Modern International Responsibility to Protect: A Study of the Cyber International Responsibility to Protect – A Case Study of Iran

By

Paniz Bahmani

Submitted to

Central European University
Department of International Relations
In partial fulfilment of the requirements for the degree of Masters of Arts

Supervisor: Professor Michael Merlingen

Vienna, Austria
2023

Abstract

The principle of R2P has been much debated amongst scholars. Nevertheless, there are aspects to it that have been somehow isolated. The link between cyberspace and R2P is one of those issues, although some attention has been rising towards it in the recent years. In this thesis, I will be studying the role of cyberspace in the implementation of R2P. The focus would be on how R2P is implemented through cyberspace. I will be studying different methods of cyber R2P and their targets, depending on their functions. Drawing from these arguments, I shall be making my argument that providing internet could be considered a case of R2P, as the aforementioned methods of cyber R2P are all based on the hypothesis that the population has access to global internet. At the end, I merge the arguments with the facts from the ongoing situation in Iran, and conclude that in the discussed manners, providing safe, un-censurable internet the protestors in Iran (2022-2023) could be considered a case of R2P.

Acknowledgements

First and foremost, to my beloved parents, Negar and Kamran, for all their love, support and dedication. Thank you, for all the bridges you made. I will always and forever love you.

Second, to Professor Michael Merlingen, for his fatherly support and his careful guidance throughout the composition of this thesis.

And last but not the least, to Dr. Benjamyn Scott, Dr. P. J. Blount, and Dr. Cameran Ashraf, for encouraging me to pursue my dreams.

Ever grateful,

Paniz Bahmani

Table of Contents

Introduction

For the past few decades, cyberspace has become an integral part of our everyday life. From ordering household needs to communicating with friends and loved ones, the world has become heavily dependent on cyberspace. Civilian use, however, is not the only way to utilize cyberspace. States, organizations and individuals have been weaponizing cyberspace in different manners to achieve a variety of goals, from hacking a user's social media, to national and international espionage, to utilizing it as an actual means of warfare causing virtual or tangible, physical damage to the assets - sometimes human assets – of a belligerent party in a conflict. This statement means that humanitarian crises can be caused, as well as prevented and stopped through cyberspace. And this, is where concepts such as humanitarian intervention, the laws of war, and the responsibility to protect (R2P) get tangled with the internet and cyberspace. I would like to narrow my focus on the matter of R2P. First and foremost, I would like to briefly introduce R2P to my readers.

The doctrine of responsibility to protect has been around for longer than it has been recognized by the United Nations in 2005. The first philosopher and legal mind to write about this concept was Hugo Grotius, Dutch jurist, who defended the concept of the international responsibility to protect in 1625, claiming in one of his works "On the Law of War and Peace" that intervention in order to assist populations against tyranny constitutes grounds for just war, and the first occurrence of its practice was the ban of slave trade by Britain in 1807, when the British Navy started patrolling the Atlantic Sea in order to identify and stop ships carrying slaves (Foreign Policy, 2011). According to Noel Dorr, one of the most well-known cases of R2P in our contemporary history – and my most favorite – is the second world war, where countries took part in a conflict to put an end to atrocities which were taking place (2008, 196).

There has been many a literature on the very debatable – and appealing to my personal interest – matter of R2P. James Bellamy, for instance, is one of the renowned advocates of the responsibility to protect. I, however, do not intend to bound myself to the traditional, more terrestrial concepts and applications of R2P.

In the first chapter of this thesis, I shall attempt to glance at the concept of international responsibility to protect. I will begin with a brief history of R2P, as well as some of the most notable discussions – those which serve to the purpose of this thesis best – over this much debated phenomenon. To name a few of these debates, I can mention the matter of sovereignty, and R2P being a "Western" invention. After presenting the literature review, I shall lay ground to prepare the reader for my second chapter.

My second chapter would discuss cyberspace and its uses in international relations and politics. The case for cyber R2P would be presented, as well as some of the fashions in which R2P could be conducted through cyberspace. This chapter also functions as a bridge between the first and the third chapter, by bringing together cyberspace and R2P.

In my third chapter, I would make my case for the ongoing situation in Iran. By referring and pleading to the content provided in the previous chapters, I shall attempt to answer my research question. I will make my arguments for the manners in which providing internet for people suffering atrocities could fall under the realm of R2P. At the end of this chapter, I would conclude my arguments and suggest my opinions on how such a measure would benefit the people of Iran.

Research Question

How can providing secure, un-censurable and free internet access to people of another nation – Iran, in this case - who are suffering from atrocities in their respective countries be considered a case of Responsibility to Protect?

Theoretical Framework

This research will be focused on finding a common ground in cyber policy and the matter of R2P. I shall draw on arguments in the literature that are supportive of R2P, and I would extend those arguments by drawing on the literature that discusses the importance of cyber space and social media in political mobilization, resistance, popular uprising, documenting human rights abuses, and etc. Most of the R2P theories will come from Alex J. Bellamy's works, specially "The Responsibility to Protect: A Defense". Cyber theories will be gathered from international as well as national cyber policies, as well as theories regarding the weaponization of cyber space.

