New Technologies and Global Governance: Challenge or Opportunity?
Preface

The history of global governance is in many ways the story of adaptation to new technologies. Advances in technology have long driven global rule-making, from the invention of the telephone and the need to coordinate international dialling codes to advances in weaponry resulting in international treaties regulating their use. Yet something feels different today. The rapid pace of technological innovation is undoubtedly shaping global governance, its norms and institutions, but it is also reshaping what global governance means. Artificial intelligence, big data, nanotechnology, and automation are just a few of many emerging technologies that have left governments and international institutions scrambling. How do these new technologies change the rules of the game? Can states even wrap their heads around their potential and danger? What impact do these new technologies have on conflict, cooperation, and our everyday lives? How can the international community mitigate their negative impact and even harness the positive potential of these advancements? How do we balance the collective benefits of data with risks to individuals?

Focusing on great power politics and global re-ordering, scholars often argue that states are unwilling to regulate these new technologies. They might even use them to enhance their position and sow discord. Cyberwarfare and the numerous hacking scandals seem a perfect example, as do the discussions about the adoption of 5G technology. Domestically, new technologies have helped governments augment their positions against oppositions and have been linked to the rise of populism, a topic we explored in last year’s edition of the Junior Scholar Working Paper Series (JSWPS). But while states are seemingly willingly using new technologies for their advancement, the bigger question is whether they and the international institutions they have created are even able to understand and regulate their use. Are states still the primary drivers in global governance or do we need to completely change our understanding of global governance because of new technologies?
When we started discussing the overarching topic for this year’s JSWPS, our young scholars took us to task. They brought to the table new technologies we barely knew existed. Through each meeting we learned something new. In many ways, the learning curve was even steeper than in previous years, a good sign of the profound impact the technologies discussed herein are having on the study and practice of global governance. In the spirit of debate, we, as a group, decided to encourage diversity, not just in their choice of topics, but also in how the authors chose to interpret what new technologies were and whether they wanted to focus on their destructive or constructive dimensions.

Each of the seven essays that is part of this volume has its own message, together highlighting the complexity of the relations between new technologies and global governance. With subjects ranging from telecommunications, biotechnology, artificial intelligence, big data and the dark web, as well as renewable energy, the breadth of the topic quickly became clear to everyone involved. But as we began discussing the specific research projects, the interconnected questions and different levels of analysis came into focus. The present volume asks big IR questions about great power competition as well as more intimate questions concerning governmental control over their own populations. Some essays are more hopeful about our future, others more pessimistic, but they all provide a nuanced and critical engagement with the world we live in. And that is an achievement we could not be prouder of.

The Centre for Global Constitutionalism is extremely proud of our internship programme. Each autumn, we hold a competitive selection process to fill roughly half a dozen positions for the academic year. Interns fulfil a variety of tasks during their tenure, assisting with the organisation of Centre events and enhancing engagement with the St Andrews student body. Our 2019-20 cohort includes both undergraduate and postgraduate (MLitt and MRes) students from the Schools of International Relations and History. As part of their internship, interns write a paper on our yearly overarching topic. Their individual research projects are compiled in this volume.
The internship programme is a vital part of the CGC’s broader community of scholars. Our Associate Fellows, Erika Brady, Mary Dodd, Robin El Kady, Josephine Jackson, Anuj Puri, and Ruoxi Wang—all PhD candidates at St Andrews—served as academic mentors for the individual projects and provided superb guidance and moral support in the development of this research. We are grateful for their help as, we are sure, are the interns. Yet the work presented here is the product of our interns’ own thinking. They are their own biggest support network, and actively provided peer review on each other’s drafts as we workshopped their papers. We enjoy this process tremendously and are delighted to be part of their learning process.

This year is a bit unusual. When we decided on our yearly topic of New technologies and global governance back in the autumn, we had no idea how the Centre’s work would be impacted by a pandemic that has rapidly expanded the prevalence of digital learning and communication technologies. Due to the COVID-19 crisis, several CGC events were cancelled and some rescheduled to the virtual space. Of these, we are most sad that we had to abandon our original plan for the JSWPS launch event. This is always a nice celebration of our interns’ achievements and serves to wrap-up our activities for the academic year. In the spirit of our topic, we will be relying on digital technologies and celebrating through a virtual launch party.

And for you, reader, enjoy this year’s volume and help us toast to the success of our interns! This year, from a safe distance.

Adam Bower and Mateja Peter
Co-Directors, Centre for Global Constitutionalism
INTENTIONALLY LEFT BLANK
# Table of Contents

<table>
<thead>
<tr>
<th>Author</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hattie Watson</td>
<td>iBorderCtrl: Exploring the Issue of Algorithmic Bias in Global Governance</td>
<td>1</td>
</tr>
<tr>
<td>Dirk Van Der Tang</td>
<td>Genetically Modified Norms: The Contested Relationship Between Genetically Modified Organisms and Intellectual Property Rights</td>
<td>13</td>
</tr>
<tr>
<td>Harris Siderfin</td>
<td>Renewable Energy Technologies and State Security: Current Shield and Future Sword?</td>
<td>25</td>
</tr>
<tr>
<td>Ella Kiley</td>
<td>Computational Propaganda During Democratic Elections: Vote Leave’s Violation of International Law</td>
<td>37</td>
</tr>
<tr>
<td>Maël Ihamouchene</td>
<td>Uncertainties of Climate Change: Demystifying New Technologies as a Silver Bullet and Embracing Uncertainties</td>
<td>51</td>
</tr>
<tr>
<td>Christine Cheng</td>
<td>Examining Huawei’s Role in the U.S.-China Trade War and Its Implications for Global Governance</td>
<td>63</td>
</tr>
<tr>
<td>Farrah Barber</td>
<td>The Secret Surfers: A Quantitative Analysis of How Domestic Political Rights Impact Upon Anonymous Internet Usage</td>
<td>75</td>
</tr>
</tbody>
</table>
“Algorithmic bias” is an unusual concern for those beyond the world of computer science, yet it is shaping decisions that could fundamentally affect the future of every individual. The issues connected to algorithmic bias that arise in a new EU funded system of border control, the iBorderCtrl project, will be the focus of this essay. This is a multi-stage platform which uses Artificial Intelligence (AI) to assist border guards in the process of managing third-party nationals entering the Schengen Area. Pilot tests took place at three EU entry points in 2019, the results of which are currently being analysed (iBorderCtrl n.d.). At this research and development stage, there is scope for mitigation and adjustment in the design which makes it an important moment at which to fully consider its ethical, practical and legal implications (d’Aquín, et al. 2018). Before turning to the case study, it is valuable to briefly outline the broader phenomenon of algorithmic bias in relation to AI. There exists extensive scholarship on the topic of AI and its ethical implications (Garcia Winter 2016/2017). Far-reaching computer science research has explored possible technical solutions that could mitigate the bias (Wortham, Theodorou and Bryson 2016) (Rovatsos, Mittelstadt and Koene 2019). I argue that, due to the human involvement of a computer programmer in the design of any algorithm, bias is an unavoidable truth and must therefore be considered and incorporated into the supporting infrastructures of the system (Bozdağ 2013) (Baer 2019). This essay will therefore conclude by suggesting two methods for managing the implications of algorithmic bias in the context of iBorderCtrl: enhanced interdisciplinary discussion, understanding and collaboration in the technical development process, and an emphasis on public education, both for prospective users but also for border control guards who will use it.
The Issue of Algorithmic Bias

As humans, we are constantly making biased decisions. It is an opportunity cost of our ability to make thousands of fast-paced choices in our lives each day (Baer 2019). What exactly is bias, and how does bias differ from having an opinion? Herbert Weisberg argues that the level of bias cannot be reduced with increasing sample size and roots his book in the definition that bias is the systematic disruption of the causal effect of a decision process (Weisberg 2011, 3). Meanwhile, Jonathan Evans et al. comment on “belief bias,” when a person shapes their response according to what might be more believable in the situation rather than the logical decision (Evans, Newstead and Bryne 1993, 243). It is important to consider whether it is appropriate to apply the same notion of bias to both humans and technology, especially considering that the notion of “belief bias” would not be risk with mechanical processes. This author’s interpretation of bias is that it involves sub-conscious and intrinsic influences within humans that continually guide decisions and actions, to a sometimes-undetectable level. In the context of this essay, algorithmic bias will be defined as the circumstance when algorithms - which instruct computers to complete tasks - create, maintain or exacerbate human biases. It arises from a process known as deep learning in sub-symbolic AI (machine learning) (UNIDIR 2018, 6). This is when the algorithm is fed training data and tasked to run its functions, in order to produce an outcome. The challenge is that this process is incomprehensible to humans and thereby creates a semantic gap (“black box” scenario); the difference between what the computer can interpret and what a human can understand. Humans with the end result of the algorithm are unable to explain every process that has occurred in order to achieve that outcome (Burton, et al. 2020). Some global businesses have argued that the ability to provide a complete explanation is not a significant concern as long as revenue is maximised (PwC 2018). However, a consequence of the semantic gap is that unintended biases may creep in because humans cannot control how the data that the algorithm is fed is used (UNIDIR 2018, 6). When the outcome directly affects the life of an individual, as in the case of iBorderCtrl and global governance, this becomes a very significant ethical and legal concern.
Two key issues that relate to algorithmic bias in the context of the iBorderCtrl are: the nature and importance of clean training data - from which the machine makes its decisions - in influencing biases and the inability to explain the outcome of the process to the person who is affected by the bias.¹

Turning to the issue of training data first, where does it come from and is it representational? What is it representational of? It is significant that humans will be involved in the process of identifying training data at some point which means that the machine is entirely reliant on what the human selects for it to learn. The consequence is that it is very challenging to eliminate the element of human bias at the stage of selecting the training data. However, poor quality data will lead to skewed results from the algorithm (UNIDIR 2018, 2-3). Recent cases, such as the Dutch case on Systeem Risico Indicatie (SyRI), highlight the challenges of ethically collecting and utilising this data. The SyRI case refers to the collection of data for an algorithmic system which identifies areas to target for law enforcement. The decision ruled that this invaded the right to privacy and therefore the use of the system should be suspended (SyRI 2020). Such limitations and challenges in collecting training data highlights that it will be very challenging to eliminate the element of human bias involved with its selection. Managing training data is a field of research in itself, as it is widely agreed that the algorithm is only as good as its training data (UNIDIR 2018, 3).

The second major issue to arise from algorithmic bias is the lack of transparency and explain-ability (Abdollahi and Nasraoui 2018). The semantic gap, which has already been discussed, creates the explanation problem however this becomes particularly significant at the application stage of the AI tool. If someone is denied their credit rating on the basis of an algorithmic decision, no-one will be able to explain to this person why this is the case. This is highly problematic considering that in the EU the GDPR, the EU privacy legal framework, explicitly outlines the right to an explanation of a decision resulting from an algorithmic outcome (GDPR, 2016, Recital 71). Lilian Edwards and Michael Veale have argued that this is limited in

¹ This is not an exhaustive list but those that will be focused on in this work.
practical reality due to the limitations of the, at times, vague and even paradoxical nature of the GDPR legislation (Edwards and Veale 2017, 18-19). However, it is a major concern that this nature of machine learning is fundamentally incompatible with the current legal framework, if anything on a symbolic over a practical basis.

**iBorderCtrl: The Technical Framework**

The iBorderCtrl is a complex platform that relies on a range of AI technologies. It will become fully operational by 2025 and its primary aim is to increase the efficiency of the border-crossing process and in addition to reducing the cost per traveller and to enhance security (iBorderCtrl n.d.). The platform is split into two stages and operates on an entirely opt-in consent basis. First the individual traveller signs up to an online user application to complete the pre-registration stage (iBorderCtrl n.d., The Project). At this point, the traveller provides their consent for their involvement in the whole platform and the use of their data. “Relevant data”, such as a copy of the travel documents and passport are inputted, and a pre-registration interview is conducted by the Automatic Deception Detection System (iBorderCtrl n.d., Technical Framework). The interview involves a video interview with an avatar posing questions and a computer assessing the responses through non-verbal facial signals (iBorderCtrl n.d.). The controversial Silent Talker software enables this stage of the process which itself raises some very significant ethical, technical and legal questions on the capabilities of machine learning (Silent Talker Intelligent Systems 2020). Is it ethical to base a risk decision on the basis of non-verbal facial recognition in a removed environment? Is a machine technically capable of serving as an effective lie detector, especially from this removed perspective? What would the training data for such a machine look like? These fundamental concerns highlight how this is one of the most problematic aspects of the system, especially from a perspective of algorithmic bias without explanation. In conjunction with this user interaction, the iBorderCtrl platform conducts a range of other checks based on a wide range of information which is gathered from databases including biometric data, facial recognition, social media and international police and legal records (iBorderCtrl n.d., Technical Framework). It is significant that as border control is classified under immigration and security, iBorderCtrl is not
subject to the GDPR regulations (Information Commissioner's Office 2019, 309). The combination of information and assessment data, gathered through the interview, documents and iBorderCtrl checks, is processed by an algorithm in order to produce an overall risk-score output. Additionally, the algorithm highlights areas for the human border guards to further investigate when the passenger arrives at the crossing. At this stage, it is only in the circumstance of a criminal record categorically inhibiting travel that the passenger will be notified of the outcome of any of these checks (iBorderCtrl n.d., Technical Framework).

When the traveller arrives at the border crossing, border guards will be able to use sophisticated technology to assist their checks, such as the Hidden Human Detection Tool for searching vehicles. The documents are rechecked though, because the main checks have already taken place in advance, this is for primarily verification purposes and therefore takes less time. Any areas that the algorithm flags are investigated. The final entry decision is ultimately the responsibility of a human border guard who is guided by the algorithm risk score (iBorderCtrl n.d.).

Once this is complete, and the traveller moves on, all the data about this individual is anonymously fed back into the system. This is processed through the integrated Border Control Analytics Tool (BCAT) which seeks to identify patterns and develop knowledge which will allow the system to improve its capacity to adapt to new situations. In essence, it is recycling its output data as training data (iBorderCtrl n.d., Technical Framework).

**iBorderCtrl: Algorithmic Bias**

Several issues of algorithmic bias are presented at each stage of this platform. Firstly, the consequence of the great range of data that is fed into the system means that there is ample scope for unintended biases to develop. Due to the semantic gap, border guards or even computer scientists, will be unable to explain to a person why they have been issued with a certain risk score. This could have very significant personal consequences for the individual which this apparently does not account for. This raises the concern of objectification, when a person is treated as an object
rather than as a human being (Gervais, et al. 2013). When considered in context of the European Court of Human Rights notion that human dignity is the absence of objectification, this becomes important (Riley and Bos n.d.). The implication is that this method of border control risks denying human dignity which Ozlem Ulgen argues, on the basis of Kant, should never be sacrificed (Ozlem 2016). Although, because the human is able to override the potentially biased decision of the algorithm at the final decision stage, it is important to consider the degree to which humans are swayed by a scoring system in their judgements. The extensive legal discussion about what constitutes “meaningful human control,” often in the case of automatic weapons systems, is relevant here and should be accounted for in relation to managing tendencies for algorithmic bias in this system (Roff and Moyes 2016) (Santoni de Sio and van dan Hoven 2018) (Cummings 2019).

