are implementations of data and give examples of how they have been implemented in different countries and their uses. Here, I will illustrate, through the use of digital identities, the pervasiveness with which critical data infrastructures are being implemented and thereby, the dangers that ignoring this issue, of data during cyberwarfare, continues to pose in what might soon be the biggest theatre of war. An understanding of these three issues will no doubt make it clearer that cyber warfare is already targeting data, that it is better regulated by considering international data protection as more suited to its characteristics, and that this data's implementation as digital identities is a lucrative honeypot that will be targeted.

4.2. Sui-generis character of data

At this stage, I hope that it is evident that not only is data one of this age's most important tool and resource, but that it is also governed by a set of international data protection regimes. These are mostly regional or elementary, but they do provide a starting place for a conversation. I also hope that it is clear that these protection regimes do not, in any way, envision the impact of cyberwarfare on this already shaky legal area. Hence the need to look at whether IHL, in

itself and also in its interaction with the wider cyberspace, has an overlap that might apply to data protection during belligerency. So far, I have explained that transposition is the main way that this overlap is considered and developed by IHL practitioners keen on seeing cyberwarfare regulated.

Taking a step back in history, the Gatling gun, famous for the psychological barrier it broke when developed, could fire around 200 rounds per minute.[171] This was around 1860 and it was mounted on a carriage and operated by a gunner turning a crank. The current standard issue firearm for the US army is the M4 Carbine. This M4 has the capability to fire up to 950 rounds per minute. It is a handheld gun.[172] This evolution of weaponry has been experienced in cyberspace as well. Only at a faster rate. As the civilian applications of data became more complex, the end result was the realisation that the most lucrative part of computer systems is their data. The type of data being targeted is also increasingly that which exists in critical civilian infrastructure like healthcare systems, electricity, and water systems.[173]

As data is weaponised, then the data-driven service industry, of which governments are now highly participative in, will be in ever increasing danger. As the IHL community realises the dangers lie not in the actual computer systems but in their data, and as they see targeted data being used in a variety of uniquely destructive ways, then the need to design a protective system focused on this hole will become increasingly apparent. To drive this point home, I will provide

[171] History com Editors, 'Gatling Gun' (*HISTORY*) <https://www.history.com/topics/american-civil-war/gatling-gun> accessed 22 August 2021.

[172] 'Colt M4 Carbine - Army Technology' <https://www.army-technology.com/projects/colt-m4-carbine-assault-rifle-us/> accessed 22 August 2021.

[173] 'Cyber Warfare: IHL Provides an Additional Layer of Protection' (*International Committee of the Red Cross*, 10 September 2019) <https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection> accessed 22 August 2021. The ICRC identifies cyberspace itself rather than data as being in danger.

examples of cyber incidents that have happened that demonstrate the issue. While not all of them, if any, amount to cyber warfare, these examples should indicate the capabilities of cyber operations. There must be a presumption that nations are more capable than the operations listed here.

Sui generis translates to 'of its own kind'. As both a weapon and target of war, data is indeed *sui generis*. Due to its dual-use nature, it is capable of being utilised in almost all domains of war and the war support ecosystem. It is well suited for information and psychological warfare and can also effect kinetic damage. Earlier on, I described what general purpose technology is and the centrality of data as part the computer, one of the world's most impactful general-purpose technology.

It is from this earlier argument that I propose data be thought of as having the characteristics of a general-purpose technology when it comes to warfare. Something that is capable of use in almost all products and processes. From managing war logistics, to managing its human resource. From defensive capabilities to direct offensive capabilities. A present-day army without an effective cyber-strategy has no right to believe itself modern, and an effective cyber-strategy necessitates plans for data. While evident that there are key differences between the tools for kinetic/traditional warfare and those for cyber warfare, allow me to stress on some of those that make data a *sui generis* tool. It is these same differences that make it necessary for a distinct and separate approach towards the regulation of data protection, and indeed cyberspace, from the context of IHL.

Ubiquity

Data is to be found in everything or about everything. The rapid computerisation/digitisation of everything is driving this data-hungry society. The growth of the internet of things (IOT) will undoubtedly lead to the explosion of this character. This then makes the potential for everything to become a weapon. Does it mean your coffee maker will explode? Not really, but

plausibly maybe. It however means that it can be turned into an intelligence gathering machine and the data, both active and passive, can be used directly and indirectly for cyber warfare. Critically, it also means that there is more and more interaction between data and critical military and civilian infrastructure. As you read this, it is unlikely that there is gunpowder next to you. However, there are a lot of data-hungry tools that surround you. To further aggravate the situation, the methods of exploitation of this data are often the same and once learnt can be easily implemented across the board.

In July 2021, there were reports of cyber-attacks on Iran's transport system. However, instead of attacking the transport means themselves, the hackers attacked the messaging board system and posted false delay and cancellation messages.[174] They also reportedly posted the Ayatollah's (top political and religious leader) phone number and asked that calls be made there for further information.

Replicability

This is perhaps the most distinguishing feature of data. The idea that it can be replicated without causing any sort of diminishing effect on the original. Add to this the automation of this replication and the ability to draw similar insights from the replicated data, and you have a tool that has been perfectly designed for military exploitation. This idea of quick and low-resource intensive replication has been a key disruptor in other industries. It has, for example, changed the entertainment industry from a sales business to a subscription model. For warfare, it means that once a cyber-weapon has been created, it is very cheap to replicate it. It means that data can be accessed without the source knowing about it. It means that misinformation can be

[174] David Rose, 'Hacked Train Screens Tell Iranians to Call Ayatollah' <https://www.thetimes.co.uk/article/hacked-train-screens-tell-iranians-to-call-ayatollah-9m2j0h0mk> accessed 23 August 2021.

spread without extra effort on the part of the disruptive party. It means that data that has been interfered with can be used in various applications without anyone being the wiser.

The replicability of cyber weapons can be seen in the Eternal Blue hack. In this case, America's National Security Agency (NSA) developed a cyber weapon called Eternal Blue that they used for cyber-attacks. In 2017, this weapon was itself stolen and then released online by a group called 'Shadow Hackers'.[175] It has now been used offensively by different parties to hack others, including Americans, whose protection is a key mandate for NSA.

In terms of data being copied, and closely related to sensitive military information, in June 2021, there were reports of a leak of the personal details of 1182 British soldiers who are members of the UK's special forces.[176] Although not confirmed if it was inadvertent or a cyber-attack, the list was copied and spread through WhatsApp to several unauthorised persons even before the soldiers themselves were aware.

Remotely accessible

There is no other weapon or target of war that is as difficult to protect as data. The fact that as a weapon it can be activated from anywhere in the world, including from friendly nations' cyberspace, is being heavily exploited. Remote access is hard to do with traditional weapons, and indeed, where possible, it is due to the addition of data-driven capabilities into these weapon systems.