Methodology and Data

The methodology of this research will be discourse analysis, as well as ethical-political and legal reasoning. I shall be looking at the concept of R2P through the prism of cyberspace, which in modern days, is an inseparable aspect of human life. My first set of data will be coming from journal articles, website and social media accounts of official news sources outside of Iran, as they provide the international community with the news of the situation in Iran. I will also be looking at news from National Iranian sources and authorities' and representatives' social media accounts, as a basis of comparison as well as getting insight on what the regime's strategy regarding the protesters is.

The second set will be unofficial news, from sources the factuality of which have been proven. This set includes any type of footage (picture and video), what people saw, heard or experienced firsthand, leaked agenda, as well as news channels run by exiled Iranian journalists in diaspora, and so on. This will give me a more accurate narrative of what is actually happening in Iran, rather than only leaning on governmental propaganda and false data. There

exist unofficial news sources whose reliability has been proven and they have dedicated their time, energy and resources on covering the revolution in Iran.

The subject of this thesis is personally near and dear to me, as I have first-hand experience on some of the issues that will be discussed. Nevertheless, I believe that this piece of literature could make a notable contribution to the discourse of the role of cyberspace in international politics and relations. I will be drawing references from highly stimulating literature and arguments regarding the responsibility to protect and its cyber manifestation. This, in my humble opinion, is important as I will be discussing the life-saving role cyberspace can play in R2P, the type of roles it can play, as well as the preventive aspect of R2P, which could change the dominant view that provoking the application of R2P happens only after a (mass) atrocity has taken place in a large scale. I believe that my work here could be contributing to the gap existing in the bridge between R2P and cyberspace, especially considering how wanting international law and relations are regarding cyberspace.

Chapter 1

The Responsibility to Protect: A Review

1.1What is R2P?

The concept of the international responsibility to protect has generated a lot of discussion among academics and in the international community. One of the first points I can bring up is whether the international responsibility to protect is a global norm or principle. I shall take a deeper look at the international responsibility to protect in this chapter, including its tenor, definition and the crimes it covers. To begin with, let us scrutinize and comprehend what R2P is and how it came to be in order to set the stage. State sovereignty and the international responsibility to protect are the two pillars that make up R2P.

The Westphalia Peace Treaty of 1648 created the sovereignty concept; a concept which stipulates that every State has a responsibility to defend its own people from (mass) crimes. According to the international responsibility to protect principle, if a government "fails" to protect a population from atrocities –meaning, fail to manifest its sovereignty - other States are still obligated to do so (R2P) (United Nations Office on Genocide Prevention and the Responsibility to Protect, resolution A/60/L.1, paras. 138–139). The international responsibility to protect's "R2P" core pillar is as follows:

> "The international community, through the United Nations, also has the responsibility to use appropriate diplomatic, humanitarian and other peaceful means [...]to help protect populations from genocide, war crimes, ethnic cleansing and crimes against humanity. In this context, we are prepared to take collective action, in a timely and decisive manner, […] on a case-by-case basis and in cooperation with relevant regional organizations as appropriate, should peaceful means be inadequate and national authorities manifestly fail to protect their populations from genocide, war crimes, ethnic cleansing and crimes against humanity" (ibid, para 139).

1.2. The Existential Aspect of R2P

Having this description and explanation of R2P and its international responsibility to protect, I would like to discuss the existential aspect of the responsibility to protect. This would fall under the jurisdiction of international law, but I would prefer to have a brief study of the matter as it would help us with the understanding of its entity as well as its level of commitment. Before proceeding, I see fit to refresh your memory on the normal hierarchy in international law. At the very top of this hierarchy comes *Jus Cogens*, or peremptory norms, which *Erga Omnes* commitments. In other words, peremptory norms are applied to all States, regardless of their membership status in the United Nations or any regional or international treaties. However, peremptory norms and laws require to be accepted by States as such, and it is only after their acceptance that States cannot opt. According to Article 54 of 1969 Vienna convention, "For the purposes of the present Convention, a peremptory norm of general international law is a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted and which can be modified only by a subsequent norm of general international law having the same character" (Vienna Convention, Art. 54). After *Jus Cogens* come the sources of international law, according to Article 38 of the statute of the International Court of Justice (ICJ), namely:

> "[A]. international conventions, whether general or particular, establishing rules expressly recognized by the contesting states; b. international custom, as evidence of a general practice accepted as law; c. the general principles of law recognized by civilized nations; d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law." (ICJ Statute, Art. 38 (1))

1.3. Debates on R2P: Friend of Foe?

In the debate about the entity of R2P, Hannah Yiu' approach is most compelling and convincing to me. Yiu regards R2P as a doctrine, of which the level of severity and commitment depends on the matter entailed in the R2P case (2009, 207). To put it in a different manner, in Yiu's opinion, it does not matter whether R2P per se is considered jus cogens or a simple norm,

but what is actually a matter of consideration is the situation to which R2P is being applied. In this argument, R2P is actually a flexible tool which adapts when it is applied to different situations with different levels of severity. As an example, according to the author, it has been argued that when jus cogens norms are at stake in an R2P case, the issue should no longer be viewed as merely one of international peace and security falling under the exclusive purview of the Security Council, but rather as one in which the use of the veto by the permanent five to block intervention would be illegal as a violation of jus cogens (2009, 208). In this case, the preemptory nature of R2P does not come from its own quiddity, but rather from *what it is trying to protect*. As we have now acquired sufficient knowledge about the nature of R2P and how its urgency is determined, I believe it is time to look at some debates for and against the doctrine.