An additional, and major, concern with the development of bias in this platform lies with the BCAT. The idea is that over time, the platform will detect patterns and will therefore become more adept at making decisions (iBorderCtrl n.d., Technical Framework). The more the tool is used, the more data it will have to be able to make sophisticated judgements which could improve accuracy. This is an exciting prospect in relation to overcoming the challenges of collecting enough representative training data for algorithms. However, there are no checks in place to ensure that the data that is being fed back is accurate (iBorderCtrl n.d., Technical Framework). The risk score is not aligned against what transpires when the person enters the country. For example, the algorithm identifies that two people who receive a similar, or even the same, risk score share the characteristics that they both have green eyes, olive skin and have liked the Starbucks Coffee page on Facebook. Regardless of whether the risk score that was attributed to these people transpired to be an accurate reflection of their behaviour when they enter the Schengen Area, this information will be used to inform decisions about similar people in the future. The relationship between causation and statistical correlation in AI outcomes is currently a topic of research and should be accounted for in this scenario (Leetaru 2019) (UCL 2020). In light of this, I argue that this feature of using an unchecked data feedback loop is particularly dangerous.
iBorderCtrl: Managing Algorithmic Bias

Algorithmic bias should not be used as a reason to inhibit innovation and the development of technology with dramatic potential. The iBorderCtrl project has impressive scope, much of which is enabled by AI. Feedback from the pilot exercises identified that the concept of having a pre-registration check incorporated with physical land border processes is unique (iBorderCtrl n.d., Pilot Results). The application was found to be user-friendly and quick to use, allowing for the costly and time-consuming checks to take place in advance (iBorderCtrl n.d., Pilot Results). This accelerates the process at pressed and busy land border crossings without compromising safety and security. In order to reap the benefits from what AI is offering to the border control system, it is important to understand and manage the technology. Two possible aspects of this is to encourage interdisciplinary discussion on the topic and to promote and develop public education and training on the matter (Dartnall 2013, 326) (Ratsch, Richter and Stamatescu 2013).

There is a growing literature on explainable and responsible AI and a plethora of activist groups and think tanks are currently working on the topic (Mojsilovic 2019, Future Advocacy n.d., The Institute for Ethical AI & Machine Learning n.d.). The development of an AI project to the implementation stage involves scholars, experts and practitioners from a wide range of disciplines ranging from computer science to law. Developing a better understanding of the different perspectives on this issue will present major challenges for the short term however, in the long term, if these challenges can be overcome or managed through creative thinking, it could lead to stunning innovation (van den Hoven and Weckert 2008). There is already evidence of interdisciplinary collaboration in various areas of AI development and I argue that interdisciplinary conversation would be productive for considering the questions of algorithmic bias in the iBorderCtrl project (High-Level Expert Group on Artificial Intelligence n.d.). For example, when addressing the question of the influence of a numerical score on human decision-making capacity, the input of psychologists, philosophers, lawyers and computer scientists would be relevant and has potential to lead to a more comprehensive conclusion.
A second area which could be developed in light of issues of algorithmic bias is public education. This applies on the one hand to implementing advanced training received by border guards in order to appropriately use and interpret the information presented to them by the iBorderCtrl platform. This would help to overcome the issue of the human made decision becoming overly influenced by the outcome risk number produced by the algorithm. Additionally, public education should focus on informing users of the border control what they are consenting to when they sign up to the platform. While this would not have a direct impact on the algorithmic bias issue, a population that is better informed about the technology that it is interacting with will be more able to make judgements in their own capacity. This could be significant for the legal frameworks of liability and responsibility in such scenarios. While it is important to consider the safety and security limitations of providing information on iBorderCtrl, lessons can be learned from the legal design movement from this perspective. Legal design aims to condense the complex technical jargon of contracts, terms and conditions and other legal documents to make them user friendly and easier to understand (Deffains and Fluet 2020, 167-168). The letter of informed consent, for those involved with the pilot project, was long and wordy and the information that is currently presented about the platform and the results of the trial on its website is one-sided and difficult for a lay person to comprehend, let alone within any shortened timeframe (iBorderCtrl n.d.). It takes one google search to notice that AI is a sensationalist topic in the media. Simplifying information to allow users to understand better what they are interacting with, and the associated risks, has potential to both manage expectations of the outcome and its limitations.

**Conclusion**

Overall, AI is an exciting development that has the potential to fundamentally change the processes and nature of global governance. One example of its application is in the realm of border control. The iBorderCtrl project is currently in a crucial development stage following its first pilot tests in 2019. It is therefore currently an optimal time to consider the risks and ethical issues relating to its use and implementation. One such consideration is that of algorithmic bias. This has
been branded as one of the most pressing concerns related to AI and therefore warrants serious consideration, especially in this context, when future lives may be at stake (Knight 2017). Two key concerns relating to algorithmic bias are the issue that it is not possible to explain every process of the algorithm process and that the algorithm is reliant on its training data. The consequence of the explain-ability problem is that humans cannot understand the source or cause of bias. It can therefore creep in and influence outcomes and decisions undetected. Therefore, addressing whether it is ethical for a human decision to be guided by a technology, that is both inexplainable and potentially displays less neutrality than a human, is essential at this stage of development. Training data is also fundamental to the degree of algorithmic bias. Poor quality data will lead to unrepresentative decisions.

In the iBorderCtrl project, unchecked information is being fed back into the system. This raises serious concerns about the scope for unintended biases to be repeated, exacerbated and become entrenched. I argue that two methods for mitigating the degree of challenge that these issues present is through education and interdisciplinary collaboration. Promoting an understanding of the technology that we interact with at all levels is central to its responsible use. This applies to expert collaboration during the technical development stage, but also assessing its context of implementation and forming the associated legal frameworks. Education is important for the border guards who interact with the platform, and for the consenting public who participate. Whilst these measures do not eliminate algorithmic bias, they do facilitate creating a climate of appropriate and responsible use of these technologies. In the age of the Fourth Industrial Revolution, it is important to embrace technological developments, whilst simultaneously working to create awareness, understanding and legal structures to encourage its ethical implementation.

**Bibliography**


Genetically Modified Norms: The Contested Relationship Between Genetically Modified Organisms and Intellectual Property Rights

Dirk Van Der Tang *

Genetically modified organisms, a potent form of biotechnology, have changed how we think about plants, animals and other organisms. Traditionally, they have been understood as natural entities, but new forms can now be created by humans (Juma 2005, 264). This article will examine the normative implications of this technology in relation to intellectual property rights, which govern the use and distribution of man-made inventions. More specifically, it will engage with constructivist theory to examine the role technology plays in norm change and norm contestation in order to discuss how genetically modified organisms influence how we think about intellectual property rights (henceforth IPR). The article will start by discussing the technological shift that genetically modified organisms represent, before introducing the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), an agreement that establishes the relationship between genetically modified organisms and private property. The article will then use constructivist theory on norm dynamics to examine the role that technology plays in norm change and norm contestation and evaluate how this informs the actions taken by states in the North and South, in particular the United States and India, to forward competing understandings of the relationship between genetically modified organisms and genetically modified organisms.

The Technological Shift: What are GMOs and Why are They Important?

Genetically modified organisms (henceforth GMOs) are a potent form of biotechnology enabled by the advent of technology for gene splitting and recombination (Juma 2005, 264). The first major breakthrough came in 1973, when Herbert Boyer and Stanley Cohen transferred a gene responsible for antibiotic resistance from one strain of bacteria to another. Following the Asilomar Conference

* 4th year undergraduate student, International Relations and Management.
in 1975, where government officials and scientists debated the safety of genetic modification, the attendees developed universal guidelines for testing. This transparency and cooperation allowed governmental bodies around the world to support research into this new scientific field of genetic modification (Rangel 2015).

A subject that has proven to be especially controversial is the impact of GMOs on agriculture. The first GMO food product to become commercially available was the Flavr Savr tomato, introduced in the US in 1994. In 2015, GMOs were grown in 28 countries on roughly 180 million hectares, which represent 10% of the world’s arable land. The US, the world’s largest producer a GMOs, accounts for almost 40% of the global area used for growing GMOs. Moreover, the US has the highest adoption rates, with 92% of maize, 94% of soybeans and 94% of cotton being genetically modified (Clive 2015, 5).

Despite their widespread use in recent years, GMOs have experienced mixed success and local opposition - most significantly in Europe and large agricultural exporters in the global South like India and Mexico (Falkner 2007, 99). Supporters of biotech crops point to their potential as a solution to mitigating the effects of climate change on our food supply, as genetic modification can make plants resistant to diseases, insects and herbicides. Additionally, genetic modification presents a more adaptable and fast-paced breeding process. Developing a new variety of potatoes, for instance, takes fifteen years using conventional breeding strategies, whereas through genetic modification it can be achieved in six months (Rotman 2013). Those sceptical of GMOs, on the other hand, have numerous concerns, including allergenicity, toxicity and antibiotic resistance. Moreover, there are important environmental concerns relating to how GMOs being released into the environment might harm biodiversity. For example, superweeds that eradicate pests can indirectly harm other types of organisms that are dependent on them (Falkner 2007, 101).

With research on the risks and benefits of GMOs being inconclusive, GMO controversy is ultimately a normative debate. GMOs impact more than just our food;
their advent is also closely linked with globalization, in its effect on social values and economic interdependence (Juma 2005, 265). Consequently, we should think of GMOs as constituting a technological shift with important normative consequences. This article will focus on this influence specifically with regards to intellectual property rights.

**Intellectual Property Rights and the WTO**

Today, the most comprehensive intellectual property rights (henceforth IPR) agreement is the 1994 Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), administered by the World Trade Organisation (WTO). It plays a significant role in facilitating trade and resolving disputes, and the WTO describes TRIPS as “legal recognition of the significance between intellectual property and trade” (WTO 2020).

TRIPS builds on the first major international agreement on industrial property, the 1883 Paris Convention for the Protection of Industrial Property. The Convention was the first step taken to ensure that creators’ intellectual works were also protected in other countries. By enshrining the norm of national treatment, which establishes that when an inventor applies to a patent in foreign country member of the Convention, the application received the same treatment as it would have, had it come from a citizen of that country (Dhavan et al. 1990, 131). However, the extent of these protections and their enforcement varied greatly between countries, and the WTO argues that as intellectual property became increasingly important in international trade, these differences were a source of tension in economic relations. As such, TRIPS attempts to bring intellectual property under common international rules.

Supporters of TRIPS argue that high uniform standards of IPR fuel innovation and a rapid transfer of technology. Moreover, they assert that TRIPS creates a more level playing field in international trade, as developing countries receive free access to the markets industrialized nations in exchange for their agreement to protect the intellectual property of foreign nationals (Hefler 2004, 2). However, conflicts have emerged between Western interests in international trade and developing countries
on the application of TRIPS to GMOs (Strauss 2009, 305). These disagreements about TRIPS demonstrate that IPR is a norm under contestation.

**Technology and Norm Change**

Constructivism is a particularly useful theoretical lens when examining normative debates due to its ontological and epistemological assertions, and it highlights the central role that technology can play. The key argument constructivism forwards is that meaning is “socially constructed,” thus positioning it as an alternative framework to the materialism of theoretical approaches like neorealism. In a socially constructed world, the existence of patterns and causal relationships depend on webs of meaning and practices that constitute them. (Hurd 2009, 300). This understanding of the social construction of interests and identities leads to the second distinguishing feature of constructivism — the mutual constitution of structures and agents. Mutual constitution importantly suggests that the actions of actors, for instance states, in international relations contribute to forming the institutions and norms of governing the international system, and these institutions and norms simultaneously influence the behaviour of those actors. For example, when states use force, they often refer to and redefine the ways in which they wish concepts like “self-defence” or “aggression” to be understood, thus reinforcing these norms of international law (Hurd 2009, 304).

These foundational concepts suggest that explaining change in the international system requires identifying the macro and micro-level practices that constitute ideational shifts (Finnemore and Sikkink 1998, 894). Wayne Sandholtz’s cyclical approach to normative change suggests that normative change is continual, a product of constant interplay between political actors. This framework provides a useful tool for understanding technology plays in this process. Sandholtz postulates that there are four phases in this process: rule structures guide actor choice, actor choice triggers disputes, disputes involve argumentation by the respective actors to advance their position, and finally, the most successful arguments result in modified rules and rule structures (Sandholtz 2007, 8-11).
Sandholtz argues that technology is particularly important to consider in relation to the second phase, when actor choice triggers disputes. Major technological changes create an international environment that generates behaviours which challenge international norms and trigger disputes. The example Sandholtz provides is the development of atomic power generating questions about what rules should apply to a potentially deadly new technology (2007, 10). The advent of GMOs similarly continues to provoke important questions about biodiversity, consumer safety, and most significantly intellectual property rights.

One of the most significant developments in this regard was *Diamond v. Chakrabarty*, a landmark 1980 US Supreme Court decision on the patentability of microorganisms. The Supreme Court ruled that a live, human-made microorganism is patentable, based on the argument development of a man-made micro-organism constitutes a manufactured invention. This decision is extremely significant, given that, previously, living beings were previously seen as a common, natural good (Brennan 1981, 341). Furthermore, it speaks to normative foundations of IPR.

**The Norm of Intellectual Property Rights**

The general definition of norms adopted by constructivist scholars is that norms are “a standard of appropriate behaviour for actors with a given identity” (Finnemore and Sikkink 1998, 891). Subsequently, the constructivist approach suggests that the reason why IPR regulation is so central to the GMO debate is that it governs the behaviour of this new technology and how it is utilised.

The World Intellectual Property Organization (WIPO) defines intellectual property as referring to “creations of the mind: inventions; literary and artistic works; and symbols, names and images used in commerce.” These can be further divided into two categories, industrial property and copyright, with GMOs pertaining to the former. Industrial property can be protected through patent protection, which means that invention cannot be used, sold or distributed without the owner’s consent (WIPO 2003, 3-5). As far as the question of the importance of IPR is
concerned, the WIPO (2003) argues that IPR encourage innovation, which in turn enhances the quality of human life.

Moreover, IPR have traditionally been legitimated on philosophical grounds through the liberal right to private property. John Locke, for example, writes in Article 26 of his Two Treatises of Government that ownership of property is created by the application of labour, given that everyone has a “property” in their own “personhood” (Locke 1823, 116). The influence of such a conception of property rights is apparent in Article 27(2) of the 1948 Universal Declaration of Human Rights, which asserts that “everyone has the right to the protection of the moral and material interests resulting from any scientific, literary or artistic production of which he is the author” (Ostergard 1999, 175).