In June 2021, there were American reports that Chinese hackers had targeted, and breached software used to remotely access networks for, among other companies, the Metropolitan

[175] 'When Cyberweapons Escape' (*The Cipher Brief*) <https://www.thecipherbrief.com/column_article/when-cyberweapons-escape> accessed 23 August 2021.

[176] 'British Armed Forces' Data Breach Exposes Identities of over a Hundred Special Forces Troops | Leigh Day' <https://www.leighday.co.uk/latest-updates/news/2021-news/british-armed-forces-data-breach-exposes-identities-of-over-a-hundred-special-forces-troops/> accessed 23 August 2021.

Water District of Southern California.[177] This company is described as providing water to over 19 million people and as operating some of the largest water treatment plants in the world.

Scalability

Data can grow and it does grow. In most systems, the scale is exponential. What starts as one small project to achieve a specific goal suddenly grows to huge levels as the data collection continues over time and, more importantly, the potential for exploitation of the data is realised. The system gets more and more components, and this new data gives birth to even more need for data.

Modern warfare makes increased use of drones. These form data gathering equipment that can include live video. Advancements have resulted in systems like the Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS). This project, for example, has evolved to the point where a single drone can capture, stream, and store the equivalent of 5,000 hours of high-definition video in the form of 1,000,000 terabytes of data, in a single day.[178]

Longevity

Data lives forever. In its original or replicated media, it is very hard to destroy once it has been put in digital form. As such, it is conceivable that data collected today will be available for an extreme length of time. Although old data might lose some of its utility, with personal data, the value might remain the same. This is because of data mining tools that can be used to link new personal data to previous ones and also because in some instances, the personal data remains

[177] Alan Suderman, 'MWD among Targets in Large-Scale Cyber-Espionage Hack Blamed on China' (*Los Angeles Times*, 15 June 2021) <https://www.latimes.com/world-nation/story/2021-06-15/critical-entities-targeted-suspected-chinese-cyber-espionage> accessed 23 August 2021.

[178] 'Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS)' (*BAE Systems | United States*) <https://www.baesystems.com/en-us/product/autonomous-realtime-ground-ubiquitous-surveillance-imaging-system-argusis> accessed 8 September 2021.

the same throughout the life of a data subject e.g. an identification card number or a birth certificate number, or biometric data.

Unregulated
The lack of concrete regulation of cyberspace and, more critically, of data as tools of war make it a lucrative option for development. It also increases the opposition to its regulation. Its low-cost high-impact political and reputational resourcing has no similar likeness in the world of warfare

4.3. International data protection principles

A major premise of the argument being made in this paper is that international data protection should be the source for the rules that are used by IHL during belligerency. This would be diametric to the current scenario where cyberspace is sourcing its belligerency rules from traditional IHL through the process of transposition. A good starting point for proposals of these rules is to be found in the data protection principles.

A key differentiator of data protection principles is that they are focused on the data subject.[179] The data subject would ordinarily refer to the person whose personal data is being processed. It is this individual-centric approach that makes these principles a good place to start the conversation of what kind of data protection should be given to persons during cyberwarfare. This is not to say that the rights and roles of other players (for example data processors) are ignored in international data protection, but rather, they are put forward via other tools within the data protection regimes. For example, data processing authority provisions cover the roles of regulators.

[179] Aurelia Tamò-Larrieux, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (1st ed. 2018, Springer International Publishing: Imprint: Springer 2018) 76.

Below, I give a small brief, and, in some cases, an example of what their implementation in cyberwarfare would look like. In order to wade through the very many different wordings and listings of the same principles, I will use those that appear in the GDPR.[180] It should be recalled that these principles are similar to and drawn from the OECD Guidelines and Convention 108 as mentioned earlier.[181]

At the end it will be obvious that not all of these principles are easily adopted into IHL. It will also further clarify that transposition, in itself, does not provide a way to properly handle issues related to data. Something else of note is that the concept of placing all the burdens of a data controller on a military in active combat may be, practically, illusionary. However, these principles provide an excellent starting point for the conversation on what happens to data protection during cyber warfare.

4.3.1. Principle of lawfulness, fairness, and transparency.

Lawfulness refers to the idea that the processing of all personal data should conform with the set-out laws that apply. These legal obligations may be general, specific, statutory, or contractual.[182] The idea of fairness has to do with the way the data is obtained, or the way information concerning the processing is provided to the data subject. Transparency has to do with disclosure of the fact that particular personal data is being collected for purposes of specified processing.

---

[180] Article 5, GDPR

[181] Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2019) 311. See also Bart Custers and others, *EU Personal Data Protection in Policy and Practice* (1st ed. 2019, TMC Asser Press: Imprint: TMC Asser Press 2019) 4.

[182] Brendan Van Alsenoy, Aleksandra Kuczerawy and Jef Ausloos, 'Search Engines after "Google Spain": Internet@Liberty or Privacy@Peril?' [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2321494> accessed 10 August 2021.

This principle is not readily capable of transposition from IHL. It requires that the ideas behind its adoption be carefully considered and translated into the cyberwarfare arena. IHL does have remotely similar rules, including that of perfidy. Perfidy, in itself, is a big issue in cyberspace especially due to the anonymity or 'false flag' aspects of this field. However, with data protection, the requirement for transparency, for example, goes beyond deliberate misinformation/misrepresentation, and into an honest approach from the beginning of data collection.

At the same time, especially with the understanding that personal data is with reference to natural persons, it is not difficult to imagine belligerency situations that can be supported by personal data. From a traditional IHL point of view, it is possible to separate, and indeed required, the civilian from the combatant and to also recognise instances when a combatant is to be treated as a civilian. While transposition may not be readily available as a tool, the principle in itself, is deserving of inclusion in data protection under IHL.

4.3.2. Principle of purpose limitation

Purpose limitation covers the idea that collected data should not be further processed other than for the purpose it was collected. There is no room for a change of mind, and should there be a different purpose intended, then fresh consent ought to be sought from the data subject. A related limb to this limitation is that this purpose must be communicated. The nexus between the communication of purpose and the strict adherence to processing for this purpose is what satisfies this principle.

This principle is also difficult to transpose from IHL as there is no directly related IHL rule on the same. Stretches can be made to argue that the principle of minimisation in IHL has some similarity to purpose limitation as far as damage is concerned. However, with data protection, it is not only for negative consequences but also with positive outcomes. Purpose limitation does not envision the use of the data, including for positive or beneficial purposes, without

fresh consent. A good example is where personal data is legitimately collected during belligerency, maybe for purposes of tracing of missing persons. Such data should then be used specifically for this tracing and should not find other purposes, including the building of enemy personnel profiles.