Just as I have mentioned before, R2P is a very controversial matter, with many scholars and academics arguing for and against it. In the upcoming pages, an attempt has been made by me to study and analyze some of the literature centering R2P. I would like to start this process by broaching the work of Alex J. Bellamy. In his notable 2014 book titled "*Responsibility to Protect: A defense*", Bellamy argues that R2P is "our most viable option for creating a world that has no tolerance for atrocities" (2014, 2). Nonetheless, while discussing or studying R2P, one must be aware of the enemy R2P is up against. To put it another way, we require a cohesive understanding of the crimes that fall under R2P's umbrella of protection. The underlying premise is that mass atrocities are an integral part of mankind and are meticulously planned (2014, 24). However, it is important to remember that carrying out mass crimes is never regarded a first "weapon of choice" (2014, 23). Interestingly enough, Bellamy claims that even the notorious Nazi Regime had a plan to transport the Jewish population to Madagascar, and that they only turned to mass murder after their original intentions fell through. (2014, 23).

This, the first resorts falling apart and the incompetence of domestic laws, is where R2P takes over: to study, comprehend, and prevent atrocities. As Bellamy argues, R2P is our most

worthwhile option for countering atrocities, as domestic legislation is very unlikely to have the power to prevent (mass) atrocities.

Domestic legislation, namely – and specially - the Criminal Code of each country, can protect people from usual crimes – homicide, robbery, kidnapping, rape, and smalltime crimes. However, when it comes to mass atrocities, such measures fall short of their protective purposes, for mass atrocities are rational and tremendously organized phenomena (2014, 24). For understanding why domestic law cannot stand against "mass" atrocities, it is crucial to know that atrocities can be committed by government forces, as well as unofficial governmental militia and non-State actors (2014, 24). When forces are ordered by the regime itself to commit such actions, naturally the common domestic laws do not apply to them any longer and they are immune – at least as long as the ordering regime stands, and it does not need to sacrifice any of the "perpetrators" in order to save its reputation and exonerate itself.

To avoid such situations, something mightier than domestic laws and criminal code is needed: an international "force". I need to clarify that the word "force" does not insinuate that R2P is exclusively connected to the "use of force" as it understood in international law and discourse, but rather the legal and political force that accompanies with the implementation of R2P, or rather, a discourse of power, which is out of the scope of this research paper.

The case for R2P presented by Bellamy is now clear. His conclusion is that none of the major R2P substitutes could legitimately claim to satisfy the aims of atrocity prevention and human protection while also being politically possible and retaining the required balance with sovereignty, to put it simply and clearly. R2P thus demonstrates a more optimistic path for the world in which we live. The consensus upon which the concept is built, the clarity of the framework it offers, the emphasis on prevention and the suppression of incitement, and its ability to mobilize a wide variety of stakeholders are only a few of the principle's key benefits.

Amongst other scholars who work on R2P, I would like to cite the work of Noel Dorr. In his 2008 article, "The Responsibility to Protect: An Emerging Norm?", he talks about some challenges that R2P may be facing as a very young doctrine in international law and relations. In this piece of literature, the author mentions the matter of State sovereignty as one of the challenges that R2P may face, as "our current international system rests on State sovereignty of individual States" (2008, 191). Many critics of R2P may argue that this principle goes against State sovereignty as it involves direct (sometimes military) intervention in the domestic matters of a State. Dorr mentions the history of State sovereignty - which is out of the scope of this paper – and refers to the second world war as a war in which States fought for their survival and sovereignty, but it was also a case of preventing mass atrocities from occurring, which led to "a new and heightened consciousness of human rights in the immediate post-war years". (2008, 196). One consequence of the second world war was the establishment of the Nurenberg and Tokyo trials, which were an important precedent in which the perpetrators of atrocities were forcibly brought to justice (2008, 197). But what mostly relates to R2P, is the second result of the war: The Convention on the Prevention and Punishment of the Crime of Genocide (the Genocide Convention). As Dorr states:

> "This was an important step beyond Nuremberg: it was not an initiative of four major powers only, after the event, but a legally binding commitment undertaken by the great majority of member states of UN at the time; it covers atrocities committed at any time and not only during an unjust or illegal war; and most relevant to the question of a 'responsibility to protect' - it imposes an obligation on the parties to the convention, not only to punish, but to take positive action to stop those crimes it defines as genocide." (2008, 197)

Dorr's article very clearly shows that R2P, although very young in its recognition by the United Nations, has its roots deep in European history, and has been established since the Europeans were trying to protect Christians in the Ottoman Empire (2008, 194). Hence, its novelty is not going to be a big challenge for the application of R2P. However, there is a delicate point in Dorr's article, and that is the fact that some may argue that R2P may be

abolished due to its Western roots. Some scholars of R2P tend to cling to the idea that R2P is purely a western concept, and by putting forward that idea, they shall argue that since it has western roots, the "Rising Powers" of the world – the "BRICS" including Brazil, Russia, India, China and South Africa – would absolutely try their best to burn it down.