Whether IPR are universal human rights is another extremely interesting debate, but one which is beyond the scope of this article. However, the discussion above suggests that IPR are not value-free legislative measures but instead powerful tools that are informed by certain Western liberal ideas about individualism and the potential of private economic power. IPR should therefore be understood as a normative concept that is subject to contestation.

Technology and Norm Contestation

Alan Bloomfield argues that the literature focusing on norm studies has conceptually privileged norm entrepreneurs, actors who promote new global norms (2016, 310). Certainly, Sandholtz’s cyclical theory of norm change, as well as Finnemore and Sikkink’s work, rely on actors in the international system to take action that stimulates normative change. These frameworks, Bloomfield asserts, fail to theorise resistance to norm change to a sufficient extent. As a result, norm change becomes a streamlined, one-way process, as opposed to an area of contestation. Examining resistance is crucial to understanding the issue of intellectual property rights and GMOs.
Bloomfield (2016) positions “the norm antipreneur” in an oppositional to “norm entrepreneurs” who push for norm change. These actors either defend or challenge the status quo, respectively. Moreover, Bloomfield suggests that these actors can be placed on a spectrum. The actors that most insistently push for change are “pure norm entrepreneurs,” and the actors that implacably resist change are “pure norm antipreneurs.”

The notion of norm entrepreneurs and antipreneurs is particularly useful for understanding GMOs and IPR, as it allows the controversy to be understood as the clash between two opposing normative paradigms. The first of these, and one which is still prevalent in many developing countries, is a tradition of farmer community rights, in which nature and its resources, for instance seeds, are regarded as gifts to be shared by the community. Therefore, these resources are not commercialized. The second paradigm is based on individual ownership and formal IPR, in which, in contrast to community rights, the farmer is distanced from the breeder (Adi 2006, 107). This latter paradigm is facilitated by the technological shift that enables living organisms to be “invented” - GMOs.

Following the constructivist framework developed in this article, the TRIPS agreement should be understood as representing a normative shift towards IPR, and one facilitated by norm entrepreneurs. These efforts were most notably led by the US, who sought an agreement designed to provide IPR standards that increase revenue flows back to countries exporting intellectual property, such as the US. US companies Monsanto and DuPont Pioneer accounted for 26% and 18.2% market share of global seed sales, respectively, in 2013 (ETC Group 2013). In fact, according to Greenpeace, Monsanto sold 90% of GMO seeds in 2009 (RESET 2019).

One reason for US' support for IPR is that its legislative bodies are inclined to taking a favourable stance to the development, protection and deployment of such new technologies. Article I: Section 8: Clause 8 of the United States Constitution grants the US Congress the enumerated power “to promote the progress of science and useful arts, by securing for limited times to authors and inventors the exclusive right
to their respective writings and discoveries” (Strauss 2009, 292), an assertion articulated in a noticeably similar manner to the Lockean right to property. It should therefore come as no surprise that it was in the US that patentability of GMOs was first established, under the landmark 1980 *Diamond v. Chakrabarty* Supreme Court case (Brennan 1981).

India, in contrast to the US, is a norm antipreneur. Agriculture plays an important role in the economy and is largely upheld by smallholder farmers. India is notably the second-largest producer of cotton in the world behind China; however, productivity has traditionally been low (Sheth 2017). This helps explain why Bt cotton become the first GMO to be introduced to the country in 2000 (Ramanna 2006). By 2012, GM cotton accounted for 88% of cotton acreage in India by 2012 (Thomas and De Tavernier 2017), yet indigenous NGOs and activists, for instance farmers in the region of Karnataka, continue to fiercely oppose GMOs. India has tragically witnessed nearly 300,000 farmer suicides over the past few decades (Mishra 2006) and opponents of biotechnology blame Monsanto, arguing their extraction of royalties pushes farmers into oft-unmanageable debt. One of India’s most vocal anti-GMO activists, Vandana Shiva, writes that “through patents on seeds, Monsanto has become the ‘Life Lord’ of our planet, collecting rents for life’s renewal from farmers, the original breeders” (2019). Moreover, the website of Shiva’s organization Navdanya features the following statement on GMOs and IPR: “The new IPR laws embodied in the TRIPs agreement of WTO have unleashed an epidemic of the piracy of nature’s creativity and millennia of indigenous innovation” (van Dycke and van Overwalle 2017).

**Norm Contestation and Power Relations**

The example of India, similar to other developing countries party to TRIPS, demonstrates the influence of power on norm contestation. Their vehemence demonstrates the relationship between developing countries and the West under TRIPS. Monsanto first approached the Indian government about Bt cotton in 1990 but was rejected. In 1995 however, MAHYCO, an Indian seed company, was allowed to import Bt cotton under a Monsanto licence, and in 1998 Monsanto
acquired a 26% share of the company. The crop was ultimately introduced through a joint venture called Monsanto-MAYCO Biotech (Ramanna 2006, 7).

The introduction of Bt cotton in India demonstrates the economic power of Western companies like Monsanto. Monsanto, in particular, asserts this power by suing small farmers in the name of protecting its GMO patents (Harris 2013). A more important example for this article, however, are the so-called “TRIPS-plus” agreements negotiated by the US and other Western states. TRIPS importantly establishes “the minimum standards of protection and enforcement” (WTO 2020). Interestingly, these minimum standards make two significant exceptions with regards to GMOs. Firstly, under Article 27(2) “members may exclude from patentability ... [that] which is necessary to protect ordre public”, and under Article 27(3)b plant varieties shall be protected by patents, an effective sui generis regime or a combination of both (Correa 2000, 17). In other words, for plant varieties, as long as there is some level of protection, including a regime’s unique to individual members, there is no requirement for international standardisation under TRIPS (Strauss 2009, 306). To overcome this provision that could weaken the intellectual property or their GMO products, the US, in particular, has pressured developing countries into bilateral “TRIPS-plus” agreements that contain more stringent standards and shorter transition periods (GRAIN 2001). The implications of these agreements are vast, especially in light of the global distribution of genetic resources. 83% of in-situ resources are found in the global South, whereas 75% of ex-situ resources can be found in the West. Moreover, roughly 70% of all biomaterials are held in collections in industrialised Western countries, despite most of these originating from the South (Adi 2006, 97).

With regards to norm contestation, the need for “TRIPS-plus” agreements suggests that, despite the technological shift that GMOs represent, the norm entrepreneurship by Western countries such as the US has only been of limited success at the WTO level. However, they are able to overcome this through their ability to pressure developing countries into bilateral agreements.
Conclusion

This article has aimed to demonstrate that GMOs constitute a technological shift with important normative implications, especially with regards to how we understand intellectual property. Whereas living organisms were traditionally seen as natural goods, genetic modification can render such organisms man-made inventions, and thus subject to IPR. To understand these normative implications, the article has used constructivist norm theory to discuss the role of technology in norm change and contestation, focusing specifically on the WTO TRIPS Agreement. The article concluded contrasting the US and India and their respective experiences of the TRIPS agreement, to demonstrate the importance of power relations for understanding how actors try to succeed in their contestation of norms - in the case of the US this involves negotiating additional bilateral treaties with developing countries.

The approach adopted by this article also provides a framework through which we can consider the norm dynamics of other technological shifts. One example that comes to mind is the implications of the advent of artificial intelligence on privacy norms and regulation. As such, this article hopes to provide a valuable contribution to understanding the impact of technology on global governance.

Bibliography


Renewable Energy Technologies and State Security: Current Shield and Future Sword?

Harris Siderfin *

“We deserve a safe future. And we demand a safe future. Is that really too much to ask?” (Thunberg, 2019)

The greatest challenge facing global politics today is climate change. Climate change does not only threaten current global practices but threatens human existence itself. Between 1880 and 2012, average global temperatures increased by 0.85 degrees (IPCC 2014). The 2018 report of the Intergovernmental Panel on Climate Change (IPCC) states that regional effects had been even more severe: 20-40% of the global population have experienced temperature increases of 1.5 degrees (IPCC 2018). If the increase in temperature continues on this trajectory, life as we know it will cease to exist. If climate change is significantly affected by human actions such as through unsustainable resource harvesting and climate change threatens state security, why do states not do more to stop climate change?

One explanation can be found by examining the neoliberal framework on which the current international system (IS) is based. Peace within the IS is maintained through the economic interdependence between states (Moravcsik 1997, 520-524). Therefore, states prioritise economic performance, since the strength of a state's economy determines the states’ relations with other actors within the IS (Khan 2016, 16). As actors in the IS are motivated by economic benefits, self-imposed restrictions on the use and extraction of finite natural resources would be detrimental to the state's interest, especially if other states did not follow the same restrictions. Another issue is that the effects of climate change do not discriminate, thus creating asymmetric interests for states as some will be affected by changing climates more than others even if they produce lower carbon emissions (Bernauer 2013, 430). So even if a state

* 2nd year undergraduate student, International Relations.
took action to reduce carbon emissions, resulting in reduced economic gains, their security would not be ensured. It would be unlikely that other actors would move away from carbon-producing energy resources, which put all states’ security at risk. Due to this, it is challenging for states to move away from these more primitive forms of energy production. Through the utilisation renewable energy technologies, states can arguably reduce security threats posed by climate change, create safe and sustainable energy, negate energy dependence between states, and eventually become geopolitical powerhouses, if they embrace this technology early.

This essay will utilise neorealist theory to discuss the current and future importance of renewable technologies. It will argue that states should utilise renewable technologies to fulfil the bedrock assumptions set out by John Mearsheimer (2001). I thus develop the argument that states’ use of renewable energy technologies is, in fact, in line with neorealist thought. This essay will firstly discuss security issues surrounding climate change and the use of fossil fuels. It will then illustrate how the use of renewable technologies could eradicate energy security issues as natural resources diminish. This essay will also discuss the ability of renewable technologies to alleviate the power imbalance between natural resource-rich and poor states, freeing states from energy reliance dynamics. Finally, this essay will argue that renewable technology and energy will allow states maximize their power and therefore satisfy the criteria laid out by Mearsheimer's neorealist bedrock assumptions.

**Mearsheimer's Bedrock Assumptions**

This section will develop the central theory of this essay, investigating the core characteristics of neorealism, as presented by Mearsheimer. In *The Tragedy of Great Power Politics*, John Mearsheimer explains why states act aggressively and seek to maximise power vis-à-vis other states. Mearsheimer theorizes five assumptions about the international system (IS) that seek to explain this state behaviour (Mearsheimer 2001, 29). I am drawing on these assumptions to develop the argument as to why states should utilise renewable technologies to maximise their relative power. Mearsheimer's first assumption is that the IS is anarchic, which is not
to say that it does not consist of a sense of order, but rather that there is no higher authority than the state (Mearsheimer 2001, 30). State sovereignty is the result of there being no higher ruling body; there is no “government over governments” (Claude 1988, 14). This is essential for understanding state interactions within the IS: there is no insurance of the state’s security. Mearsheimer states that all great powers inherently have offensive power, which allows them to harm each other (Mearsheimer, 2001, 30). This offensive power manifests itself in the form of weaponry or the population size, which could be mobilised in a military capacity. I want to add a state's ability to produce and export energy as a critical component of offensive power in the 21st century. The so-called “energy weapon” is an essential tool in a state’s arsenal (Stegen 2018, 78; Yergin 1990). As most states have a form of offensive capability, without another structural mechanism to ensure their security, such as supranational organisations (an organisation with authority over the state), states fear one another. Only a true hegemon can be in a position where they do not fear other states. This leads to another bedrock assumption of Mearsheimer: a state’s intentions can never be guaranteed. Intentions are liable to change over time in a system with no form of over-arching authority, and the uncertainty of other states’ intentions is inevitable (Mearsheimer 2001, 31). The final assumptions proposed by Mearsheimer that shape neorealist theory are that survival is the primary goal of states and great powers and that states are rational actors. States understand the system they exist within and will act strategically and rationally to survive and adapt to a self-help system (Mearsheimer 2001, 30-32; Waltz 1979, 88-93). The combination of these assumptions determines how a state should act in the IS and explains why states' interactions can become hostile and defensive.

**Fossil Fuels and the Immediate Security Issue of Climate Change**

Mearsheimer’s fourth assumption, according to neorealist theory, should be all states’ priority: The issue of a state's immediate security. Climate change became an issue of global discussion in the 1980s when strong links were drawn between industrial activity and global warming (Cass 2017). More greenhouse gasses (GHGs), such as carbon dioxide and methane, are present in the earth’s atmosphere today due to human activities such as the burning of fossil fuels and intensive farming
A continuous increase in global temperatures has and will continue to threaten both state and civilian security. Increased global temperatures lead to rising sea levels, drought, and extreme weather, all of which have significant and harmful effects on human life (Cass 2017). The 2017/18 Cape Town drought illustrates how a minor change regional climate can have a significant adverse effect on a state. In agriculture alone, the drought in Cape Town cost the South African economy an estimated 5.9 billion rand as well as causing widespread civil unrest across the region (Smith 2018). Although deaths during natural disasters appear to be relatively small, the economic and cultural damage is unfathomable. The 2019/20 bush fire season in Australia took the lives of 33 people, blackened a total area roughly the size of Ireland, destroying thousands of homes while releasing further toxic gases into the atmosphere. Australia’s unique wildlife and ecosystems will never fully recover from these fires (Corderoy and Cox 2020). The Australian economist John Quiggin (2020) stated that the fallout from these fires would cost the Australian government over 100 billion Australian dollars (Quiggin 2020).

Following these events, the domestic public, through the use of national summits, called for more stringent climate policy, imploring the government to commit to a zero-emissions plan (Doherty 2020). Despite this public concern for climate change, Australia ratified emission reduction goals set in the Paris agreement from 26-28% reduction in 2030 to 17-19% reduction (Climate Action Tracker 2019). The United States (US) is the second-largest contributor to CO2 emissions only being surpassed by China, a state with a population of approximately 1.393 billion compared to the US’ 326 million (World Bank 2020; Wang 2020). Despite climate change threatening large coastal areas of the US and its significant contribution to its security threat, the US pulled out of the Paris Agreement in 2016 (US Department of State 2019). Here we face a paradox: according to neorealism, the state should prioritise its survival above all else. There is strong evidence that burning fossil fuels contributes to climate change. For states to continue using fossil fuels to produce energy is irrational and defies, Mearsheimer’s fourth and fifth assumption about states. The utilisation of renewable technologies to produce clean energy would resolve these security issues in a way to ensure state security. Other alternative energy production
methods such as nuclear power are less stable and can threaten global state security (see Fukushima Daiichi (2011) and Chernobyl (1986) nuclear disasters). Therefore, in order to maintain both economic and state security, states should utilise renewable technology as an energy-producing means.