As with all things, there are exceptions. In the GDPR, the exceptions can be found in Article 6 (4) and it provides basis for consideration of extraneous processing of personal data. Likewise, it would be expected to hear arguments for, and interesting to see, exceptions that consider the realities of belligerency.

4.3.3. Principle of data minimisation

Data minimisation is the idea that the amount of data collected, and subsequently processed, should not be more that the least amount necessary to achieve the purpose for collection. This minimisation applies in both breath and depth. Therefore, only the type of data needed should be collected, and also, of the type needed, only the minimum amount required shall be collected. Van Alsenoy describes it as adequacy and relevancy.[183]

Another of the principles that does not have an equivalent in IHL. Like with the principle of data minimisation, extremely flimsy relation can be made with the IHL principle of minimisation that calls for the least damage. However, as debunked above, this is negative while data minimisation also applies positively.

4.3.4. Principle of accuracy

This principle calls for data to be precise and updated, where relevant. It is hard to imagine this principle being achieved where the data subject does not know both the type and quality of information being held by the data controller. The direct application of this principle in IHL is

[183] Brendan Van Alsenoy, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019) 36.

hard to imagine. Would it be reasonable to expect a nation that is at war with another to then update its counterpart about the personal information it holds?

Modern translations of cyberwarfare agree that, just like in kinetic warfare, there is a prohibition against indiscriminate targeting of military objectives, lawful or not.[184] This idea of accuracy is however limited in its extension to data. While it would apply to ensure that only the required data is targeted, where lawful, it says nothing towards the need for such data to be precise and updated. Veracity of data would be highly relevant with the data protection principle of accuracy, while for IHL, what matters would be the accurate selection of targeted data.

These are the realities of the nature of data, and the modern blurring of the nature of war. The result is a situation where it is not very easy to tell how some ideas would be applied in a context of IHL. Deliberate deliberations are very much necessary.

4.3.5. Principle of storage limitation

The idea behind this principle is that personal data should be stored for the least amount of time required to utilise it for the declared purposes. After this period, the data should be destroyed. Where one is not sure about the length of this period, then a reasonable date should be set up when the time required can be reviewed.

Key questions would include, for example, should a belligerent get rid of all personal data it has collected at the end of a war? Should it need personal data to achieve a legitimate military objective and it collects this data, should it then get rid of the data after attainment of the objective? Take for example the Korean war armistice. This has been in effect since July 27th

[184] Michael N Schmitt and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017) 455. See rule 105

1953.[185] Therefore, the war is technically ongoing despite the lack of actual hostilities. While an extreme example, it is a reality. As such, and given the high level of technical advances in current South Korea, would the acquisition of personal data for military purposes be an acceptable means of war? If so, should its retention be envisioned to last as long as this war has?

4.3.6. Principle of integrity and confidentiality

This principle is premised on the idea of security of the personal data that has been collected. This principle includes physical security and also imposes a duty to notify for data breaches. The requirement is that the data controller ensures that the physical security of the data is guaranteed. The guarantee is against breech both internally and externally. As such, only authorised officers of the data controller should have access to this data and only while they are legitimately processing it.

The existence of non-state actors in cyberspace is a huge issue as far as integrity and confidentiality are concerned. The ability to confuse and confound enemy objectives through the use of subterfuge, espionage, and perfidy are best done through non-state actors. Indeed, it is unlikely that any other arena of war sees, or will see, more activity by non-state actors than cyberspace. The allure of cloaking attribution, an already complex issue in cyberspace, by the use of non-state actors is too great to resist.[186] This results in direct attempts to manipulate both the integrity and confidentiality of data.

Information and psychological warfare are nowadays carried out through cyberspace. The ability to manipulate ever-increasingly sensitive public opinion can mean the difference

[185] History com Editors, 'Armistice Ends Korean War Hostilities' (*HISTORY*) <https://www.history.com/this-day-in-history/armistice-ends-the-korean-war> accessed 12 August 2021.

[186] Schmitt, '*Tallinn Manual 2.0*' (n 127)83.

between the start of a war and the victory in one. In the discussion on electronic IDs below, I take the view that this critical data infrastructure is open for manipulation. For example, the legality of President Obama's American identity was called to question to the extent that he had to produce his physical birth certificate.[187] Would the manipulation of such personal records during a state of war, for purposes of shortening the war, be allowable?

4.3.7. Principle of accountability

I like to refer to this principle as the 'blame' principle. By default, it places the blame for breach of the rest of the principles on the data controller. The first presumption is that the data controller has a direct obligation to not only adhere to these principles, but to also demonstrate such adherence as and when legally required.

Article 24 of the GDPR uses the phrase 'technical and organisational measures' in relation to the responsibilities of the controller. As such, the controller is tasked with not only putting these measures in place with respect to all the above-mentioned principles, but also, particularly through the principle of accountability, he is tasked with being capable of demonstrating adherence.

Needless to say, this principle does not have a direct counterpart in IHL. Additionally, the good faith required here, especially in a situation like IHL where individual prosecution of personal rights is not envisioned, is almost unprecedented in IHL.

4.4. Digital Identities

The question of what a digital identity is can be simple or complex. There are technical meanings, especially in security engineering. There is also a simpler meaning that can be

[187] 'Barack Obama: "I Was Born in Hawaii"' *BBC News* <https://www.bbc.com/news/av/world-us-canada-13213810> accessed 12 August 2021.

thought of as an application of any of the ordinary meanings of identity, into the digital world. For example, one can have a digital identity through their social media accounts.

In security engineering, a digital identity would refer to the information through which a computer system activates an account.[188] When you visit an internet account, for example, the service provider has your credentials in their system. Providing a copy of these credentials will then allow you to identify yourself to the system and therefore get access to your specific protected account. This is the process of identification. As such, it is possible to have several of these digital identities and each might be represented by a different identification infrastructure. Indeed, for each account, the attributes associated with the identity can be both different and of differing values. I can claim to be of a different age in all my online accounts. These, I would refer to as virtual digital identities.

However, there is a more persistent instance of digital identity that would represent your actual real-world self. Such a digital identity would be a unique instance that is provided by a trusted guarantor rather than the owner of the identity. This trust can then be relied upon by third parties. The process of verification of the identity is, as with virtual digital identities, the process of identification. For simpler differentiation purposes, let us refer to this as an electronic ID, or an eID for short.

As with most things, the virtual or digital version starts as a reflection of the physical or real-world representation. Therefore, most people will think of the digital representations of their government provided credentials as their eID.[189] While this is a most rudimentary place to start,

[188] Maryline Laurent and Samia Bouzefrane (eds), *Digital Identity Management* (ISTE Press [u.a] 2015). 1

[189] Tewfiq El Maliki1 and Jean-Marc Seigneur, 'Online Identity and User Management Services' in John R Vacca (ed), *Computer and Information Security Handbook* (Third edition, Morgan Kaufmann Publishers, an imprint of Elsevier 2017). 985

many eID identification ecosystems are going beyond digitised facsimiles and into full grown national digital ecosystems.