Amongst those who raise the concern of R2P's Western roots is James Pattison. Pattison expresses his concern about the – grave – challenges that are awaiting R2P in his 2021 article under the name "The International Responsibility to Protect in a Post-Liberal Order". In this article, Pattison comes up with three bleak scenarios centering the future of R2P in a post liberal world, based on the governing system of this alternative. The alternative world is governed by one of the three options: Realist-Nationalism, Pluralist-Sovereignism, and Lingering Liberalism. In his first scenario, Pattison predicts that some major democracies shall transition to far-right autocracies, and that the European Union will dissolve. There shall be a rise in authoritarianism and international institutions, such as the United Nations Security Council and the International Criminal Court become much weaker (2021, 891). So far, Pattison's concern seems global: weaker international organizations, specially the security concern, may lead to a decrease in the implementation of R2P. Pattison, however, continues to unveil his main concern: A weaker America. According to him, although the US would still maintain its hegemonic position, it shall become more and more insular and push a conservative and nationalist agenda, while a nationalist China would conduct its foreign policy forcefully in South-East Asia and Africa, regularly disobeying the norms of nonintervention and state sovereignty (2021, 891). I believe I can sense a sort of dualism – or hypocrisy, if you dare – in this hypothesis: Is not one of the main concerns regarding R2P undermining State sovereignty? If so, thus one may conclude that the violations of R2P by China may be considered cases of R2P. Or is it only accepted as conducting one's "responsibility to protect" rather than "aggressively conducting foreign policy" when it is conducted by a more globalist America

than Pattison's first scenario? In his second scenario, Pattison claims that the BRICS shall rise notably, and with their rise nationalism, authoritarianism and isolationism would rule the world, as matters like human rights would be seen as merely domestic to States (2021, 891). Once again, Pattison seems to firmly believe that the rising powers are going to abolish R2P altogether as it is a western concept, but so is most of international law and order, and if all of these are to be abandoned, the whole world order shall evaporate and the concepts he is using to put his hypothesis together would no longer exist.

It is worth noting that Pattison clung to the idea that R2P is a purely Western principle and practice, and non-Western countries would completely reject and abolish it. This has been the basis of many arguments which critical scholars of R2P bring up, but as I presented my counter arguments, that is not necessarily the only scenario awaiting the fate of R2P, nor it is basis for refusing to implement the doctrine in certain countries in dire need of it. In other words, vetoing the application of R2P due to the belief that some States may consider it a Western principle and "not believe in it" does not certainly make any of those beliefs true. At last, I shall not commence with Pattison's third scenario as it is basically liberalism, in which the situation with R2P is the same as we see today. I believe studying it – alongside the whole of Pattison's article – would make this chapter unnecessarily long and my readers impatient with boredom.

The last work I would like to refer to – which could be response to Pattison's cynicism- is the 2018 article by Noele Crossley titled "Is R2P still controversial? Continuity and change in the debate on 'humanitarian intervention'". In this article, the author claims that the point of view towards R2P has shifted since the early 2000s. According to her, the R2P discourse used to be filled with negative bias and fear, especially in the case of sovereignty, but it has been turned into a softer and "more supportive" approach (2018, 431). Crossley states that the goal of the R2P concept was to advance particular values and shape political behavior in accordance

with a particular worldview, and it was created by cosmopolitans, reflected a solidarist philosophy, and was supported by liberal people and organizations (2018, 428). As Crossley puts forward, R2P has significantly influenced the global discussion on intervention and humanitarianism in only briefly over ten years. The primary paradigm for evaluating measures in response to serious human rights breaches has in fact been superseded by the "responsibility to protect" rather than "humanitarian intervention" (2018, 429). One of the interesting points to me in her work, is her study of the international Non Governmental Organizations (NGOs) in relation to R2P. According to her, although a large number of NGOs are critical of R2P due to their pacifist nature and activities, 89 NGOs are members of the International Coalition for the Responsibility to Protect (ICRtoP) at the moment, but in general, Crossley concludes, NGOs are cautious in their approach towards R2P (2018, 427). Nonetheless, the most notable part of this article is that she elaborates how feminist critique of R2P made it stronger and positively affected its "comprehensive development" as, according to Crossley, the feminist critique of R2P took a 180 degree shift when some feminists started to argue that R2P possesses the potential to actually be used as a tool for advancing women's rights (2018, 427). Initially, the feminist response to R2P had been one of skepticism owing to R2P's link with the use of force – an instinctive response, as it has been the case with many other actors and critiques - however, placing a solid emphasis on prevention and integrating R2P, as well as aligning it goals with the Women, Peace, Security (WPS) agenda, the assisted with mainstream R2P and lessened some of the feminist skepticism (2018, 427).