The Issue of Energy Security

Having investigated the immediate security threats, this section will now discuss energy security and how the use of fossil-based energy poses significant issues for a state’s energy security. States must have a rationale for employing non-sustainable methods of energy production. This leads to the issue of “energy security.” Simply defined by Deutcht and Schlesinger, energy security is the “the reliable and affordable supply of energy” (Deutcht and Schlesinger 2006, 3). Energy security has been an issue of increasing importance in states’ foreign policy. It is becoming more prevalent in American foreign policy as relations between the US and oil-producing middle eastern states have deteriorated. As Klare states, energy is central to all human endeavours; as society grows and develops, the more reliant it is on energy (Klare 2018, 498). Today’s society utterly depends on a consistent and reliant source of energy. Without energy security, states would be unable to maintain domestic life and defend itself sufficiently from other powers within the IS. The modern state is completely and utterly at the mercy of energy. Due to states’ dependence on energy, I argue that a significant energy supply and a means to export contributes to a state's offensive power. As energy/resource-poor states energy security is dependent on the supplying state, the energy supplying state could coerce dependent states with the threat of cutting off energy supply and, in doing so, compromising resource-poor states energy security. This has led states such as the US to increase domestic energy production to increase their relative power, as well as kerbing other states’ (Klare 2018, 502; Friedman 2018).

The primary sources of energy are oil, gas, and coal, which are harmful to the environment, causing climate change issues, as already discussed. The second significant issue of these fuels is they are finite; they will run out, and when they do states’ energy security will be severely threatened. Some scholars fear a period of
insufficient energy supplies at crucial points in the near future (Kalicki and Goldwyn 2013; Klare 2008).

As the global population continues to increase, the demand for energy also increases. Between 2012 and 2040, global energy consumption is estimated to rise from 549 to 815 quadrillion British thermal units (BTUs) (U.S. Energy Information Administration 2016a, 163). As consumption increases, availability of fossil fuels decreases. This inverse relationship highlights a significant issue of energy security when states rely on fossil fuels for energy production. At the current global consumption rates, it is predicted that the majority of “easily” accessible natural gas, oil and coal reserves will be depleted by 2030 (Moriarty and Honnery 2009; Heinberg and Fridley 2010). Only remote or hard to reach locations such as deep-sea and artic location will be options for resource extraction (Klare 2018, 498). Extraction from such locations makes recovery of such resources more difficult and thereby making extraction more costly. The longer states rely on fossil fuels for energy production; the less affordable energy will become. This undermines Deutch and Schlesinger’s second concern for energy security an “affordable source of energy.” As the affordability of natural resources will continue to decrease, states should utilise renewable technologies. The initial immediate economic disadvantages of renewables would be cancelled out over several years, as they would provide the state with a source of sustainable energy, which costs would not be dependent on the supply of natural resources. The reliance on energy produced by natural resources poses a threat to energy security and, therefore, economic and state security. This means that if Mearsheimer’s assumptions are acted upon, the rational action for states would be to invest in renewable technologies to ensure energy security in the future.

Energy Dependence Relations: A Threat to State Security

Another critical aspect of energy security is the “unhindered delivery” of energy from the producer to the eventual consumer (Kalicki and Goldwyn 2005). The traditional definition of geopolitics acknowledges the influence of geography upon the foreign relations of states (O’Sullivan, Overland and Sandalow 2017, 1). Oil and
natural gas resources are not equally distributed among states. As nearly all states in
the IS require substantial amounts of energy but do not have sufficient supplies
within their territories to meet their demands, they must rely on imports from
foreign suppliers (Klare 2018, 498). There are several issues when energy supply is
dependent on external suppliers. The first issue being the movement of supplies
from one region to another. Oil tankers and pipelines are vulnerable to attacks from
terrorist groups and hostile state actors (Klare 2018, 498-499). An example of this is
the seizure of two British oil tankers by Iranian forces in 2019 (Marcus, 2019). If
accessibility of foreign energy supplies is not guaranteed, this compromises a state’s
energy security. Another compromising factor of trans-national supply relate to the
origins of the resources. Significant amounts of global oil are extracted in Middle
Eastern states (US Energy Information Administration 2020). Middle Eastern States
have been prone to disruption of oil supplies due to embargos, terrorism, and
conflict, as the current political climate is unstable (Klare 2018, 499). Securing the
energy supplies in this region thus entails dimensions of foreign policy, diplomacy,
and military intervention. For example, the US has had a significant military
presence in the Gulf region since the Carter doctrine ensured the flow of oil to the
US and the global economy (Klare 2018, 501-502). The extensive cost of maintaining
this oil flow is unnecessary. If renewable technologies were utilised, energy security
would not be dependent on costly and vulnerable transportation methods and
would allow for easier access to remote areas. A better use of economic resources
would be an investment in renewable technologies which are wider-reaching and
less susceptible to disruption. This can be seen in India, where more than 10,000
remote villages have received basic electricity through distributed renewable energy
from solar and wind farms (O’Sullivan, Overland and Sandalow 2017, p. 2). If states
want to maximize their power and to gain the most from the investment of their
resources, it is essential for them to focus on modern energy security that allows
secure and reliable renewable energy.

Hydrocarbon dependence also creates an unequal power dynamic as the dependent
state attempts to maintain its energy security (Stegen, 2014). The resource supplying
state can utilise the dependency to create leverage and force the dependent state to

31
act in a way that the supplying state wishes. A recent example of a state offensively utilising energy supplies would be the disruption of gas supply from Russia to the Ukraine in 2014 after relations began to breakdown between the two states (Kirby 2014). This illustrates how energy security and supply can be utilised offensively, giving the energy resource-rich state greater ability to coerce other actors in the IS. To freely give states this power goes against the principles of neorealist theory. In order for a state to survive, a state must attempt to be more powerful than other actors within the IS (Morgenthau 1948; Mearsheimer 2001). The relative power of resource-rich states will further increase as natural resources become scarcer. Resource-rich states’ leverage over-dependent states will increase, as non-renewable wielding states have little option to ensure energy security, leading to increased economic cost and reduction in authority for dependent states. However, when states utilise renewable technology to produce domestic energy, they will no longer be affected by this power dynamic, disarming resource-rich states “energy” weapon as state using renewables become self-sufficient. This would be in line with neorealist theorisations of independence as a basis of power maximising (Krasner 1978; Mearsheimer 2001).

Once states make the transition to renewable sources of energy instead of hydrocarbon, a power transition will slowly occur from fossil fuel reliant states to states that use renewables. As fossil fuel supplies decrease, the relative power of resource-rich states decreases as well, thus threatening states’ energy security. As renewable wielding states will not be affected by this, their power will increase within the IS. As fossil fuel-dependent states’ energy security is jeopardised by decreasing hydrocarbons, they will need to look to alternative energy supplies. States who have started early to invest and develop in renewable efficient technologies are likely to gain the power lost by oil supplying states. Like an hourglass, power will slowly diffuse from natural resource-rich states to independent renewable states. This could eventually lead to a complete flip of the energy economy, where states which process sophisticated renewable technology will become the suppliers of energy to a new kind of energy market between states.
Conclusion

In conclusion, the argument for the use of renewable energy is in line with neorealist theory. Drawing on neorealist theory, a power maximising state should develop and use renewable technology for energy production. Alternative energy sources such as nuclear and hydrocarbon-based energy production methods threaten a state's security (the most critical issue for a state according to neorealism). This is illustrated by the fact that hydrocarbon-based fuel is a significant contributor to climate change, which threatens most aspects of the current IS. The finality of fossil fuels also poses a significant issue for energy security as they will eventually run out. Reliance on natural resource energy also creates unequal and unacceptable power dynamics between resource-rich and poor states, which only escalate further as resources diminish. The utilisation of advanced and efficient renewable technologies would mitigate the issues faced by states using fossil-based energy supplies. The utilisation of renewable technology would also give renewable wielding states more relative power in the future IS and the energy economy - as natural resources diminish, thus making these states, as proposed by neorealism, maximize their power.

Bibliography


Computational Propaganda During Democratic Elections: Vote Leave’s Violation of International Law

Ella Kiley *

This paper aims to display how computational propaganda during democratic elections undermines international law, and thus how it is possible to integrate such concerns under this framework to protect the rights of the individual during democratic processes. For the purpose of building a specific case, the Vote Leave campaign on Facebook will be used as an example, but the basic case can be applied to multiple campaigns across the world. It is therefore an issue for international law as it occurs in multiple states with the use of transnational computational corporations. Vote Leave, in partnership with data mining company AggregateIQ, used techniques of microtargeting and disinformation on Facebook as part of their official campaign in the run up to the Brexit referendum. The paper will divide the issues contravening international law into three components: microtargeting and big data, the disproportionate targeting of immigrants as objects of discontent, and disinformation. It will identify the laws that these issues contravene, and suggest ways in which the specifics of computational propaganda can be incorporated explicitly into legislation. I will argue that the campaign’s use of computational propaganda constitutes information warfare in the implementation of psychological operations (PSYOPS), and contravenes international law on at least nine accounts. As many conventions of international law are not legally binding and are instead based on norms, this paper does not seek to suggest or encourage legal repercussions for the campaign, but rather to situate such a phenomenon in international constitutional consciousness, and to highlight the implications so that future campaigns may be better identified and regulated.

* 4th year undergraduate student, Arabic and International Relations.
Microtargeting and Big Data

This first section concerns the methods, rather than the content, of the Vote Leave campaign. Microtargeting during democratic campaigns refers to the use of marketing techniques to spread political propaganda in the creation of “finely honed messages targeted at narrow categories of voters based on sophisticated combinatorial analysis of data garnered from individuals’ demographic characteristics and consumer and lifestyle habits” (Gorton 2016, 62). Two problematic elements of this method include a lack of freedom of access to information, as the information an individual is exposed to is decided by a computational algorithm; and the inhibiting of public dialogue, as individuals are prevented from accessing information that challenges their beliefs and values, and interaction only occurs between like-minded people, known as the “echo chamber” effect (Del Vicario et al. 2017, 6; Helbing 2019). Vote Leave used the microtargeting technique by employing AggregateIQ to disseminate targeted propaganda on social media.

Microtargeting and the resultant “echo chambers” undermines the principle of the “wisdom of the crowds,” a theory underpinning decision-making in democracies, whereby educated people are required to independently gather and judge information in order to form their own opinions (Helbing 2019, 58-59). The importance of accessing information through serendipity, especially during democratic processes, is a widely understood necessity for human development (Ratti and Helbing 2019; Gorton 2016; Helbing 2019). Microtargeting’s inhibiting of the individual’s autonomy over the information they access, when datasets are formed of target audiences for specific propaganda content, contravenes the International Convention on Civil and Political Rights. Article 19 states that “everyone should have the right to hold opinions without interference… this right shall include the freedom to seek, receive, and impart information on ideas of all kinds.” The technique of microtargeting in political campaigns undermines Article 19, as there is a severe lack in the freedom to seek and receive information, hampering individual autonomy over the information, and thus knowledge, acquired.
The use of big data and microtargeting reframes what constitutes knowledge (or what is thought to be true), and the implementation of such a technique raises major concerns surrounding the agency of publics, as Baack (2015, 1) suggests that “agency is deeply connected to the distribution of knowledge and power.” This agency needs to be protected if a free and fair democratic political campaign is to be carried out in the future. The undermining of public agency in relation to the acquisition of knowledge is in violation of the International Convention on Civil and Political Rights, as Article 18 states that “everyone should have the right to freedom of thought, conscience, and religion.” Similarly, the Universal Declaration of Human Rights Article 19 emphasises “Freedom of Opinion and Expression” to be integral to the rights of every individual. The building of data profiles on individuals, and subsequent use of this data to target such individuals, seeking to “alter voters’ beliefs and behaviours by intentionally and precisely targeting their unconscious and cognitive processes” (Gorton 2016, 75), inhibits this requisite for freedom of thought, opinion, and expression. Targeted computational propaganda therefore inhibits freedom of opinion and expression by undermining a robust marketplace of ideas (Leiser 2019). Individuals’ potential to act in an agentic manner is significantly stunted (Baack 2015, 2) when their access to information and thus knowledge is predetermined by a heteronomous technocratic agent.

Additionally, AggregateIQ’s harvesting of data often occurred without the individual’s knowledge or consent, whereby the traces of data people leave behind are “often unconscious and not meaningful to them” (Baack 2015, 2). This significantly violates Article 12 of the Universal Declaration of Human Rights which concerns the “Right to Privacy.” There are significant data protection laws in place that are often not adhered to. The existing laws under the EU General Data Protection Regulation that should be incorporated in order to safeguard publics in online campaigns during democratic processes include Article 21, which states the “Right to Object,”2 and Article 22, which incorporates “rights related to automated

---

2 The GDPR gives individuals the right to object to the processing of their personal data in certain circumstances. Individuals have an absolute right to stop their data being used for direct marketing. In other cases where the right to object applies you may be able to continue processing if you can show that you have a compelling reason for doing so. You must tell individuals about their right to
decision-making including profiling." It is my suggestion that these two Articles are incorporated into the International Convention on Civil and Political Rights under a new subcategory pertaining to “Data Rights in Political Campaigns.” It is then my suggestion that Facebook (and other platforms) incorporate Articles 21 and 22 in their privacy settings, so that every individual user is able to actively opt out of their data being processed and utilised for political targeted messaging campaigns.

**Immigrants as the Primary Objects of Propaganda**

A challenge to analysing data for such investigations is that the dissemination of such graphics relies on computational algorithms and carefully compiled datasets. Many of the graphics are also untagged and anonymous, further making them difficult to track. Therefore, unless the researcher falls inside a dataset and is exposed to the content this way, accessing the graphics is challenging unless the agents release them to the public. The following data presented was collated by myself, after analysing the compilation of graphics that were supplied to Facebook by the Vote Leave campaign. Facebook submitted over 100 pages of graphic content to the UK Government’s Digital, Culture, Media and Sport Committee during an investigation into Fake News after the referendum. I personally analysed every graphic that was submitted. All evidence is based on these graphics alone, including any quotations.

The identification of immigrants as the main objects of discontent makes up the largest proportion (32%) of the themes displayed in the graphics. It is important here to recognise the need to uphold Article 19 of the Universal Declaration of Human Rights, regarding “Freedom of Opinion and Expression.” The issue taken with the focus on immigration in the Vote Leave content is not with the subject of immigration itself, but with the fact that specific nations and peoples are targeted, and also due to the false information regarding these nations’ relevance in the specific political campaign. Figure 1 illustrates the various named objects of the

---

object. An individual can make an objection verbally or in writing. You have one calendar month to respond to an objection.” (Information Commissioner’s Office)

3 “[A]utomated individual decision-making (making a decision solely by automated means without any human involvement); and profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.” *Ibid.*
graphics concerning immigration. It is worth emphasising that non-European nations and peoples constituted 79% of the Vote Leave campaign’s visual propaganda that targeted immigrants as objects of Britain’s dissatisfaction with the EU.