Therefore, in summary, my use of the concept of identity will be distinguished as virtual digital identities; eID; and identification. Three different but interrelated concepts. Of note is that all these systems implement data and are therefore in danger of being targeted during cyber belligerency. For purposes of this paper, let us however restrain the conversation to eIDs.

4.4.1. eID

The focus on eID stems from the premise of this paper. There is a direct link between data protection and digital identities, and indeed identification systems. Digital identities, including eIDs, are composed of data, mainly personal data,[190] that is then processed by identification systems. Do data protection rules, especially those of the international sort discussed above, apply to them? Invariably, yes they do. As such, I will briefly look at the concept of eIDs, their increased proliferation, and the idea behind their usefulness. A brief understanding of these concepts should demonstrate the honeypot that eIDs will become to belligerent nations, and consequently, the need to have IHL keep watch over them.

Internationally, the idea of identification can be traced to the UDHR. Article 6 states that '*everyone has a right to recognition everywhere as a person before the law*'.[191] This is the concept of legal identity. Legal identity is defined by the UN as '*the basic characteristics of an individual's identity'*.[192] The idea of 'recognition everywhere' should be extended to the

[190] Ana Beduschi, 'Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights' (2019) 6 Big Data & Society 205395171985509.

[191] See also Article 16 of the ICCPR. A verbatim repetition of Article 6, UDHR.

[192] 'Home — UN Legal Identity Agenda' <https://unstats.un.org/legal-identity-agenda/> accessed 20 June 2021.

digital space; and either way, attempts to ignore this space have been overtaken by its growing importance.

There is a rush to get eID programs started. Some of the nations that are undertaking similar programs in one form or another are: France, Germany, India, Canada, Kenya and the EU. They come in various forms, some being purely digital while others being a mix of digital and physical. The unifying fact is that they represent a means by which a set of data representing the persons attributes are digitally stored, accessed, and verified in order to ascertain the identity of the person.

In France the issuance of an eID was rolled out in March 2021. The new eID is a physical card (therefore similar to the ID cards of old) but with digital components. It contains an electronic chip and a QR code.[193] The chip contains digital versions of the information on the card i.e. name, date of birth, gender etc. It also contains the holder's photograph and two fingerprints. The QR Code works as both an electronic seal and a repository of some data. The QR code will therefore confirm authenticity of the card, and consequently its physical and electronic content.[194]

In India, the world's largest eID system is to be found. It is named Aadhaar and currently contains over 1.295 billion entries.[195] Calling that a vast number is an understatement. An Aadhaar number is described as a unique 12-digit number that is assigned to each applicant,

[193] 'The New National Electronic Identity Card' (*IN Groupe*) <https://www.ingroupe.com/en/newsroom/new-national-electronic-identity-card> accessed 20 June 2021.

[194] 'REVEALED: What You Need to Know about France's New Digital ID Cards' (*The Local France*, 16 March 2021) <https://www.thelocal.fr/20210316/revealed-what-you-need-to-know-about-frances-new-digital-id-cards/> accessed 20 June 2021.

[195] 'Aadhaar Dashboard' <https://uidai.gov.in/aadhaar_dashboard/india.php> accessed 20 June 2021.

being a resident of India, and is purposed to identify a unique person.[196] Each number is associated with biometric and demographic information of the person. The biometric information is the persons 10 fingerprints, two iris scans, and facial photographs. The demographic information includes the person's name, date of birth, gender, mobile phone number, email, and address. Beginning October 2020, the Aadhaar number can be got as a physical ID card.[197] This is in addition to the paper-based version, the eAadhaar, and the mAadhaar. The eAadhaar is an electronic form that is validated by QR and also online, and the mAadhaar is a mobile app-based form of the eID. It is reported that 95% of Indian adults have Aadhar.[198]

In Estonia, the country prides itself as the first users of eIDs.[199] Not just the first, but probably the most prolific in terms of issuance and also use cases. It is used for government services, banking, voting, telecommunication services, taxes, medical records, and as an e-signature.[200] It is arguable that they provide a vision of the future uses of eID and a test case for their widespread adoption as part and parcel of not only private sector services, but more importantly, government services. Indeed, as per Prisallu publishing in June 2017, the entire

[196] Reetika Khera (ed), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan).

[197] 'Order Aadhaar PVC Card' (*Unique Identification Authority of India | Government of India*) <https://uidai.gov.in/contact-support/have-any-question/1024-faqs/aadhaar-online-services/order-aadhaar-pvc-card-online.html> accessed 20 June 2021.

[198] State Of Aadhaar 2019, 'Key Findings: State of Aadhaar 2019' (*State Of Aadhaar*) <https://www.stateofaadhaar.in/top-10-insights.php> accessed 20 June 2021.

[199] . Miguel Goede, 'E-Estonia: The e-Government Cases of Estonia, Singapore, and Curaçao' (2019) 7 Archives of Business Research <http://scholarpublishing.org/index.php/ABR/article/view/6174> accessed 22 June 2021.

[200] 'Estonia, the Digital Republic | The New Yorker' <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic> accessed 22 June 2021. See also 'ID-Card' (*e-Estonia*) <https://e-estonia.com/solutions/e-identity/id-card/> accessed 22 June 2021.

Estonian government information system offered 4196 services.[201] This eID is mandatory and comes in the form of a physical ID card, a digital ID card (digital file) and a mobile ID (SIM Card based).

In Kenya, the state is currently in the process of implementing the huduma number. This huduma number, and its accompanying huduma card will form the basis of an eID that will be managed through the National Integrated Identity Management System (NIIMS). The idea behind the huduma number is that it will be a part of NIIMS, which shall contain foundational and functional data. Foundational data has been defined as the 'basic personal data of a resident individual for attesting the individual's identity and includes biometric data and biographical data'.[202] Functional data has been defined as the 'data of a resident individual created in response to a demand of a particular service or transaction'.[203] The intended purpose of the NIIMS is glimpsed in the Huduma Bill, 2019. Services are listed as requiring mandatory obligations to present the huduma number include:[204]issuance of a passport, paying taxes, opening a bank account, registering a company, registering for electricity connection, registering a marriage, access social protection, deal with land, and register for a phone number, and consequently, mobile banking. This list, despite being inexhaustive, is punctuated with the rider, 'any other specified public service'.

[201] Jaan Priisalu and Rain Ottis, 'Personal Control of Privacy and Data: Estonian Experience' (2017) 7 Health and Technology 441.

[202] Rule 2, Registration of Person (National Integrated Identity Management System) Rules, 2020.

[203] Rule 2, Registration of Person (National Integrated Identity Management System) Rules, 2020.