What I take from Crossley's work is that some critique groups of R2P have discarded their cynical bias and softened towards the principle. Her example of feminist critiques, and how some feminists initially voiced the idea that R2P could in fact be utilized in pushing the feminist agenda paves the way for other critiques to probably take a new approach, or at the very least, be open to the new ideas and aspects that may arise regarding the theoretical

framework as well as the practical implementation and manifestation of R2P. There may be more potential for R2P to be utilized in other realms as well – just as it was with feminism and women's rights – but no one would know unless new ideas are embraced, and critiques would soften their guard to some point.

1.4. Closing Remarks

To close off this chapter and the discussion regarding R2P, I would like to quote Gareth Evans, the Chair of the international Advisory Board of the Global Center for the Responsibility to Protect. In a speech he delivered at the center, he mentioned:

> "Normatively, the concept of 'the responsibility to protect' has achieved a global acceptance unimaginable for the earlier concept of 'the right of humanitarian intervention,' which R2P has now rightly and almost completely displaced. Although many states are still clearly more comfortable with the first two pillars of R2P than they are with the third, and there will always be argument about what precise form action should take in a particular case, there is no longer any serious dissent evident in relation to any of the elements of the 2005 Resolution. The best evidence for this lies in the General Assembly's annual debates since 2009, which have shown consistent, clearly articulated and overwhelming numerical support for what is now widely accepted as a new political (if not legal) norm, and in the more than eighty resolutions and presidential statements referencing R2P that have now been generated by the Security Council (the great majority of them coming after the bitter disagreements over Libya in 2011 […]" (2020).

Now, I believe we all have an acceptable grasp of R2P – its nature, its level of command, its benefits and the challenges it may face. However, this was only the beginning of my research. As the title gives away, I shall attempt to link the concept of R2P to cyberspace in the remaining chapters of this thesis, and to do so I shall lay some groundwork. I have already done so with the doctrine of R2P, and presently I invite you to continue to the next chapter, where I will be providing some background information about cyberspace, as well as some research centering the role of cyberspace in international politics and relations.

Chapter 2
R2P and the Role of Cyberspace

Human access to technology has been greatly accelerated in the recent decades. International law – and relations based on that – however, have been struggling to catch up in some areas. One of those areas, in my opinion, is cyberspace, which is a very novel dimension of human existence – let us say since the 1990s – and yet, after approximately forty years, it is still suffering from a severe lack of (international) legislation. I believe this "negligence" if I dare say, is a result of the intangibility of cyberspace, which is both a blessing and a curse. Cyberspace, according to Mark Graham, is not "real" in the sense that it is not tangible, and it is not "locatable" as an item, but it is very real in the sense of the impacts and effects it has on our tangible and locatable world (2013, 179).

Cyberspace has been affecting our lives little by little since its emergence. It offers a various range of services, from ordering food online and streaming televisions series, to writing academic papers using artificial intelligence. It seems that our normal daily lives have been completely taken over by cyberspace, but that is not all. Cyberspace and technology have been playing major roles in (international) politics as well. One of the uses of cyberspace in international relations is in the peacebuilding process, where according to Andreas T. Hirblinger, propaganda and positive instances of members of the different sides of a conflict working together are spread to the public through social media and other platforms, and the positive mindset people build of the "enemy" shall help the peacebuilding process and the transition from conflict to peace to go smoother (2023, 133).

Another example I can present of the roles of cyber space in international relations – and this one is a personal favorite - has been empowering marginalized actors. According to Reardon and Choucri, in their 2012 conference paper "The Role of Cyber Space in International Relations: A Review of the Literature", the matter of empowering marginalized actor could be

a subject of dialogue between scholars researching global civil societies or authoritarian regimes and scholars working on cybersecurity would be of extreme benefit (2012, 26). This proves that first, "marginalized actor" does not apply only to small organizations or terrorist groups, and "people" with their right to self-determination are also actors on the stage of international relations and global politics. Second, it insinuates the important role – and greater potential it holds – in civil society activities, specially mobilizing against authoritarian regimes, which would be the core subject of my argument in this chapter. One of the major roles that cyberspace can play in cases of uprising against totalitarian regimes is providing other States with the opportunity to implement the principle of international responsibility to protect, without actual military intervention. Allow me to elaborate on that.

2.1. The Different Levels of R2P Implementation

R2P is not always implemented by military involvement, as different levels of it can be dependent on the different levels of the severity of the situation at hand. As I mentioned in chapter 1, according to the United Nation General Assembly's Draft Resolution Outcome of the 2005 World Summit, the members of the United Nations "have a responsibility to use peaceful" and diplomatic measures, and they "are prepared to take collective action" in more severe form in case those measures, as well as governments fail in protecting populations from atrocities (resolution A/60/L.1, paras. 138–139). In other words, in order to implement military level R2P, alternative (peaceful) possibilities must be taken into account first. One important – and quote recent – instance of non-military R2P is the case of Rohingya. As Zhu Xianghui, associate researcher at the Myanmar Research Institute & Center for China's Neighboring Diplomacy Studies of Yunnan University states, "[i]n the case of the Rohingya crisis, non-military interventions are valued. Due to the restriction of great power politics, the sensitivity of developing countries to sovereignty and the dispute over the connotation of the

‘responsibility to protect’, the United States and other western countries exercise the ‘responsibility to protect’ to solve the Rohingya” (2019, 14).