*Figure 1: Named objects of immigration discourse*

The content illustrated in Figure 1 contravenes Article 20 of the International Convention of Civil and Political Rights, which states that “any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be prohibited by law.” By identifying particular nationalities to be the objects of dissatisfaction, the campaign was guilty of incitement to discrimination of these targeted peoples. No target communities should be named as objects of dissatisfaction during a political campaign, and therefore the only legitimate content relating to immigration should be the 27% relating to EU laws and policy. Identifying specific peoples and nations to induce fear of the “other” during the campaign constitutes discriminatory content. This also contravenes Article 4 of the International Convention on the Elimination of all Forms of Racial Discrimination, which states that “States Parties condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination.”
To give an example of this incitement to discrimination, Graphic 1 is an exemplification of the targeting of named nationalities as objects of discontent. The image portrays non-white, non-European immigrants to be an existential threat to the British public.

*Graphic 1: an example of one of the graphics provided to Facebook by Vote Leave*

![Map graphic](2968.jpg)

Graphic 1 constructs two distinct groups. The distinction between the “British self” and the “non-white immigrant other” is denoted by using contrasting colours to shade the two groups on the map, and through the use of the possessive pronoun “our” to describe the NHS (highlighting British group identity as separate from “them”). This inference to a British “us” makes the NHS symbolic of the British public as a whole. The British public is presented to be under threat from the peoples of the counties named and highlighted. By showing figures of people in the arrows emanating from these countries towards the UK, the graphic is suggesting that stopping the influx of these people would “save” the NHS. The graphic is therefore projecting the fragility of the British public sector, in this case the NHS, onto non-white immigrant objects. The projection therefore portrays the “immigrant other” as an existential threat to the British public sector, and the British public by association. The graphic, like many others, constructs named peoples as objects of discontent, and thus constitutes discriminatory content.
This discourse can be considered to have legitimised racialised populist ideas that culminated in racist hate crimes rising 500% in the four weeks after the referendum (Virdee and McGeever, 2018). It has been reported that the irony of the racist attacks reflects the Vote Leave campaign, in that many of the attacks reported were not against EU immigrants. For example, a Sikh radiographer reported how a patient declared “we voted you out.” Virdee and McGeever’s (2018, 1808) analysis sees how the wave of violence reflected the (ill)logic of the Vote Leave visuals: “perpetrators made little attempt to distinguish between black and brown citizens [of the UK] and white European migrants – in their eyes, they were all outsiders.” This campaign therefore worked to contravene the Universal Declaration of Human Rights Article 29, which stresses that the “Duty to your Community” should be respected. The disproportionate targeting of non-white groups in the campaign content has resulted in the legitimisation of racially driven discrimination towards existing non-white UK citizens, as well as current and future migrants.

It is important to emphasise that this is not a suggestion that the content of the Vote Leave campaign has a causative relationship to the rise in racially driven hate crime in the UK, but rather has a correlative relationship. It would be incorrect to suggest that the computational propaganda created racist views, rather the graphics legitimised such views – facilitating “a fillip to popular racism” (Burnett 2017, 85) - as the norm for individuals who received targeted messaging with no countering viewpoints in their “echo chamber.” Where a political campaign disproportionately targets named groups of people as objects of dissatisfaction, and this is materialised in a rise of cases whereby this rhetoric is actualised in acts of hate, the political campaign should be held accountable. This can be done by further integrating such scenarios into existing international law, through Article 2 of the Universal Declaration of Human Rights, which expresses the importance of “Freedom from Discrimination.”

**Disinformation**

Disinformation refers to “inaccurate or manipulated information content that is spread intentionally” (Bennett and Livingstone 2018, 133). It is distinct form
misinformation, which refers to the inadvertent spread of inaccurate information (134). As Figure 1 shows the majority of the immigration rhetoric to be focused on non-EU individuals and nations, it is also important to recognise how such content is not only discriminatory and inflammatory, but also misleading, and, at worst, actively supplies disinformation. Inflammatory and false statements dominate the content, such as “we are giving £2 billion to Albania, Macedonia, Montenegro, Serbia and Turkey to join the EU. Seriously.” This discourse is providing active disinformation to voters by stating that certain countries are joining the EU and naming a precise figure that it is said to be costing, when some of those mentioned have merely applied, and so far, been unsuccessful. Syria and Iraq, which make up 12% of the content, have no relevance to the EU whatsoever, and appear to be examples of blatant xenophobic disinformation. The danger of this discourse has been noted by UN High Commissioner for Human Rights Zeid Ra’ad al-Hussein, who stated that “while migration and refugee issues are completely valid topics for public debate, it is imperative that migration policy decisions that affect people’s lives and fundamental human rights should be made on the basis of fact – not fiction, exaggeration, or blatant xenophobia.” (Office of the High Commissioner for Human Rights 2015) Figure 2 shows the nature of the immigration content, and the significantly high proportion of disinformation in such inflammatory graphics.

*Figure 2: Nature of information concerning immigration*

These results display how the use of computational propaganda is “one of the most powerful new tools against democracy” (Woolley and Howard 2017, 7). The fact that
microtargeting produces mass messages that are able to “fly under the radar of the press and broader public, markedly increasing their power to mislead and misinform viewers with impunity” (Gorton 2016, 72) contributes to the understanding of how the Vote Leave campaign and use of deliberate disinformation was able to dissipate to voters without being visible to those who would criticise and question such rhetoric. Article 21 of the Universal Declaration of Human Rights states that “the will of the people shall be the basis of the authority of government; this will shall be expressed in periodic and genuine elections which shall be by universal and equal suffrage and shall be held by secret vote or by equivalent free voting procedures.” Here, I draw into question the genuineness of the campaign, after viewing the evidence that shows the active misleading of voters.

Figure 3 shows the broader nature of information supplied by the Vote Leave campaign, taking into account the entire body of visual content. Where disinformation is concerned, graphics displayed actively false information, such as numerous claims that the UK spends £350 million on the EU every week, or that Turkey, Albania, Macedonia, Serbia, and Montenegro are all imminently joining the EU.

**Figure 3: Nature of information in graphic content**

![Nature of information chart]

It is here that I propose that legislation be incorporated into international law to condemn the use of disinformation, and that partnered with the technique of microtargeting in computational propaganda, it constitutes a form of information
warfare. In order to protect values of freedom of speech, I am suggesting that the use of statements that purposefully mislead voters should be condemned under Article 21 of the Universal Declaration of Human Rights, that indicates rules and norms for the functioning of democratic processes. It is only the active disinformation that should be regulated, rather than any ideological opinion.

The disinformation graphics should be considered a form of PSYOPS (campaigns aimed at conveying selected information to targets in order to influence their motives, emotions, and objective reasoning, with the aim of affecting the behaviour of governments, groups, or individuals (Blokh and Alexandrov 2016)), which should be thought of as a weapon. It is worth emphasising that many data harvesting companies, such as the SCL Group (whose subsidiary is Cambridge Analytica) started as military contractors (The Great Hack, 2019). Brittany Kaiser, former employee of Cambridge Analytica, highlighted how the targeting tool of such propaganda used to be so dangerous that it was designated “a controlled export” by the British government, meaning that the methodology was considered to be a weapon, and such computational propaganda constitutes “weapons grade communications tactics” (Kaiser 2019, The Great Hack). Therefore, it is my suggestion that a new article be built into Article 21 of the Universal Declaration of Human Rights, prohibiting the use of active disinformation in political campaigns. Where political campaigns use disinformation in computational propaganda, they are deliberately targeting the emotions of individuals using false information in order to influence their behaviour (Leiser 2019). When a campaign uses this to obtain votes, this is an act of information warfare.

Conclusion

The Vote Leave computational propaganda – which is constituted by the method of microtargeting using big data, the disproportionate demonization of immigrants as objects of dissatisfaction, and the active use of disinformation - violates international law on numerous accounts. This is noticeable in Articles 18, 19, and 20 of the International Convention on Civil and Political rights; Articles 2, 12, 19, 21, and 29 of the Universal Declaration of Human Rights; Article 4 of the International
Convention on the Elimination of all Forms of Racial Discrimination; as well as Articles 21 and 22 of the EU General Data Protection Regulation. It is my proposition that these two latter laws be integrated into Article 19 of the International Convention on Civil and Political Rights. Disinformation is the most difficult issue to regulate in international law, due to the important standard of upholding freedom of expression and political thought. It is worth emphasising that the technique of microtargeting actually further inhibits freedom of opinion and thought. I therefore want to suggest that disinformation campaigns targeting a population during a democratic process should be considered to be an act of information warfare, and should be prohibited, by being integrated into Article 21 of the Universal Declaration of Human Rights. It is possible to regulate the emerging and fast-paced new technologies that threaten our autonomy and the future of democracy.

Bibliography


INTENTIONALLY LEFT BLANK
Uncertainties of Climate Change: Demystifying New Technologies as a Silver Bullet and Embracing Uncertainties

Maël Ihamouchene *

Ever since the emergence of climate change at the top of the global political and scientific agenda, its uncertainties made the policy decision-making process increasingly speculative and vulnerable to attacks. As time goes on, these uncertainties take over the debate, leading the way to ideologically-b(i)ased decisions in place of fact-based ones. Insofar as climate uncertainties can be decreased, but are unavoidable, they are a major issue. Although they are inherent to science, the debate around climate change has been weakened by climate sceptics who have made of climate uncertainties an argument to strengthen the validity of their denialism. This paper explores how new technologies will impact the uncertainties of climate change and, ultimately, its governance. It will suggest a new approach on climate uncertainties. Rather than perceiving them as a politically constraining issue, the paper will argue that uncertainties are fostering innovative knowledge and that their reification should be addressed through an emphasis on their social construction. The first part of the paper will contextualise the debate in addressing the links between climate change governance and its uncertainties and the second section will suggest a new paradigm regarding their perception.

Uncertainty and Climate Change Governance

The Intergovernmental Panel on Climate Change (IPCC) is considered as the main scientific authority regarding the climate issue (Hughes 2012). Administratively linked to the United Nations (UN), the organisation was created in 1988 in order to “provide governments at all levels with scientific information that they can use to develop climate policies. IPCC reports are also a key input into international climate change negotiations” (IPCC, n.d.). This organisation is the world’s primary source of what we know about the climate challenge. The IPCC Bureau, which guides the

* MRes student, International Relations.
organisation’s endeavours, is composed of thirty-four members, each from different countries. It avoids a skewed representation of either developed or developing ones.

Although the organisation has a central place in the climate debate, as explained by Hulme and Mahony, the IPCC is also criticised. As such, they explained that the “knowledge that is claimed by its producers to have universal authority is received and interpreted very differently in different political and cultural settings” (Hulme and Mahony 2010, 715). As of 2019, the IPCC has published five Assessment Reports (ARs). The latter are the organisation’s flagship documents addressing the climate issue. The latest report was released in 2014 (AR5) and the AR6 is due to arrive in 2022. It will notably address “the role of innovation and technology” (IPCC 2019) which is an important feature of the climate debate and will be discussed further in this paper. According to the AR5, uncertainty is defined as a

\[ \text{cognitive state of incomplete knowledge that results from a lack of information and/or from disagreement about what is known or even knowable. It has many sources ranging from quantifiable errors in the data to ambiguously defined concepts of terminology to uncertain projections of human behaviours.} \] (Kunreuther et al. 2014, 155).

These uncertainties are plural, they do not question the very existence of the crisis and the imperious need to be addressed. They rather lie in the scope of the impacts of climate change and its complex ramifications at all levels. It concerns, for instance, the lack of data to assess the impact of climate change on marine ecosystems (Payne et al. 2015), on food production (Lalic et al. 2018, 228) or even the uncertainties regarding the effects of the policies implemented to address the issue. (Buurman and Babovic 2016).

In the AR5, the authors linked the uncertainties inherent to the climate challenge with the notion of risk since making decisions whose outcomes are uncertain implies taking risks. Hence, it leads to different approaches in the elaboration of policy decisions. As explained in the AR5,
psychological research has documented the prevalence of affective processes in the intuitive assessment of risk, depicting them as essentially effort-free inputs that orient and motivate adaptive behaviour, especially under conditions of uncertainty that are informed and shaped by personal experience over time (Fincuane et al. 2000; Loewenstein et al. 2001; Peters et al. 2006 in Kunreuther et al. 2014, 166).

It means that these uncertainties gradually lead to the way to an emotional debate from which will stem normative and subjective policy decisions increasingly less informed by science.

This paper draws on a social constructionist conception of knowledge which *de facto* entails an acknowledgement of linguistic significations and language as both having “the quality of objectivity” (Berger and Luckmann 1966, 53). Indeed, through the recurrent assignment of language to specific understanding, it crystallises reality. Berger and Luckmann explain that the language has a “coercive” effect on us for we use it as “a facticity external to” ourselves (Berger and Luckmann 1966, 53). Consequently, pointing out the negative connotation of uncertainty is far from being anecdotical. The language used framed our perception of what is observed and we are stuck within these representations.

This is acknowledged by the AR5, which provides the guidelines for reporting uncertainties. The report states that IPCC’s authors should “be aware that the way in which a statement is framed will have an effect on how it is interpreted” and that “in some cases, it may be appropriate to describe findings for which evidence and understanding are overwhelming as statements of fact without using uncertainty qualifiers” (Mastrandrea et al. 2010, 2). The AR5 ultimately urges lead authors to “communicate uncertainty carefully, using calibrated language for key findings” (Mastrandrea et al. 2010, 4). The strategy seems to avoid the audience’s focus on these uncertainties in calibrating the language used accordingly (E.g., in the AR4: “Be aware that the way in which a statement is framed will have an effect on how it is interpreted. (A 10% chance of dying is interpreted more negatively than a 90% chance of surviving.) Use neutral language, avoid value laden statements” (IPCC 2005). However, it will be argued that trying to avoid these uncertainties that do not
question the very existence of the crisis is weakening the debate and fostering climate sceptics’ attacks.

Furthermore, this demonstrates that the interpretation of uncertainty is influenced by its terminology. As such, Corner et al. in The Uncertainty Handbook explain that “uncertainty has become an argument for discrediting and doubting climate science, and for delaying policy responses” (Corner et al. 2015, 3). This corroborates the previous discussion on the negative connotation of uncertainty in the discourses of several political leaders who instrumentalise climate uncertainties as it will now be discussed.

Negative uncertainties?