[204] Section 8, Huduma Bill. This refers to the Bill presented for public participation in 2019.

4.5. Conclusion

Data has no equivalent in all domains of war. There is nothing to compare it with. Yet it will quickly become one of the most valuable military tool and objective. Its unique characteristics will also make it both a defensive and offensive weapon. It means it is of dual use in nature and that it will have, probably, the largest overlap between military and civilian objects.

It has truly taken a long time to develop international data protection to its current, albeit incomplete, level. This experience is centred on civilian rules and is backed up by decades of international debate and subsequent application of agreed rules. This debate has been reduced into the data protection principles and discussions of what data protection should look like in IHL, ought to begin with this wealth of knowledge rather than stretching and transposing IHL. If this is not done, then the increasing utilisation of data in more critical sectors, as manifested by the eID, will set up lacunas for massive failure by IHL should cyberwarfare openly break out. It is time to consider the protection of such critical civilian data infrastructure from the unbridled exploitation by the military machine.

5. CONCLUSION.

The journey to the creation of a new (sub-)branch of law is often long and arduous. The ability of humankind to come together to work for the benefit of all is often derailed by the definition of 'all'. Tribalism and nationalism often take the centre stage.

The forefathers of IHL were alive to the ability of warfare to change in terms of tools and methods used. Indeed, their main motivation for the creation of this branch of law was their experience on seeing how new technologies had changed the battlefield. As such, they included a failsafe switch in the law they wrote. It first appeared in the Preamble to the Hague Convention of 1899 as the Martens Clause.[205] It currently lives in the AP I under Article 1 (2):

> *In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.*

However, the idea behind a failsafe is that it be employed as a last resort mechanism, not as the standard. Otherwise, the law ought to develop as the situation changes. Boyle has described the international law-making process as one that needs improved law-making processes that allow for amendments and creation of new laws.[206] That is the ideal, not the reality. The reality is that traditional international law-making process can never keep up with the pace of technological changes in warfare, and in particular, cyberspace.[207]

---

[205] Heather A. Harrison Dinniss, 'The regulation of cyber warfare under the *jus in bello*' in James A Green (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015) 149.

[206] Alan E Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press 2007) Chapter 4.

[207] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017) 16.

The reality is that soft law often plays an important role in the period between the emergence of the need for international law and its eventual enactment. Boyle also has a simplified description of soft law as a variety of non-legally binding instruments used in contemporary international relations.[208] Thirlway describes it as obligations that are not yet binding but carry with them an expectation of compliance despite the lack of a legal duty.[209] However, the nature of warfare is that not very many participants are willing to give a quarter.

Other forums have called on a different path forward, mostly with the knowledge that most governments, especially those with UN Security council veto, will not easily accept regulation. The previously discussed 2021 OEWG called for what it described as confidence building measures.[210] Examples given of these measures include improved communication, exchanging observers and performing inspections, establishing behaviour rules, and self-restraint.[211] Indeed, the non-binding nature of such measure is seemingly preferred.[212]

Other soft law alternatives that can be considered and indeed should be attempted include guidelines, recommendations, and codes of conduct. They often provide an easier platform to establish a pattern of acceptable behaviour, whose basis will then form the gist of the

[208] Alan E Boyle and Christine Chinkin, *The Making of International Law* (Oxford University Press 2007) chapter Chapter 5.2.2.

[209] HWA Thirlway, *The Sources of International Law* (Second edition, Oxford University Press 2019) 188-189.

[210] UNGA, Open-ended working group on developments in the field of information and telecommunications in the context of international security, 'Final Substantive Report' (10 March 2021) A/AC.290/2021/CRP.2. See paragraph 41.

[211] Marie-France Desjardins, *Rethinking Confidence-Building Measures: Obstacles to Agreement and the Risks of Overselling the Process* (Oxford University Press for the International Institute for Strategic Studies 1996) 5.

[212] François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 5.

conversation. One form of soft law that has been given weight in the IHL world are the documents produced by ICRC or adopted in expert meetings.[213] The options do veritably exist.

5.1. Is it time for an additional protocol IV?

The legitimisation of all these potential sources of law discussed above into a coherent one is most likely the best way forward. Indeed, since the last Additional Protocol was adopted in 1977, there have been several treaties that have expanded *jus in bello*. These include the Chemical Weapons Convention, which covers 98% of the global population;[214] and the Protocol on Blinding Laser Weapons. The precedent for new hard law in the field of IHL is there, what may be unavailable is the will or a sufficiently strong platform upon which to carry out the conversation.

This paper is neither alone nor unique in its call for a protocol to govern cyberwarfare. Microsoft has called for what it has termed as a Digital Geneva Convention.[215] Delerue explains that the conversation is also happening on the international scene with some support from Russia but opposition from United States and Europe.[216] Where this paper takes it further is in the idea that such a convention should also focus energy on the idea of data protection within the context of cyberwarfare.

---

[213] Marco Sassòli and Patrick Nagler, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019) 33.

[214] 'Chemical Weapons Convention' (*OPCW*) <https://www.opcw.org/chemical-weapons-convention> accessed 19 August 2021.

[215] Brad Smith, 'The Need for a Digital Geneva Convention' (*Microsoft On the Issues*, 14 February 2017) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> accessed 19 August 2021.

[216] Delerue (n 193) 26-27.

A Digital Geneva really ought to recognise that so far, the offensive activities and general developments in cyberwar have been child's play compared to what will happen when countries fully move their critical data-dependent infrastructure online. Rather than transpose an already aged convention or wait until the problem is empirically serious, there should be concerted efforts to bring the idea of data protection to the front and centre of the conversation of extending protection of civilians during cyber warfare.

5.2. Findings and recommendations

My primary recommendation would be an answer to the above asked question of whether it is time for an additional protocol IV. The recommendation is that IHL practitioners start putting into action plans to transition the use of transposition in the larger cyberwarfare arena. This can be done by legislating an additional protocol that focuses on cyberspace and cyberwarfare. This protocol will take care of the nuances of specialised sui-generis fields within cyberspace, like international data protection. Barring this, then it is time to start pushing for sui generis soft law options that can include guidelines, recommendations, codes-of-conduct, and confidence building measures. These soft laws can then be mutated into an eventual digital Geneva convention, an Additional Protocol IV, so to speak.

The main finding in chapter two is that international data protection is currently not regulated by IHL in a situation of cyberwarfare. It is arguable that the civilian protections of International Data Protection will still apply, however, these are far removed from the better designed IHL regime. The resultant recommendation is that this lacuna be filled as quickly as possible. This can start with soft law and mature into the above-mentioned protocol IV, a Digital Geneva.