2.2. The Weaponization of Cyberspace and the Case of Cyber R2P

We must keep in mind that virtually all classes of actors, including governments and armed organizations, are turning the internet into a battlefield. Cyberspace is being weaponized when a government only provides its citizens with propaganda, which occasionally has the ability to stoke social unrest, or when a non-State actor organization disseminates racist or sexist viewpoints via its websites or other online platforms. According to Rhiannon Neilsen – whom I shall come back to in great detail later on - the Nigerian Army and Cameroonian soldiers, for instance, have been known to record live images of beheadings, murders, and immolations of "alleged" Boko Haram fighters (including women, children, and newborns) on their mobile devices. These are also widely disseminated through a number of platforms, including Facebook and WhatsApp, “as a ‘warning’ to anybody who might be enticed to join Boko Haram” (2023, 302). While in reality, criminals who perpetrate atrocities routinely videotape their actions and post the video online as a sort of recognition.

Additionally, noted by Troy E. Smith in his paper from 2017 titled "The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare," the Islamic State of Iraq and Syria is responsible for filming and disseminating footage of its atrocities, primarily as a deterrent and to assess the political cost-effectiveness of actions against it. It is also accused of recruiting members online (2017, 56). The really sensitive aspect in this situation is that, if the internet and cyberspace can be used as weapons to commit atrocities, they can equally be used to prevent or discover atrocities.

One precious piece of literature on the matter of cyber R2P is Tina J. Park and Michael Switzer's 2020 article titled "R2P & Cyberspace: Sovereignty as a Responsibility". In this goldmine of an article, the authors address the fact that the international community has been very ignorant towards the potential that cyberspace holds in the prevention of and response to mass atrocity crimes (2020, 114). They build up their argument by defining the three main categories of cyber capabilities, namely Cyber Material Sabotage (CMS), Cyber Information Collection & Manipulation (CICM), and Cyber Social Influence (CSI). As to explain each of these terms, Park and Switzer elaborate:

> "[C]MS capabilities enable an actor to damage another actor's capacity to function […] CICM capabilities enable an actor to obtain, organize and manipulate information about a population, institution, agency or operation – albeit in a way that does not cause material damage […] [and] CSI capabilities enable an actor to alter the perceptions, beliefs and decision-making of a given population" (2020, 119).

The authors then commenced to present the challenges and opportunities which each of these categories entail relating to R2P, of which for the sake of this paper I shall only reflect the opportunities that Park and Switzer discuss. They start with CMS, which, in their own words, provides very limited chance of "acceptable" use as a prevention tool, due to the legal limitations set by the United Nations Security Council and international documents such as the "Tallinn Manual" (2020, 121). According to Park and Switzer, the Tallinn Manual bans intervention in the domestic affairs of other States, including through cyberspace, or non-cyber measures against cyber infrastructures and capabilities of other States, and this poses a bit of legal difficulty to use CMS as a tool of R2P against States, especially as Material Sabotage is aggressive and coercive in nature (2020, 121). There is, nonetheless, precedent of CMS being used against non-State actors, as the United States government did against ISIS in 2016, which was considered a preventive measure (2020, 121).

Park and Switzer continue with CICM capabilities, which can be of great assistance with the documentation of mass atrocity risks as it enables civilians and journalists in recording

and organizing data via their smartphones and ICTs (2020, 123). This could provide great measures of atrocity prevention in three ways: 1. ICTs can be used as a means of "early warning and mobilization", a notably interesting example of it being the Egyptian revolution in which the people circumvented governmental censorships and recorded evidence of police brutality against protestors as well as the governing political repression at the time on their phones 2. The capacity of persons experiencing ongoing atrocity crimes to self-report permits such actors to provide policymakers and the general public with a steady stream of information. For instance, the recent disclosure of 24 papers about China's incarceration of Muslim communities in Xinjiang has sparked intense attention on a global scale in possible crimes against humanity 3. Third, by using timely data produced by the use of digital technology, a new and rich body of prospective evidence has been formed. Due to the fact that both of the ICC warrants for Libyan Commander Al-Werfalli were based on recordings taken from social media, this is already the case (2020, 123). Opportunities are presented by CSI capabilities because they enable actions that counter hate speech. Targeting hate speech entails both proactive, constructive interaction with the target audience and the suppression of hostile actors through attacks on their online presence (2020, 125).