Indeed, some scholars demonstrated further how “perceived uncertainty” is “one of the most important factors” fuelling “climate change scepticism” (Corner, Whitmarsh and Xenias 2012, 465). In other words, climate uncertainties are among the primary means to constrain the emergence of a climate agenda. As such, President Trump’s interviews on climate change are insightful empirical materials to understand how this instrumentalisation is achieved. As the leader of the second largest country emitter of greenhouse gases (United States Environmental Protection Agency 2016) his scepticism resonates in the climate debate. In an interview on the 16th of October 2018 for the Associated Press, Donald Trump explained:

I am a person that believes very, very strongly in the environment. I am truly an environmentalist…. Some say that and some say differently. I mean, you have scientists on both sides of it…. I will say that you have scientists on both sides of the picture. (The Associated Press 2018)

In another interview on the 29th of October 2018, he had to comment on the fourth national climate assessment of his own administration which alerted the dangers of climate change for the US, he answered:

I believe it goes this way, and I believe, yes, men, meaning us people, men and women, to be politically correct, but – because everyone says men, but now we have to add women to that one, too. Men and women. We do have an impact. But, I don't
believe the impact is merely what some say, and other scientists that dispute those findings very strongly. (HBO 2018)

In both examples one can see how climate change is reduced, because of its uncertainties, to a belief. It henceforth entails that one can choose to believe it or not. While these uncertainties are increasingly explored from a social science perspective, there is still room for furthering the debate. Nieuwall et al. explained that “the knowledge base for defining the problem and possible solutions is insufficient and disputed: what exactly is the problem, and what specific action should be undertaken?” (Nieuwall et al. 2009, 7) Because of the negative connotation of uncertainties, much of the debate with climate sceptics and deniers has been focused on uncertainties as issues. The argument raised in the first section is, therefore, that instead of embracing the uncertainties of the climate challenge, the IPCC decided to avoid it as much as possible. In doing so, it strengthens the argument of climate sceptics who instrumentalise these uncertainties and demonise them. However, in order to efficiently deal with the threat of climate denialism, uncertainties should not be avoided but embraced and re-framed around its opportunities and implications. Uncertainties are not inherent to climate change but to science and there is no possibility of avoiding it.

New Technologies and Uncertainties

Indeed, there is no silver bullet to this uncertainty. Nevertheless, new technologies helped to manage uncertainties and to some extent, to decrease them. Yet, they cannot be avoided. Joseph et al., for instance demonstrated that uncertainty can be reduced in changing the uncertainty model regarding the hydrologic impacts of climate change (Joseph et al. 2018) but going beyond such achievement is hardly possible. Moreover, referring about uncertainty as a whole should be avoided insofar as “uncertainty can be generally categorised as either epistemic or aleatory” (Kundzewicz et al. 2018, 1). This means that one can act only on the former, which “is a consequence of a lack of knowledge, arising due to human ignorance and indolence. It can be reduced by gathering more data or by refining models” (ibid.).
Nonetheless, as it comes to aleatory uncertainties, which are “the intrinsic randomness of a phenomenon… there is no possibility of reducing it” (ibid.).

In the case of epistemic uncertainties, some important actions have been made and have been embodied by the Joint Programmes (JPs) of the European Energy Research Alliance (EERA). Those JPs are “technology-specific research partnerships” (European Commission 2012) addressing all scientific-related issues to climate uncertainties in order to increase human knowledge on those phenomena and, therefore, decrease epistemic uncertainties. The EERA Bioenergy JP is one of the 17 JPs and aims to “contribute to the decarbonisation of the energy sector… [and] to accelerate the implementation of biomass technologies in Europe” (European Commission 2014). Such initiatives are all deriving from the Strategic Energy Technology Plan (SET Plan) which is a framework that identified “ten actions for research and innovation” (European Commission 2014).

However, even if new technologies are addressing some issues, this paper argues that the problem is less uncertainties per se than the understanding and the framing of them. As such, Fischhoff and Davis recall that “all science has uncertainty. Unless that uncertainty is communicated effectively, decision makers may put too much or too little faith in it” (Fischhoff and Davis 2014, 13664). It is clear that, notwithstanding the progress made, since suppressing them will not be possible, the focus on uncertainties by climate deniers and sceptics is problematic and new technologies will not magically wipe them out. Furthermore, although Nordhaus acknowledged that we do not know “how damaging climate change will be for the economy as well as non-market and non-human systems”, still, “the bottom line here is that this most recent taking stock has more bad news than good news, and that the need for policies to slow climate change are more pressing and not less pressing” (Nordhaus 2016, 4). Consequently, bearing in mind the impossibility of completely avoiding these uncertainties and its instrumentalisation which fuels climate denialism, this paper argues for a new approach. In other words, shifting from a paradigmatic “uncertainty-as-an-issue” to “uncertainty-as-a-solution.”
Uncertainties-as-a-Solution

Technological change is not created *ex nihilo*, it is a social construct. The Social Construction of Technology theory (SCOT) has interesting insights with regard to the origins of technological change, opposing a determinist view of innovation. Technological determinism is “the common belief that technological change is inevitable and unambiguously represents progress” (Restivo and Croissant 2008, 219). The SCOT opposes this determinism considered as a myth. The theory emphasises on the links between social contexts and technological developments. Hence, it would seem irrelevant that the technologies developed to foster a global environmental change, mitigate the climate consequences and foster an adaptation to the contingencies of the natural disasters came *ex nihilo*. Opposing the determinist view of innovation, it means that technological change is not inevitable.

Indeed there is a machinery behind such innovations as demonstrated above with the EU’s EERA. Hence, it is the stance of this paper to argue that uncertainties inherent to climate change are also fostering innovations. These innovations arise more globally from a global new era embodied by the Anthropocene. The latter is defined by a “human-dominated geological epoch supplementing the Holocene” (Ehlers and Krafft 2006, 5). However since the finding was objectified through its terminology that made the Anthropocene a reality, scientific efforts have sought to address the environmental issues and uncertainties, at the core of the debate helped to foster “a new system of global environmental science” (Ehlers and Krafft, 2006, 8). In other words, from a social constructionist perspective, one could observe the phenomenon as such. First of all, the Anthropocene has been framed into a scientific finding and has become part of the common stock of knowledge and within that, the climate issue has gradually come into being as a priority and one of the greatest threats of this era. At the core of this threat, uncertainties have contributed to fuel the innovative thinking process required to rethink the way we were living or other aspects such as our energy consumption or production. This process is however constrained in its capacity in some realms in light of the negative framing of uncertainties which has led to their instrumentalisation for political purpose. Many scientists and governments have
tried to emphasise on a need to communicate differently and “carefully” on uncertainties such as the IPCC mentioned above. This is a laudable idea regarding how linguistic frames inform our perception of the reality. However, the approach is still avoiding uncertainties, considering them as a burden and this, one could argue, strengthens the vagueness and mistrust towards something that is, again, inherent to science. The claim is once again tightly linked to a concept developed by Berger and Luckmann which is the “detachment of knowledge” (Berger and Luckmann 1966, 104) in their book *The Social Construction of Reality*. The latter, being based on a phenomenological analysis, is not meant to serve as a ready-made conceptual framework but overall this paper’s call is based on the question of the detachment of knowledge addressed in the book.

They explained that “the scientific universe of meaning is capable of attaining a good deal of autonomy” (ibid.). Consequently, this paper calls for a new re-appropriation of uncertainties to release their innovative abilities and reduce their constraining properties human beings have themselves ascribe in its meaning and perception. Robert and Tapinos for instance unravelled that “firms seem willing to engage in risky innovation activity even where they face considerable environmental uncertainty” and more importantly that “firms’ probability of undertaking green innovating is positively related to both environmental uncertainty and the market-relative risks of innovation.” (Roper and Tapinos 2016, 361). A new thinking process, fuelled by uncertainties, is necessary in this era where re-inventing our whole production systems but also way of living are imperious.

**Conclusion**

To the question how new technologies are going to impact the climate governance, this paper sought to demonstrate that, if new technologies are going to help decreasing the level of uncertainties regarding the climate issue, it is unlikely that it will decrease the uncertainties completely. Furthermore, uncertainties as a threat is a social construct that is nurtured not only by climate sceptics such as Trump, but also to some extent by prominent organisations such as the IPCC, which tends to avoid it in carefully crafting their communication of it. It is suggested to shift the
understanding of climate uncertainties as a problem, to an understanding of it as a solution. Science informs policymakers and political leaders on how uncertainties are a problem and, therefore, impacts the way in which agents are informed of how to view uncertainties. Social sciences can foster a new understanding of uncertainties as a solution, it could differently inform policymakers and political leaders and it will inevitably affect the climate change governance.

Bibliography


HBO. “President Trump on Climate Change | AXIOS on HBO.” Youtube video, 2.02. Posted by ‘HBO,’ Nov 4, 2018. https://www.youtube.com/watch?v=UZq2L_49PBQ.


https://apnews.com/28928a1e43294af5b76177423fd44d03.

Huawei Ltd., the largest privately-owned company in the People’s Republic of China (PRC), has led globally in the telecommunications industry (Tao and Wu 2015, 1). With its relatively affordable price and quality gadgets, many customers choose its communications networks over its main competitor—Apple. Huawei has experienced rapid growth in the consumer electronics industry, including smartphones, laptops, and tablets (Sachs 2018).

Despite the company’s success as a product of China’s astounding growth, Huawei has been part of a political rivalry. The arrest and extradition of Huawei Chief Financial Officer (CFO) Meng Wanzhou by the Government of Canada in Vancouver, at the request of the United States Government, triggered grave diplomatic crisis between Chinese and the West (i.e. U.S., Canada). In light of the realist and liberal theories of international relations (IR), the Huawei phenomenon has become a subset of the broader Western policy debate over whether China’s rise should be contained.

This paper aims to contribute to the debate on the study of technology and its impact on global governance in the context of Huawei, and within the theoretical approaches that explain U.S.-China relations. In that sense, this paper addresses Sino-American relations in times of President Donald Trump and President Xi Jinping’s leadership. The selection of the controversy surrounding Huawei is reasoned for its relevance for its significant news coverage and public attention within the broader context of the bilateral relations between the U.S. and China (Paulson 2018, 3). Thus, this case regarding technology and governance provides a microcosm of the evolution of the most consequential bilateral relations. The

* MLitt student, Legal and Constitutional Studies (School of History).
former—an established power, and the latter—an economic colossus and rising power will define the future course of IR.

The findings indicate that Sino-American relations have been complicated by technology—from 5G networks to artificial intelligence (AI). This paper argues that realist theories can better explain the U.S. perception and response to China’s policy in terms of competition between the major powers. The Huawei dispute has magnified the existing trade war between the two global superpowers. This conflict is caused not only by the ongoing disagreement between Washington and Beijing, but more importantly by both leaders’ assertiveness in the importance of technological advancement. The case Huawei provides a microcosm of increasing mismatch of the balance of power between the status quo and rising power. In the long run, there will be foreseeable effect on the global economy, but whether the world would disintegrate into two blocs politically remains unclear.

This paper is structured into four sections. The following one explores the theoretical frameworks that explain Sino-American relations. The second section outlines the issue of the trade war, technological warfare, and Huawei crisis. The third section presents the findings regarding Huawei’s role in the Sino-American discourse with regards to technology and global governance. The final section provides a conclusion and discusses its implications for IR.

**Theories of IR and U.S.-China Relations**

The emergence of China as a great power, and its implications for both IR as an academic discipline and IR in practice, especially its relationship with the United States is one of the most pressing issues in global politics. Scholars have discussed different scenarios regarding Sino-American relations. The following three are widely evaluated among them, in which these theories are not mutually exclusive:
Thucydides’ Trap/Offensive Realism

Realist theorists (e.g. Waltz 1959; Mearsheimer 2001; Walt 1998) argue states pursue power because they are trapped in an iron cage where they have no option but to compete with each other for power to ensure their own survival. Realism depicts states as operating in a nasty and brutish Hobbesian world that prompts them to vie for power and influence at the expense of other nations (Walt 1998, 29). In that sense, a revisionist state (China), will ultimately confront the status quo state (U.S.).

In the pessimist view, the rise of China is likely to or will cause inevitable instability and conflict. Thucydides’ Trap refers to the idea that when a rising power threatens to displace a ruling one, the most likely outcome is war. Accordingly, the message of the Peloponnesian War warns of the most perilous trap into which today’s great powers will; inevitably fall—an unnecessary war. Furthermore, in Allison’s (2017, 384) case study, he identified 12 out of 16 cases in the past five hundred years in which rival power challenged an existing power, the end result was war.

Mearsheimer (2001, 22-23) derived a theory famously known as “offensive realism”. The five assumptions outlined by Mearsheimer’s realism and China’s rise include (1) states operate in an anarchic global system (2) states possess some offensive capability, (3) states’ intentions are unknowable, (4) Survival is the most important goal, and (5) state are rational actors. He asserted that China’s rise is or never will be peaceful. Rather, it will become “an aggressive state determined to achieve regional hegemony.” (Mearsheimer 2001, 29-40). The conflicts become more likely depending on how the U.S. will respond—launching a preventive war or slowing down China’s economic growth.

Cold War 2.0

The difficulty for the two states to reach a modus vivendi is likely to pave the path of a second Cold War. Former U.S. Treasury Secretary Hank Paulson warned that if the U.S. and China fail to resolve their strategic differences, an “iron curtain” is likely to descend on the world. As such, both states are implementing policies that could
forcibly disintegrate bilateral relations, starting with the technology transfer blockade (Paulson 2018, 3). Mutual distrust and confrontation resemble a new “Red Scare” during the Cold War between the U.S. and former USSR (Trivedi 2019). The Chinese military, technological level achieved in a short time, the branded economic system known as “socialism with Chinese characteristics,” coupled with global projects like the Belt and Road Initiative (BRI) are considered to be contrary to the U.S. interests. Mattis and Schrader (2019) argued that China cannot ensure the continuity of liberal order because of different civilizations phenomena based on Samuel Huntington’s clash of civilization. The U.S. sees China as a competitor who establishes a different system—Beijing Consensus that share antagonistic values to the Washington Consensus (Ramos 2004, 1).

Neoliberalism/Cooperative Rivalry

The central issues that neo-liberalism address are the difficulties of achieving peace and cooperation in international relations, and the methods that can contribute to that achievement. Increasing globalization, the rapid rise in communication technology, and increasing international trade imply that states no longer rely on simple power politics but complex interdependence (Keohane 1970). Liberal theorists (e.g. Ikenberry 2008) assert China’s rise occurs in an open, integrated, and rule-based world order. Today’s Western order is difficult to overturn and easy to join, which allows the accommodation of a rising power. Nye (2018, 6) suggests today’s Sino-American bilateral relations as “cooperative rivalry.” He rejects offensive realism that an outbreak of war between the superpowers is destined. Both China and the U.S. both face challenges that require cooperation, including climate change, infectious diseases, and terrorism. Despite the two states have significant disagreements over trade and policy, but interactions create win-win situations. Therefore, the accommodation of rising power is welcomed, but depending on whether the U.S. is able to come in terms of a “cooperative rival.”
Trade War, Technological Warfare and Huawei Ban

The initiation of the trade war can be seen largely as a rejection of cooperative rivalry and a return to offensive realism. The main reasons that the U.S. has waged a trade war against China are two: its accusation that China is an unfair trader, and an attempt to contain China’s rise (White House 2017, 45). These “unfair trade practices” have been widely blamed for the significant U.S. trade deficit with China, which accounted for $345.6 billion in 2019 (Office of the United States Trade Representative, 2019). In light of offensive realism, U.S. perceives China as a threat to the “America First” principle (White House 2017, 23). In return, China responded vigorously to the U. S.’s criticism. In People’s Daily, the official media of the Communist Party of China, Beijing retorted that the primary motivation of the U.S waging an unnecessary trade war is to contain China’s quest for hegemony (Ren 2018).