The main finding in chapter three is that transposition, as I have defined it, is widely used in bridging the gap between IHL and new areas of weapon development. This is especially true in cyberwarfare, where IHL has been extensively transposed into this legal area. This particular

use of transposition in cyberwarfare is tenuous and results in some unclear and impractical applications of core IHL principles. The recommendation from this finding is that the currently transposed laws should be treated and referred to as lacuna-filling, minimum standard laws awaiting more sector appropriate soft and hard law.

The main finding in chapter four is that transposition would not work for the international data protection arena during belligerency. This is due to data and, consequently, data protection being sui-generis aspects of modern life. The recommendation from this is that therefore, it is prudent that any conversation about data protection by IHL begin with the question of how to borrow from the civilian regime of international data protection, and in particular its data protection principles. Although possibly the harder path, it should allow for better protection of data in the envisioned IHL scenarios.

This harder path will include increased research into the interplay of data protection in scenarios of belligerency. It will demand coalition building by willing nations to push the issue of specific international regulation of cyberspace, or some of its aspects. It is therefore useful to jump-start the conversation on what happens to data during belligerency. This conversation must recast the protections provided by transposition of IHL into cyberspace as temporary protections that are meant to hold the fort while better fitting legal regimes are designed. Finally, there must be improved research, publishing, and access to data on breaches of data protection by nations, or their associated non-state actors, in scenarios that can invoke IHL. The launch of open data portals would be the ultimate goal in enabling this improvement.

BIBLIOGRAPHY

Books

Adams M and Bomhoff J (eds), *Practice and Theory in Comparative Law* (Cambridge University Press 2012)

Allhoff F, Henschke A and Strawser BJ (eds), *Binary Bullets: The Ethics of Cyberwarfare* (Oxford University Press 2016)

Bakardjieva Engelbrekt A and Nergelius J (eds), *New Directions in Comparative Law* (Edward Elgar 2009)

Bertino E and Takahashi K, *Identity Management: Concepts, Technologies, and Systems* (Artech House 2011)

Bygrave LA, *Data Privacy Law: An International Perspective* (First edition, Oxford University Press 2014)

Camenisch J (ed), *Digital Privacy: PRIME - Privacy and Identity Management for Europe* (Springer 2011)

Croddy E and Wirtz JJ (eds), *Weapons of Mass Destruction: An Encyclopedia of Worldwide Policy, Technology, and History* (ABC-CLIO 2005)

Crowe J and Weston-Scheuber K, *Principles of International Humanitarian Law* (Edward Elgar 2013)

Custers B and others, *EU Personal Data Protection in Policy and Practice* (1st ed. 2019, TMC Asser Press : Imprint: TMC Asser Press 2019)

Delerue F, *Cyber Operations and International Law* (Cambridge University Press 2020)

'Digital Government in Chile - Digital Identity' (2019)

Driver J, *Consequentialism* (Routledge 2012)

Europäische Union and Europarat (eds), *Handbook on European Data Protection Law* (2018 edition, Publications Office of the European Union 2018)

Fawcett E, *Liberalism: The Life of an Idea* (2nd edition, Princeton University Press 2018)

Fingas MF (ed), *Oil Spill Science and Technology: Prevention, Response, and Cleanup* (Elsevier/Gulf Professional Pub 2011)

Fiorentini F and Infantino M (eds), *Mentoring Comparative Lawyers: Methods, Times, and Places: Liber Discipulorum Mauro Bussani* (Springer 2020)

Focarelli C, *International Law* (Edward Elgar Publishing 2019)

Francis L and Francis JG, *Privacy: What Everyone Needs to Know*® (Oxford University Press 2017)

Garner BA and Black HC (eds), *Black's Law Dictionary* (9th ed, West 2009)

Glorioso L and Taddeo M (eds), *Ethics and Policies for Cyber Operations: A NATO Cooperative Cyber Defence Centre of Excellence Initiative* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Green JA (ed), *Cyber Warfare: A Multidisciplinary Analysis* (Routledge 2015)

Gutwirth S (ed), *Computers, Privacy and Data Protection: An Element of Choice* (Springer 2011)

Harrison Dinniss H, *Cyber Warfare and the Laws of War* (Cambridge University Press 2012)

Henckaerts J-M and others (eds), *Customary International Humanitarian Law* (Cambridge University Press 2005)

Khera R (ed), *Dissent on Aadhaar: Big Data Meets Big Brother* (Orient BlackSwan)

Kittichaisaree K, *Public International Law of Cyberspace* (1st ed. 2017, Springer International Publishing : Imprint: Springer 2017)

Kolb R, *Advanced Introduction to International Humanitarian Law* (Edward Elgar 2014)

Kuner C, Bygrave LA and Docksey C (eds), *The EU General Data Protection Regulation (GDPR): A Commentary* (Oxford University Press 2019)

Laurent M and Bouzefrane S (eds), *Digital Identity Management* (ISTE Press [u.a] 2015)

Lehto, M and Henselmann G, 'Non-Kinetic Warfare : The New Game Changer in the Battle Space' in Brian K Payne and Hongyi Wu (eds), *The proceedings of the 15th international conference on cyber warfare and security* (Academic Conferences International 2020)

Lipsey RG, Carlaw K and Bekar C, *Economic Transformations: General Purpose Technologies and Long-Term Economic Growth* (Oxford University Press 2005)

Makulilo AB (ed), *African Data Privacy Laws* (1st ed. 2016, Springer International Publishing : Imprint: Springer 2016)

McGlinchey S and others, *International Relations Theory* (2017) <https://open.umn.edu/opentextbooks/BookDetail.aspx?bookId=544> accessed 30 January 2021

McLaughlin R and Nasu H (eds), *New Technologies and the Law of Armed Conflict* (1st ed. 2014, TMC Asser Press : Imprint: TMC Asser Press 2014)

Miller S, *Dual Use Science and Technology, Ethics and Weapons of Mass Destruction* (1st ed. 2018, Springer International Publishing : Imprint: Springer 2018)

O'Neil C, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (First edition, Crown 2016)

Organisation for Economic Co-operation and Development and SourceOECD (Online service) (eds), *OECD Glossary of Statistical Terms* (OECD 2008)

Porche I, *Cyberwarfare: An Introduction to Information-Age Conflict* (Artech House 2020)

Roland A, *War and Technology: A Very Short Introduction* (Oxford University Press 2016)

Rosenfeld M and Sajó A (eds), *The Oxford Handbook of Comparative Constitutional Law* (1st ed, Oxford University Press 2012)

Rule JB and Greenleaf GW (eds), *Global Privacy Protection: The First Generation* (E Elgar 2008)

Sassòli M and Nagler P, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare* (Edward Elgar Publishing 2019)

Saul B and Akande D (eds), *The Oxford Guide to International Humanitarian Law* (First edition, Oxford University Press 2020)

Saxon D (ed), *International Humanitarian Law and the Changing Technology of War* (Martinus Nijhoff Publishers 2013)