Another important, and the last for this chapter, article on the matter – which also caters to my needs perfectly – is Rhiannon Neilsen's 2023 article titled "Coding Protection: 'Cyber Humanitarian Interventions' for Preventing Mass Atrocities". In this piece of literature, with a nod to James Pattison who I have formerly cited, Neilsen argues that R2P is "'mostly about the alternatives' to conventional military intervention", and as an alternative, she defines cyber R2P as "the use of sophisticated cyber operations to prevent and mitigate mass atrocity crimes" (2023, 300). According to Neilsen, aside from the theoretical foundation, these activities also try to undermine the motives and means of the offenders (2023, 301). As an instance of such measures, I shall quote Maziar Motamedi from Aljazeera news agency on the cyber attacks

conducted by the "Anonymous" hacktivist collective on numerous "government related or State affiliated media websites" of Iran, after the death of Mahsa Amini, as a way of showing support for the people of Iran (Motamedi, 2022). According to Motamedi, after the attacks the collective released a video in which one of the members declares in an artificial voice that "[t]his was the last straw. The Iranian people are not alone" (ibid). Reported by Iran International news agency, this collective also blocked the access of the Iranian government to its bank accounts and financial assets, claiming that the money belongs to the people (Iran International, 2022). As I mentioned by quoting Park and Switzer, blocking the assets of a perpetrator is a way of protecting citizens from mass atrocities.

Commencing with Neilsen, I would like to study her examples of ICTs in R2P. The first one she mentions is satellite imaging, which has been used by organizations such as the United Nations Human Rights Watch, "to 'cut through' the fog of extreme human rights violations in locations including Iraq, Myanmar, North Korea, South Sudan, Syria and Ukraine" (2023, 304). Another one, to which I will refer back in my third chapter, is called crisis mapping of "mass source data", in which any witness to an atrocity is given the ability and opportunity to record and submit the issue through the internet on a specific website, which results in a realistic and "near real-time" picture of the matter (2023, 304). Quoting Kristin Sandvik, Neilsen argues that the defined goal of humanitarian technologies is to assist communities in obtaining vital information they can use to save themselves, however, vulnerable communities have very limited means to protect themselves and are frequently unable to make effective use of such technology (2023, 305). One more argument Neilsen makes to criticize the current use of ICTs in R2P is that at this time, internet is mostly used passively to avert atrocities, in order to (hopefully) prosecute offenders and provide transitional justice, and these technologies are almost solely utilized for the identification, observation, verification, collecting, and documentation of evidence of crimes (2023, 306). She believes

that the best use of ICTs in R2P would be receiving and sharing early warning signs of atrocities, especially with policymakers who are responsible for the safety of people (2023, 306). If by policymakers, she means international entities, that is a valid argument. However, in the case of domestic policymakers, I beg to differ. In cases where the policymakers are a part of the body of the government who *is the perpetrator against its own people*, sharing early warning signs with the policymakers or executive bodies of government is not only useless, but sometimes dangerous.

Back to Neilsen – and bear with me, as this is my last reference to her for the chapter – her main idea is that cyber R2P can directly target the perpetrators, and in one of two ways can prevent atrocities: First, by interfering with operationally necessary infrastructure, such as communication networks, logistical supply chains, and financial transactions, such attacks might hinder (possible) perpetrators' ability to carry out crimes. Second, through what the author refers to as "targeted teaching campaigns", cyber interventions might secondarily target (possible) offenders' reasons for committing crimes (2023, 306). I shall briefly go through the methods she proposes: "1. Blocking communications and deleting propaganda (2023, 306). 2. Manipulating logistical supply chains (2023, 309) 3. Freezing financial revenues and leaving no trace (2023, 310) 4. Targeted educational campaigns (2023, 311)".

2.3. Closing Remarks

I would like to close this chapter with a quick review of it, as well as laying down some groundwork for my next. We started this chapter by studying cyber space, its effects on our life and the role it has been playing in international relations and politics, such as peacebuilding and empowering marginalized actors. Then, we saw that all classes of actors can be using cyber space to their benefit, and this includes non-State actors, such as terrorist organizations, as well the general public. I took that idea and mixed the idea of R2P with the civilian citizens using

cyber space, and referred to the works of Park and Switzer, as well as Neilsen to broaden the horizons for cyber R2P. Now that this is settled, in my next chapter I shall put forward my own idea of Cyber R2P, and build my case based on the citations of the present chapter, especially Parks and Switzer, and Neilsen.

Chapter 3
Cyber R2P: A Case Study of Iran

In the previous chapters, I talked about the principle of R2P, its scope of application, and its validity, as well as the role of cyber space in international relations and politics. Then, I commenced with bridging R2P and cyber space, and studied the concept of "Cyber R2P" and its possibility, the manner of its application and how it could actually work. Now, in this present – and final chapter – I would like to bring forward my own arguments based on a recent case, but first, allow me to present to you my case study. Before I continue, it is noteworthy that the translations of sources and data from Persian to English are done by myself unless I state otherwise.

3.1. A Brief Background of the Situation in Iran

In September 2022, as I was spending my last few weeks in Iran, a 22-year girl named Mahsa (Zhina) Amini died in the custody of the Morality Police forces in Iran, the reason for her arrest being "inappropriate attire" (Amnesty International Public Statement, 2022)." It is necessary for me to explain that the Morality Police is a branch of Iran's police force in charge of monitoring the state of "hijab" in public places, as wearing one is mandatory under Iran's criminal code. The news of Mahsa Amini's death went viral on social media platforms e.g. Twitter, Instagram, Telegram channels, etc. This caused a widespread uprising of Iranians, demanding explanations as well as the prosecution of the officers responsible, to which the government reacted with brutal crackdown and fake scenarios. The unclear answers as well as the bloodthirstiness of security forces caused deeper rage in people, leading them to organize protests and demonstrations through social media, as well as spreading news, photos and videos of the viciousness and ferocity of security forces, which reached to news sources outside of Iran, bringing international attention to the escalating situation.