Huawei is caught in a tug of war between its role as China’s representation of rapid expansion and modernization of telecommunications network, and Western concerns regarding the security implications of its equipment in national telecommunication system (Ahrens 2013, 9). Currently, Huawei operates in 170 countries/regions and employs roughly 188,000 people globally. According to the company, nearly half of the world’s population uses a telecommunications network supported by Huawei equipment or technology. (Huawei 2017). As a global leader in the industry, Huawei is competing to provide 5G wireless networks with its rivals (Sachs 2018). However, the U.S. has treated this company as a threat to national security since 2012, arguing that the Chinese government uses it as an espionage platform (Morell and Kris 2018). In U.S. Defence Authorization Act passed in August 2018, Huawei equipment is blocked in government networks and market, as the company threatens the integrity of American communications technology and national security (Salinas 2018).

On 1 December 2018, Huawei’s CFO Meng Wanzhou was detained by Canadian authorities in Vancouver International Airport at the request of the U.S. government for the charges of circumventing American sanctions imposed on Iran, conspiring to

The trade war, coupled with Huawei’s controversy, unleashed a new era of technology war between the superpowers. The U.S. has directed numerous attacks that resemble the “Red Scare,” and China has retaliated in multiple fronts. On one hand, the U.S. government seeks the cooperation of its allies to ban Huawei. Many U.S. allies, including Japan, Australia, and New Zealand, have curtailed Huawei’s operations domestically (Morell and Kris 2018). In addition to Huawei, many Chinese companies have been added to the Entity List that bans them from buying U.S. components without the government’s approval. Most of the companies on this list are high-tech such as electronics, aviation, engineering, and IT (Office of Public Affairs 2019, 10-16). Xinhua (2019) reported on 8 June 2019, that China’s National Development and Reform Commission would establish a national technological security management list system, with the aim of more effectively taking preemptive measures against national security risks. While these “weapons” enhance China’s bargaining power when negotiating with the U.S., they are also sources of friction between the superpowers. This intricacy has significantly upset the fundamental strategic partnership between them.

Sino-American Relations, Technology, and Global Governance

The foreign policy guidelines of U.S. and China have not changed radically, but there are certainly shifts in philosophy and policy under President Trump. The conflict is caused not only by the ongoing disagreement between Washington and Beijing, but more importantly by both Trump and Xi’s assertiveness in the importance of technological advancement as a weapon in the quest for hegemony. While Xi’s administration seeks to realize the “China Dream” and the revival of “great renaissance of the Chinese nation” (People’s Daily 2019) the formulation of Trump’s election promise “Make America great again” by applying the “America First” ultra-nationalist principle shares similar goals. The U.S. has moved from
“liberal hegemony” for nearly 30 years to confrontation measures to ensure economic growth and national security.

The “Made in China 2025” plan was announced in 2015 by Premier Li Keqiang and his Cabinet (Li 2018, 1). Essentially, it is a blueprint for the development of the manufacturing industry for the Chinese government, with a strong emphasis on Chinese leadership in information technology. In that sense, China does not hide the fact that it is seeking global market leadership in a wide range of advanced technologies, including the 5G network (Kennedy 2015, 1).

It is no surprise that the U.S. remains vigilant towards China’s pursuit of technological leadership. Trump fulfilled his election pledge by issuing a memorandum directing the Office of the United States Trade Representative (USTR) to investigate China’s actions, policies, and practices concerning technology transfer, intellectual property, and innovation under Section 301 of the Trade Act in August 2017 (USTR 2019). The report on the investigation, released on 22 March 2018, heavily criticized the technology transfer rather than trade imbalance (Office of the United States Trade Representative 2018a, 2018b).

The trade war signifies that the U.S. has shifted its foreign policy towards China from increased partnership to increased rivalry, meaning restricted flows of trade and investment, human capital, and technology. According to the White House, technology transfer has become a crucial policy for the U.S. to deter the rise of China (White House 2017, 4). By strengthening its national security (cybersecurity) system, imported technology from the U.S. to China has become more difficult. In addition, the tightening restrictions on U.S. companies to perform business transactions with technological companies in China, notably Huawei 5G has brought the trade war into an overt technology war (Sachs 2018).

According to the theory of offensive realism, the U.S. perceives China’s rise as a threat to its existing political hegemony (Mearsheimer 2001, 401), the Trump Administration has imposed additional tariffs on imported Chinese goods and
tightened restrictions on technological transfers and business operations, notably Huawei (Office of the United States Trade Representative 2018a, 1, 32). Trump has also banned companies that are “threats to national security and foreign policy interest,” thus blocking trading with Chinese telecommunication magnates like Huawei (Office of the United States Trade Representative 2018b, 7). In return, Chinese officials have condemned that such national security concerns are unduly exaggerated and fabricated, lacking concrete evidence, and denying of China’s pursuit of economic development (Ren 2018).

The conflict presents a lose-lose situation for all. With the flows of capital, goods, technology, people, and information between them tightly regulated, transnational cooperation can no longer optimize allocation of resources by investing globally, and supply chains would have to be reshaped to adapt to this new environment. A prolonged trade war depresses both states’ economic growth rate. Consequently, transnational companies relocate their business operations out of China to Southeast Asia to avoid the additional costs of raising tariffs. Moreover, the U.S. government has tightened restrictions on acquisitions of U.S. technological companies by Chinese companies, which decelerates China’s productivity growth. As a result, China can no longer use its comparative advantage in exporting intermediate goods and contributing to global supply chains. With strict business restrictions, American companies are forced to move from China to other countries. As a result, the U.S. would not only lose its market share in China but would also have to import from more expensive sources.

The negative impacts on global trade and investment, as well as economic growth, far exceed that of the Brexit. More alarmingly, this can lead to dividing the global economy into two major blocs lead by China and the U.S. respectively. Some experts warn that tensions between Washington and Beijing over technology could lead to a “digital iron curtain,” which would result in governments having to decide between doing business with the U.S. or China (Champion 2019). With the intensification of economic competition, a Cold War 2.0 is likely to occur in a bipolar world.
Conclusion

The trade war has made Sino-American relations confrontational rather than cooperative. Huawei serves as an allegory in the broad context of the Sino-American rivalry, escalating the trade war into a technological war. The technological company has generated a greater issue arising from the trade war, which has heightened the existing conflict between the great powers. The controversy of Chinese firms competing for market share in technological dominance and using it as a weapon for (cyber) espionage poses challenges to global governance, as it hurts the two largest economies in the world, and consequently to the most important bilateral relations and their allies. With its increasing importance, the question of technology competition among great powers will continue to generate debate in years to come.

Bibliography


Office of the United States Trade Representative. 2018b. Findings of the investigation into China’s acts, policies, and practices related to technology transfer, intellectual property, and innovation under Section 301 of the Trade Act of 1974. March 22. https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.


Anonymous internet usage is a troublesome practice, especially for liberal states that place impetus on technological progression and personal freedoms whilst wanting to maintain a degree of surveillance on their population. Toeing the fine line between exercising the fundamental principles of a liberal democracy, including freedom of speech and the right to privacy, and maintaining a degree of societal surveillance, is thus a difficult task (Denardis 2014, 224). As governments globally are falling into what can be seen as a security dilemma of digital surveillance, there has never been a more appropriate time to consider what this means for global societies (Denardis 2014, 225).

Thus, this paper sets out to investigate the interaction between domestic political freedoms and anonymous internet usage within a state, through which I aim to test the following hypothesis:

\[ H1: \text{The lower the level of domestic political rights, the higher the level of anonymous Internet usage.} \]

This paper will conduct quantitative analysis built on a computational model incorporating various datasets. To preface this work, with a very limited (n) due to the Tor Project only publishing the ‘Top-10’ countries per bridge and relay access, I do not attempt to prove causation. What this paper seeks to do is investigate if there is any relationship between domestic political freedoms and Tor usage, and is not attempting to prove indefinite causation, largely because of limited bandwidth and access to data. This paper, rather, is an example of explorative methodology.

* 4th year undergraduate student, International Relations.
The hypothesis of this paper is that there is a negative correlation between domestic political freedoms and Tor usage, and to test this hypothesis I will use quantitative analysis using R. My hypothesis rests upon the assumption that individuals within states that constrain political freedoms are more likely to engage in activity that grants them greater autonomy, relatively emancipated from the prying eyes and forceful censorship of their government.

Anonymous internet usage within this paper shall be investigated in terms of the access one seeks to the Tor browser. The Tor browser (The Onion Router) offers anonymity to those who use it for internet browsing, and its mechanisms shall be later explained in this paper. Causes for concern surrounding Tor usage vary state by state, and the reasons for using Tor vary widely (Jardine 2015, 2). The Tor browser is the technology through which one can access the Dark Web, engage in untraceable (thus potentially illegal) activity and operate in an almost supra-state condition of untouchability (Macrina 2015, 17). Alternatively, it may be accessed by activist organisations wanting to leak information (WikiLeaks was a Dark Web enterprise), and grant citizens of oppressive regimes greater individual and political autonomy.

This paper is to offer insight into how the use of the Tor network interacts with global domestic governance structures by delineating how it operates, and what it can be used for- in such exploring what it means to have anonymity online (Choucri 2016, 57). As is noted on the Tor Project website, “While it is thrilling to speculate about undesired effects of Tor, when it succeeds, nobody notices.” (Tor Project 2020) This paper seeks to defend the over-simplification that the use of the Tor browser is necessarily nefarious and naturally conducive to illegal activity through the proliferation of the Dark Web. By mapping domestic political freedoms against Tor usage, I wish to gain some insight into whether there is any validity in my hypothesis, through such hoping to draw attention to the importance of Tor in states with limited political freedoms. What I wish to consider, too, is if other factors may play a role in increasing anonymous internet usage. Whilst the scope of this paper allows only a quantitative analysis of the interplay between domestic political
freedoms and anonymous internet usage, I shall speculate where appropriate on other factors that may play a role in encouraging Tor use.

As a caveat, this thesis does not attempt to argue that there is no illegal activity conducted on the Tor browser, nor that the technology is not exploited by those wishing to engage in crime. However, this thesis is a small nod to the importance of anonymity for political liberty. This thesis aims to avoid the arguably ‘easy’ condemnation of anonymous internet usage and argue on the contrary that where there is less political freedom, there is higher Tor usage for reasons that this thesis shall attempt to investigate.

The Tor Browser: What Is It?

The Tor Project, that operates the Tor browser, is a non-profit organisation that exists to facilitate online anonymity. Their product effectively allows one to surf the internet unabetted by governmental restriction or fear of being tracked by existing surveillance programmes. It works by destroying the direct connection between a device and a server that hosts online material. By establishing a three-node circuit between a device and a server which re-encrypts all data at each stage, the Tor network uses Onion routing, thus routing with many layers, to circumvent any direct connection between a user’s device and a server (Tor Project 2020). The network through which Tor redirects traffic is free, global, and voluntary, and consists of more than 7,000 relays to conceal information about users. This means that it is incredibly difficult to decipher any information about a user, including their name, IP address, home address, search history, etc.- which is oft easy to deduce from conventional internet usage.

The Tor Project does not condone nor encourage accessing the Dark Web despite it being the most common means through which one can access it. Very briefly, the Dark Web comprises sites called hidden services, which are web services hosted off the ‘normal’ Internet, that have their IP address masked. These sites are identifiable by ‘.onion’ being appended onto the URL, and one must already know the URL of the site that they wish to access due to the Dark Web being non-indexed, suggesting
that it is highly unlikely that one would ‘stumble upon’ Dark Web sites, and those that access it intended to do so. Indeed, there is illicit activity on the Dark Web and this activity, from people and narcotics trafficking and beyond, goes to a large extent in countering personal liberties. However, this paper lacks the bandwidth to elaborate further on this topic but saw it to be crucial to acknowledge this argument.

The Tor Project (2020) instead presupposes that its network may be used to:

- Protect user privacy from unscrupulous marketers and identity thieves.
- Protect user communications from irresponsible corporations.
- Protect one’s children online.
- Research sensitive topics.
- Skirt surveillance.
- Circumvent censorship under domestic Internet laws.

Tor can be leveraged for good, with the anonymity that it grants allowing activities such as confidential communication between activist organisations and individuals of politically oppressive regimes seeking to avoid the vigilant surveillance and censorship of governments (Jardine 2015, 2-6). Herein lies the dilemma: anonymity is a cornerstone of both democracy and villainous activity. Roger Dingledine, an original developer of the Tor browser, argued that “there are important uses for hidden services, such as when human rights activists use them to access Facebook or to blog anonymously,” and that “these uses for hidden services are new and have great potential.” (Chertoff 2017, 26) Thus, whilst I acknowledge that there are those that misuse Tor for illicit activity, I shall instead be focusing on the positive impact that it has on domestic political freedoms, hypothesising that indeed anonymous internet usage does increase where domestic freedoms decrease.

**Study, Methodology and Findings**

I refer again to the hypothesis put forth in the introduction to this paper as I begin the quantitative analysis:
**H1: The lower the level of domestic political rights, the higher the level of anonymous Internet usage.**

**Method**

The model used in this paper is linear regression as robust bivariate and multivariate models can be used to display the interplay between dependent, independent and control variables. This study regresses data on domestic political freedoms as provided by Freedom House in their 2019 report with average daily Tor users as provided by the Tor Project website (Freedom House 2019a, 5). This analysis intends to represent a survey through which the relevant (n) sample size is as representative of (N) as the general population as possible. To counter in a small manner the causation-correlation difficulties herewith, I opt to hold nominal GDP per capita ($) and obstacles to internet access per country constant. I shall reiterate throughout this paper that this methodology is explorative. The sample size (n) used is extremely small, yet this research paper provides an interesting insight into a sparsely researched relationship. The consequences of a small (n) sample size will be delineated later in this section.

I regress both the number of Tor users that use relay and bridge access with domestic political freedoms. The data provided by the Tor Project is of the Top-10 countries by raw (n) access, scaled per number of Internet users in each country. The key difference between relay access and bridge access is as follows: Relay access can effectively be blocked, insofar as users can be blocked from entering and exiting Tor (Tor Project 2020). To block users coming out of Tor, a downloadable list of Tor exit nodes can be used to block any traffic from these nodes. To block users from entering Tor, every site would be blocked, by downloading the comprehensive list of guard relays and, again, blocking any traffic through these relays. Bridges are a solution to this problem. Bridges are effectively just unpublished entry relays. The Tor Project publishes a very small list of bridge relays through which a user can access the Tor network, as they should only need a small number of relays and keeps the rest a closely guarded secret. It is possible to locate bridges, through users that could leak the bridge address and possibly utilising fast port scanners such as
ZMap, however bridges do offer a reasonably efficacious solution to the barriers to entry problem within relay access (Tor Project 2020). Thus, to simplify the matter, relay access is more likely in states where a government is less likely to attempt to block anonymous internet usage, and bridge access is more likely in states that would attempt to block anonymous internet usage. Hence, it is important to analyse both bridge and relay access.