Schmahl S and Breuer M (eds), *The Council of Europe: Its Law and Policies* (First edition, Oxford University Press 2017)

Schmitt MN and NATO Cooperative Cyber Defence Centre of Excellence (eds), *Tallinn Manual on the International Law Applicable to Cyber Warfare: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence* (Cambridge University Press 2013)

—— (eds), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Second edition, Cambridge University Press 2017)

Schneier B, *Data and Goliath* (WW Norton & Company 2015) <http://api.overdrive.com/v1/collections/v1L2BaQAAAJcBAAA1M/products/ad5aa0d1-9521-419d-b0c9-6d3412a334b8> accessed 19 May 2021

Shakarian P, Shakarian J and Ruef A, *Introduction to Cyber-Warfare: A Multidisciplinary Approach* (Syngress 2013)

Shimizu H, *General Purpose Technology, Spin-Out, and Innovation: Technological Development of Laser Diodes in the United States and Japan* (Springer Singapore Imprint,Springer 2019)

Sullivan C, *Digital Identity: An Emergent Legal Concept* (University of Adelaide)

Tamò-Larrieux A, *Designing for Privacy and Its Legal Framework: Data Protection by Design and Default for the Internet of Things* (1st ed. 2018, Springer International Publishing : Imprint: Springer 2018)

Tsagourias NK and Buchan R (eds), *Research Handbook on International Law and Cyberspace* (Edward Elgar Publishing 2015)

Vacca JR (ed), *Computer and Information Security Handbook* (Third edition, Morgan Kaufmann Publishers, an imprint of Elsevier 2017)

Van Alsenoy B, *Data Protection Law in the EU: Roles, Responsibilities and Liability* (Intersentia 2019)

Watson A, *Legal Transplants: An Approach to Comparative Law* (University Press of Virginia 1974)

Williams BK and Sawyer SC, *Using Information Technology: A Practical Introduction to Computers & Communications* (Eleventh edition, McGraw Hill Education 2015)

Journal Articles

Beduschi A, 'Digital Identity: Contemporary Challenges for Data Protection, Privacy and Non-Discrimination Rights' (2019) 6 Big Data & Society 205395171985509

Casey-Maslen S, 'Non-Kinetic-Energy Weapons Termed "Non-Lethal": A Preliminary Assessment under International Humanitarian Law and International Human Rights Law' [2010] Geneva Academy of International Humanitarian Law and Human Rights <https://www.geneva-academy.ch/joomlatools-files/docman-files/Non-Kinetic-Energy%20Weapons.pdf> accessed 22 August 2021

Fazal TM, 'Why States No Longer Declare War' (2012) 21 Security Studies 557

Goede M, 'E-Estonia: The e-Government Cases of Estonia, Singapore, and Curaçao' (2019) 7 Archives of Business Research <http://scholarpublishing.org/index.php/ABR/article/view/6174> accessed 22 June 2021

Goldbach TS, 'Why Legal Transplants?' (2019) 15 Annual Review of Law and Social Science 583

Kramer IR, 'The Birth of Privacy Law: A Century Since Warren and Brandeis' 39 Catholic University Law Review 703

Mather H, 'Natural Law and Liberalism' (2001) 52 South Carolina Law Review 331

Örücü E, ‘Law as Transposition’ (2002) 51 International and Comparative Law Quarterly 205

Priisalu J and Ottis R, ‘Personal Control of Privacy and Data: Estonian Experience’ (2017) 7 Health and Technology 441

Van Alsenoy B, Kuczerawy A and Ausloos J, ‘Search Engines after “Google Spain”: Internet@Liberty or Privacy@Peril?’ [2013] SSRN Electronic Journal <http://www.ssrn.com/abstract=2321494> accessed 10 August 2021

Warren S and Brandeis L, ‘The Right to Privacy’ (1890) 4 Harvard Law Review 193

Yilma KM, ‘The United Nations Data Privacy System and Its Limits’ (2019) 33 International Review of Law, Computers & Technology 224

Websites

‘28 January - Data Protection Day’ <https://www.coe.int/en/web/portal/28-january-data-protection-day> accessed 30 May 2021

Aadhaar 2019 SO, ‘Key Findings: State of Aadhaar 2019’ (*State Of Aadhaar*) <https://www.stateofaadhaar.in/top-10-insights.php> accessed 20 June 2021

‘Aadhaar Dashboard’ <https://uidai.gov.in/aadhaar_dashboard/india.php> accessed 20 June 2021

‘About the OECD - OECD’ <https://www.oecd.org/about/> accessed 28 May 2021

‘African Union Convention on Cyber Security and Personal Data Protection | African Union’ <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> accessed 1 June 2021

‘APEC Privacy Framework’ (*APEC*) <https://www.apec.org/Publications/2005/12/APEC-Privacy-Framework> accessed 17 June 2021

‘Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS)’ (*BAE Systems | United States*) <https://www.baesystems.com/en-us/product/autonomous-realtime-ground-ubiquitous-surveillance-imaging-system-argusis> accessed 8 September 2021

‘Barack Obama: “I Was Born in Hawaii”’ *BBC News* <https://www.bbc.com/news/av/world-us-canada-13213810> accessed 12 August 2021

Barber N, ‘1991 Gulf War Oil Spill’ (23 November 2018) <http://large.stanford.edu/courses/2018/ph240/barber1/> accessed 3 May 2021

‘BĂRBULESCU v. ROMANIA’ <https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-159906%22]}> accessed 1 June 2021

‘BBC - Ethics - Introduction to Ethics: Consequentialism’ <http://www.bbc.co.uk/ethics/introduction/consequentialism_1.shtml> accessed 31 January 2021

‘Berkshire Hathaway Portfolio Tracker’ (*CNBC*, 16 May 2019) <https://www.cnbc.com/berkshire-hathaway-portfolio/> accessed 15 April 2021

‘British Armed Forces’ Data Breach Exposes Identities of over a Hundred Special Forces Troops | Leigh Day’ <https://www.leighday.co.uk/latest-updates/news/2021-news/british-armed-forces-data-breach-exposes-identities-of-over-a-hundred-special-forces-troops/> accessed 23 August 2021

‘Chart of Signatures and Ratifications of Treaty 108’ (*Treaty Office*) <https://www.coe.int/en/web/conventions/search-on-treaties> accessed 24 May 2021

‘Chemical Weapons Convention’ (*OPCW*) <https://www.opcw.org/chemical-weapons-convention> accessed 19 August 2021

‘China Is Laying the Groundwork to Nationalize Private Companies’ Data’ (*protocol*) <https://www.protocol.com/china/china-national-security-data-exchange> accessed 17 June 2021

‘Collective Action Problem’ (*Encyclopedia Britannica*) <https://www.britannica.com/topic/collective-action-problem-1917157> accessed 31 January 2021

‘Colt M4 Carbine - Army Technology’ <https://www.army-technology.com/projects/colt-m4-carbine-assault-rifle-us/> accessed 22 August 2021

‘Convention 108 and Protocols’ (*Data Protection*) <https://www.coe.int/en/web/data-protection/convention108-and-protocol> accessed 28 January 2021

‘Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data’ (*Treaty Office*) <https://www.coe.int/en/web/conventions/full-list> accessed 24 May 2021

‘Cyber Warfare: IHL Provides an Additional Layer of Protection’ (*International Committee of the Red Cross*, 10 September 2019) <https://www.icrc.org/en/document/cyber-warfare-ihl-provides-additional-layer-protection> accessed 22 August 2021

DeCew J, ‘Privacy’ in Edward N Zalta (ed), *The Stanford Encyclopedia of Philosophy* (Spring 2018, Metaphysics Research Lab, Stanford University 2018) <https://plato.stanford.edu/archives/spr2018/entries/privacy/> accessed 20 May 2021

‘Definition of MUTATIS MUTANDIS’ <https://www.merriam-webster.com/dictionary/mutatis+mutandis> accessed 20 July 2021

Editors H com, 'Armistice Ends Korean War Hostilities' (*HISTORY*) <https://www.history.com/this-day-in-history/armistice-ends-the-korean-war> accessed 12 August 2021

——, 'Gatling Gun' (*HISTORY*) <https://www.history.com/topics/american-civil-war/gatling-gun> accessed 22 August 2021

'Estonia, the Digital Republic | The New Yorker' <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic> accessed 22 June 2021

'Forbes Billionaires 2021: The Richest People in the World' (*Forbes*) <https://www.forbes.com/billionaires/> accessed 15 April 2021

'Group of Governmental Experts – UNODA' <https://www.un.org/disarmament/group-of-governmental-experts/> accessed 20 July 2021

'Home — UN Legal Identity Agenda' <https://unstats.un.org/legal-identity-agenda/> accessed 20 June 2021

'ID-Card' (*e-Estonia*) <https://e-estonia.com/solutions/e-identity/id-card/> accessed 22 June 2021

'Industrial Revolution | Definition, History, Dates, Summary, & Facts' (*Encyclopedia Britannica*) <https://www.britannica.com/event/Industrial-Revolution> accessed 16 April 2021

'Kirby, Michael --- "Privacy Today: Something Old, Something New, Something Borrowed, Something Blue" [2017] JlLawInfoSci 1; (2017) 25(1) Journal of Law, Information and Science 1' <https://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html#fn39> accessed 1 June 2021

Lee EC Yen Nee, 'New Chart Shows China Could Overtake the U.S. as the World's Largest Economy Earlier than Expected' (*CNBC*, 1 February 2021) <https://www.cnbc.com/2021/02/01/new-chart-shows-china-gdp-could-overtake-us-sooner-as-covid-took-its-toll.html> accessed 17 June 2021

Neufeld D, 'The Richest People in the World in 2021' (*Visual Capitalist*, 9 March 2021) <https://www.visualcapitalist.com/richest-people-in-the-world-2021/> accessed 15 April 2021

'New Aadhaar PVC Card with Enhanced Security Features: All You Need to Know - Times of India' (*The Times of India*) <https://timesofindia.indiatimes.com/business/india-business/uidai-launches-aadhaar-pvc-card-with-enhanced-security-features-all-you-need-to-know/articleshow/78716339.cms> accessed 20 June 2021

Niiler E, 'How the Second Industrial Revolution Changed Americans' Lives' (*HISTORY*) <https://www.history.com/news/second-industrial-revolution-advances> accessed 16 April 2021

‘OECD Work on Privacy - OECD’ <https://www.oecd.org/sti/ieconomy/privacy.htm> accessed 30 May 2021

‘Order Aadhaar PVC Card’ (*Unique Identification Authority of India | Government of India*) <https://uidai.gov.in/contact-support/have-any-question/1024-faqs/aadhaar-online-services/order-aadhaar-pvc-card-online.html> accessed 20 June 2021

‘Privacy and Human Rights - Overview’ <http://gilc.org/privacy/survey/intro.html> accessed 21 May 2021

‘Protocol Amending the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data’ (*Treaty Office*) <https://www.coe.int/en/web/conventions/full-list> accessed 27 May 2021

Refugees UNHC for, ‘Refworld | Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion’ (*Refworld*) <https://www.refworld.org/cases,ICJ,4b2913d62.html> accessed 2 August 2021

‘REVEALED: What You Need to Know about France’s New Digital ID Cards’ (*The Local France*, 16 March 2021) <https://www.thelocal.fr/20210316/revealed-what-you-need-to-know-about-frances-new-digital-id-cards/> accessed 20 June 2021

Rose D, ‘Hacked Train Screens Tell Iranians to Call Ayatollah’ <https://www.thetimes.co.uk/article/hacked-train-screens-tell-iranians-to-call-ayatollah-9m2j0h0mk> accessed 23 August 2021

‘Sistema HJ - Resolución: SENTENCIA 292/2000’ <http://hj.tribunalconstitucional.es/es-ES/Resolucion/Show/4276> accessed 1 June 2021

Smith B, ‘The Need for a Digital Geneva Convention’ (*Microsoft On the Issues*, 14 February 2017) <https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/> accessed 19 August 2021

Suderman A, ‘MWD among Targets in Large-Scale Cyber-Espionage Hack Blamed on China’ (*Los Angeles Times*, 15 June 2021) <https://www.latimes.com/world-nation/story/2021-06-15/critical-entities-targeted-suspected-chinese-cyber-espionage> accessed 23 August 2021

Swant M, ‘The 2020 World’s Most Valuable Brands’ (*Forbes*) <https://www.forbes.com/the-worlds-most-valuable-brands/> accessed 28 January 2021

‘The Bizarre Evolution of the Word “Cyber”’ (*Gizmodo*) <https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487> accessed 18 July 2021

‘The New National Electronic Identity Card’ (*IN Groupe*) <https://www.ingroupe.com/en/newsroom/new-national-electronic-identity-card> accessed 20 June 2021

‘The Principles’ (21 March 2021) <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/> accessed 10 August 2021

‘What Are the Origins of International Humanitarian Law? | The ICRC in Israel, Golan, West Bank, Gaza’ <https://blogs.icrc.org/ilot/2017/08/07/origins-international-humanitarian-law/> accessed 6 July 2021

‘What Is Privacy?’ (*Privacy International*) <http://privacyinternational.org/fr/node/56> accessed 20 May 2021

‘When Cyberweapons Escape’ (*The Cipher Brief*) <https://www.thecipherbrief.com/column_article/when-cyberweapons-escape> accessed 23 August 2021