Linear regression presupposes normality, or the condition within which the error term is normally distributed. When this isn’t present, the data presents heteroscedasticity. To counter such, I have used robust regression to downweigh outliers and offer a better fit model. The use of robust regression within this paper, and robust standard error, is common practice within linear regression analysis, and is why I feel it was appropriate to use in this paper. To conduct the quantitative analysis within this paper I used R 3.6.3. The process that I took was as follows: I first collated the data required into .xlsx files to be imported into R. Once I had imported the relevant libraries and datasets, I plotted the Cooks Distance and QQ plots. This is because with such a small sample (n), it was necessary to downweigh outliers to prevent large skews in the data. The QQ plots included below exemplify why this was significant, as minimal outliers could have severe impacts upon the veracity of the statistical significance of the model.

I then conducted a simple OLS regression analysis to compute the Cooks distance and build the relevant data frame for analysis. I was then able to generate the standardised residuals within the sample, sort in order of standardised residuals, and conduct Huber and BiSquare weightings to deduce which robust analysis was the most relevant for this study. This was done both with and without the control variables incorporated within the model. All source code is listed in the Appendix.

**Data Selection**

*Dependent Variable*

As has been discussed in detail above, the data regarding mean daily Tor usage was taken from the Tor Project website for users of both bridge and relay access (Tor
Project 2020). The Tor Project lists only \( n = 10 \) of the countries of both bridge and relay access.

**Independent Variable**

This study has harvested the cumulative scores of Freedom House’s *Freedom in the World* report (2019a, 4). The Freedom House score is calculated as an aggregation of their collected data on: Electoral Process subcategory, Political Pluralism and Participation subcategory, Functioning of Government subcategory, Political Rights category, Freedom of Expression and Belief subcategory, Associational and Organisational Rights subcategory, Rule of Law subcategory, Personal Autonomy and Individual Rights subcategory, Civil Liberties category. It was this cumulative score that was used to represent ‘domestic political freedom’ that acted as an independent variable, which is listed in the regression tables as ‘Freedom House Score’.

**Control Variables**

The control variables were nominal GDP per capita (\( \$ \)) and obstacles to internet access. The 2019 nominal GDP per capita of each state within this study was taken from the IMF website (International Monetary Fund 2019). Furthermore, the obstacles to internet access variable included as a second constant was drawn again from the Freedom House *Freedom on the Net* report (2019b, 5). This encompasses ‘infrastructural and economic barriers to access, legal and ownership control over internet service providers, and independence of regulatory bodies’ (Freedom House 2019b, 8). These constants were selected in order to offer some solution to the causation-correlation debate that higher wealth is immediately indicative of a higher level of Tor usage due to access to more technology. Surveys exist that depict a strong positive correlation between high GDP and high amount of internet access, meaning that controlling for this variable was a crucial (Poushter et al. 2018). The obstacles to internet access data operates in a similar vein, and allowed me to control for a plethora of explanatory factors that may have played a significant role in the outcome of the model.
Problems and Limitations

The most notable limitation is the extremely small ($n$) due to the limited amount of data available from the Tor Project, wherein they only provide data on the top-10 countries by bridge and relay access. I wish to emphasise that I am not attempting to prove overall causation as there is insufficient data to achieve such. Rather, I aim to seek to understand the interplay between domestic political rights and daily Tor usage more comprehensively and be explorative in my methodological approach. Bandwidth meant that there was limited capacity to consider other control variables and to build a more efficacious model. Furthermore, the regression tables within this paper display very high standard error and regression coefficients, and this can be caused by either poor explanatory variables or a small sample size. I would argue that, in the case of this study, the latter is the most appropriate explanation, as when the robust analysis was conducted there was statistical significance drawn from variables within the model.

Findings

The following section shall delineate the findings of the model built. The basic OLS linear regression analysis is represented on a scatterplot graph to show the regression line between the level of domestic political freedoms and mean daily Tor usage per relay and bridge access. Both plots exemplify some degree of covariance between the two variables, and the QQ plots featured are useful indicators as to why I chose to conduct robust regression analysis to give less weight to outliers. Important to note however is that these scatterplots are based on domestic political freedoms not isolated from other variables.
Table 1. OLS Linear Regression between Mean Daily Relay Tor Users and Domestic Political Freedoms.

![Top-10 Countries by Relay-Users](chart1.png)

Table 2. Normal Q-Q Plot showing the spread of outliers within the sample used from Cooks Distribution to explain the use of weighted distribution and BiSquare Regression.

![Normal Q-Q Plot](chart2.png)
Dependent Variable: Daily Tor usage - Relay access (2019)

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom House Score</td>
<td>1330.6882**</td>
<td>-4886.9981**</td>
</tr>
<tr>
<td></td>
<td>(-242.8876)</td>
<td>(1351.7106)</td>
</tr>
<tr>
<td>Obstacles to Access</td>
<td></td>
<td>12368.3408*</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(7685.2755)</td>
</tr>
<tr>
<td>Nominal GDP ($)</td>
<td></td>
<td>15.4113***</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(3.2684)</td>
</tr>
<tr>
<td>(Constant)</td>
<td>292326.0006***</td>
<td>222789.3341**</td>
</tr>
<tr>
<td></td>
<td>(108880.8738)</td>
<td>(85915.6451)</td>
</tr>
<tr>
<td>Robust Std.error</td>
<td>88380 on 8 DF</td>
<td>38650 on 6 DF</td>
</tr>
<tr>
<td>R²</td>
<td>-0.1751</td>
<td>-0.810</td>
</tr>
<tr>
<td>Adjusted R²</td>
<td>-0.07197</td>
<td>-0.301</td>
</tr>
</tbody>
</table>

Figures are coefficients with t-value in parentheses. Significance: *** p < 0.01; ** p < 0.05; * p < 0.10.

**Analysis**

The mean daily relay access to Tor, or in other words access that is less likely to be stopped by a government, has a statistically significant relationship with the level of domestic political freedom in the states analysed in this paper, shown by the P Value of P < 0.05, suggesting that I can reject the null hypothesis that there is no statistical significance. Russia and the United States proved to be outliers to this observation, possibly because Russia is somewhat lagging in its fight against Tor, highlighted by the Russian Government offering financial remuneration to those who can help their efforts against anonymous internet browsing. I would hypothesise that the United States being an outlier may be linked to factors outside of this model, such as a more robust technological education climate, which could be investigated further through a state-by-state analysis – for example, does California have higher levels of Tor access than Alabama. The initial R² proved to be lacking in statistical significance, though when the control variables were added, the statistical significance increased. Again, the exceptionally high standard error and correlation co-efficient are highly likely due to the very small sample size.
Thus, this short analysis concludes that a statistically significant relationship can possibly be drawn, defending H1, and that it can be argued that there is a negative linear relationship between relay access to the Tor browser and domestic political freedoms. Indeed, many of the states within (n) sample have high levels of political freedom, namely the UK, France, Germany and the Netherlands. Thus, it may be difficult to discern why they would need to use Tor at all. I would argue that this is why individuals within these states are more likely to use relay access, for there is less real concern about anonymous internet usage being blocked or domestic political rights, with a background climate of technological progression and individual liberty– an inference to some extent reinforced by the high degree of statistical significance of nominal GDP per capita to this model.

Table 3. OLS Linear Regression between Mean Daily Bridge access Tor Users and Domestic Political Freedoms.
Table 4. Normal Q-Q Plot showing the spread of outliers within the sample used from Cooks Distribution to explain the use of weighted distribution and BiSquare Regression.

![Normal Q-Q Plot](image)

<table>
<thead>
<tr>
<th>Dependent Variable: Daily Tor usage – Bridge access (2019)</th>
<th>(1)</th>
<th>(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Freedom House Score</td>
<td>-2.6861*</td>
<td>-6.9239*</td>
</tr>
<tr>
<td></td>
<td>(-13.8896)</td>
<td>(-24.0926)</td>
</tr>
<tr>
<td>Obstacles to Access</td>
<td>82.6752</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(152.2195)</td>
<td></td>
</tr>
<tr>
<td>Nominal GDP ($)</td>
<td>0.1029*</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(0.0663)</td>
<td></td>
</tr>
<tr>
<td>(Constant)</td>
<td>1977.5761**</td>
<td>768.0108</td>
</tr>
<tr>
<td></td>
<td>(847.1608)</td>
<td>(1419.6080)</td>
</tr>
<tr>
<td>Robust Std.error</td>
<td>11840 on 6 DF</td>
<td>1162 on 6 DF</td>
</tr>
<tr>
<td>R²</td>
<td>-0.248</td>
<td>-0.46</td>
</tr>
<tr>
<td>Adjusted R²</td>
<td>-0.128</td>
<td>-0.4278</td>
</tr>
</tbody>
</table>

Figures are coefficients with t-value in parentheses. Significance: *** p < 0.01; ** p < 0.05; * p < 0.10.
Analysis

As was hypothesised, the states that saw higher levels of bridge access are those with more oppressive political regimes, with examples of observations within (n) being Belarus, Indonesia, Iran and Turkey. The $R^2$ of the model displays a lower coefficient of determination that the relationship existing between relay access and domestic political freedoms. The linear relationship between domestic political freedoms and daily Tor usage through bridge access did represent minor statistical significance, which remained when the control variables were added to the model, though the explanatory power of the model is lower. The most interesting insight is that there is a degree of statistical significance existing between nominal GDP per capita and daily Tor bridge access, despite Iran being downweighted as an outlier. Perhaps, this statistical significance can be attributed to the fact that there are many countries that have coinciding high national wealth, such as China and Russia, yet low domestic political freedoms.

I would suggest that bridge access tells a far more complex story than that of relay access because it is either A. a novelty technology for those in wealthy countries with less oppressive regimes, that are less concerned about government surveillance (UK, Germany) or B. A near necessity for those who wish to use the internet unabated by government surveillance – and this paper doesn’t have the bandwidth to deduce which is a more reasonable hypothesis to draw. The lower explanatory value within the bridge access model, I suggest, is because there is friction between the variables and (n) observations within the model. China and Russia, as has been mentioned, are wealthy but oppressive. Belarus, Iran and Turkey, are less wealthy, whilst also oppressive. The United States, Germany and the UK, are wealthy and not relatively politically oppressive. Thus, I am extremely hesitant to draw an overarching deduction from this model and suggest that more research is done on what influences the use of bridge access to the Tor browser in lieu of relay access- most notably for the sample states with a higher nominal GDP.
Conclusion

Domestic governments must grapple with the weight that they award to rights and freedoms when attempting to tackle the use of the Tor network. Attempting to block the Tor network has clearly not been successful, and for citizens to seek to utilise networks such as Tor can be indicative of deeper systemic issues that this thesis lacks the bandwidth to investigate.

This paper has sought to draw attention to a possible interplay between domestic political freedoms and anonymous internet usage through calling upon existing empirical evidence and formulating a short computational study to reify such. Whilst indeed I have reiterated the small sample size and thus avoidance of concluding on any overall causation, I feel that this small project offers some insight into the interaction between the use of the Tor browser and domestic political rights. Indeed, many of the observations within the relay access (n) provided by the Tor Project are not politically oppressive regimes, and Tor may be deemed to be a novelty enterprise, a new technology, a guarantor that one can surf free from government surveillance. However, this is clearly not always the case. For some, Tor provides a way to move through the looking glass to a cyberspace not traced by an oppressive government, nor marred by censorship. Whilst I want to avoid the generalisation that Tor is universally used for positive purposes, it can emancipate those that exist in states with limited political freedoms.

This paper concludes anecdotally with a case from 2014. Turkish Prime Minister (and now President) Recep Erdoğan and some fellow ministers were photographed engaging in corruption and bribery; soon after the circulation of those photographs, Erdoğan utilised his authority to force the passing of a court order that demanded that the central telecommunications provider ban the use of Twitter across Turkey. This was, however, too little too late: a handful of Turkish citizens had already circulated the images across the Tor network, and “traffic from Turkey was 55,000-more than double the number of users from Turkey before the ban was instituted” (Chakraborty 2018, 20). The Tor browser saw its growth from 10,000 new Turkish users per week, to 10,000 per day. Tor effectively allowed for a circumvention of an
undemocratic violation of political liberty - and herein lies the dilemma: anonymity is a cornerstone of both democracy and illegal activity.

Bibliography


Appendix A: Source Code for Relay Access Robust Regression Model

```r
1
2 install.packages("MASS")
3 install.packages("car")
4 require(MASS)
5 require(car)
6
7 data(USArrests)
8 attach(USArrests)
9 summary(USArrests)
10
11 x <- as.data.frame(USArrests)
12 x <- x[, names(x) != "Murder"]
13
14 model <- lm(Murder ~ ., data = x)
15 summary(model)

The Tor Project, Inc. 2020. Tor Project: Bridges.
Appendix B: Source Code for Bridge Access Robust Regression Model

```r
install.packages("MASS")
install.packages("foreign")
require(MASS)
require(foreign)
Rickey_RA_DATA <- read.xlsx("C:\\Users\\Farrah\\Documents\\CCG\\Bridge Users_ROBUSTREG.xlsx")
attnick(Bridge_users_ROBUSTREG)
summary(Bridge_users_ROBUSTREG)
#plot cooks distance and check for outliers
plot(cooks.distance(mean_daily_users ~ freedom_house_score + obstacles_to_access_per_FM + nominal_GDP, data=Bridge_users_ROBUSTREG))
qqnorm(mean_daily_users); qline(mean_daily_users)
summary(ols <- lm(mean_daily_users ~ freedom_house_score + obstacles_to_access_per_FM + nominal_GDP, data=Bridge_users_ROBUSTREG))
#compute cooks distance
dist <- cooks.distance(ols)
dist <- data.frame(dist)
#generate standardized residuals
s <- stdres(ols)
a <- cbind(Bridge_users_ROBUSTREG, dist, s)
#sort in order of standardized residuals
sabs <- abs(s)
a <- cbind(Bridge_users_ROBUSTREG, dist, s, sabs)
assorted1 <- a[order(sabs),]
assorted1[1:n,]
#sort the Huber weightings

summary(rr.huber <- rlm(mean_daily_users ~ freedom_house_score + obstacles_to_access_per_FM + nominal_GDP, data=Bridge_users_ROBUSTREG))

huber <- data.frame(mean_daily_users = BRIDGE_USERS_RA_DATA$mean_daily_users, resid = rr.huber$residuals, weight = rr.huber$weights)

huber[1:10,]
#square weighting too

rr.bisquare <- rlm(mean_daily_users ~ freedom_house_score + obstacles_to_access_per_FM + nominal_GDP, data=Bridge_users_ROBUSTREG, psi = psi.bisquare)

summary(rr.bisquare)
```