As a result, the Islamic republic regime shut down the internet completely. It was shut down for few weeks on and off, and still after eight months many services and platforms are filtered. However, this was not unprecedented. In one of the latest and most well-known cases, the Ministry of Communications – under the order of the Supreme National Security Council— cut off the internet for a week in November 2019 proceeding the protests to an increase in petroleum prices. During that week, 1500 protesters were killed by governmental forces. When facing international criticism for cutting access to the internet, the Islamic republic claimed that Iranians had free access to the "national internet" or intranet the whole time (ISNA, 2019), which is strictly monitored by the Stare. Since September 2022 up to the time of the composition of this thesis, thousands of arrests and hundreds of cases of murder, unlawful execution, rape, disablement, and torture have been reported (see e.g. New York Times, 2022).

In fear of such news spreading, especially internationally, the government cut down the internet and in some cases that it was not able to do so, interruptions and denials of access, especially to international messengers, social media, and news were still enforced. Cutting off access to (global) internet at times of crisis has turned into common practice for the Islamic regime in Iran, as a means of punishment for people, to prevent them from mobilizing, and most importantly, to prevent the news of its inhumane behavior from reaching western countries.

The specific targeting of some minorities – e.g. Kurds, Balochs and religious minorities such as Bahaies - and women in Iran by the regime escalates the situation from mere unrest to an atrocity. Baloch detainees are suffering mass executions and murders (Deutsche Welle, 2022) and Kurds have been targeted with military-grade heavy machinery in their towns (Reuters, 2022). On another occasion, Ali Akbar Raefipour, a member of Iran's Islamic Fundamentalist party addressed the protesters in a tweet: "If you have a death wish, come to the streets. Especially if you have a beautiful face" (Saednews, 2022). This refers to many

female detainees being raped, and many female protesters being deliberately shot in their faces from a close proximity, which causes the deformation of their face for life.

3.2. Are We Facing an Atrocity?

It has been debated that the situation and the severity of the crackdown in Iran could be considered an atrocity. For instance, in early March 2023 Javaid Rehman, the special rapporteur on human rights, reported to the United Nations Human Rights Council that:

> "[D]irections given by the highest state authorities point out a deliberate policy to crush protests at all costs...[v]ideos, reports and eyewitness testimonies have shown security forces (including the police, the Islamic Revolutionary Guard Crops and the Basij militia) violently cracking down on protesters and have revealed a widespread pattern of unlawful lethal use of force, including the use of shotguns, assault rifles and handguns against the protesters"

However, referring back to Bellamy, we must bear in mind, as a most crucial point, that mass atrocities do not happen suddenly and pointlessly, rather they are meticulously planned and executed towards a goal (2014, 23). Also considering the report provided by Javaid Rehman, it is safe to assume that atrocities are taking place in Iran, and, in most cases, it cannot be determined whether they are considered mass atrocities. My point is, it is unclear in which cases the vicious crackdown by the government is meticulously planned, and in which the security forces are just using brutality to subside the protests. In my opinion, the crackdown operations can be generally categories. One is police brutality merely to subside the protests, and one is carefully planned operations to kill, disable or arrest protestors, coming along with a huge amount of propaganda. For instance, on September 30, 2022, in Zahedan, Iranian security forces used unlawful lethal force on a number of protestors, killing and injuring a number of dozens of them. This was the worst day of the protests, known as "Bloody Friday," with the greatest number of fatalities (Human Rights Watch, 2022). Zahedan is the capital of "Sistan and Baluchistan" province, populated by Sunni Balochs. The people of this part of Iran,

just as Kurdistan, have been deliberately discriminated against by the regime, mostly due to them being Sunni, and the crackdown and brutality against them has been specifically inhumane. This could be considered part of a systematic and carefully planned atrocity – a case of a mass atrocity.

3.3. The Preventive Nature of R2P

My personal belief is that the ongoing situation in Iran – regarding Javaid Rehman's report to the United Nations Committee on Human Rights – is severe enough of an atrocity – even if not "mass" - to provoke a case of R2P. The sanctions western countries are activating against the Iranian regime and its high-ranking individuals are the diplomatic form of R2P. Nonetheless, I would like to argue that lower levels of non-diplomatic R2P can be applied to lower levels of atrocities – those which are not considered "mass atrocities". In other words, if after the failure of diplomatic methods, a case of military R2P can be applied to a case of mass atrocity, to a case of mere but consistent atrocity a lower level of R2P could be applicable – namely, cyber R2P. After all, the responsibility to prevent is to some extent at the heart of R2P, and such cases could be considered preventing atrocities from developing into mass atrocities – a form of preemptive prevention, if you will.

On this subject matter, I would like to quote the work of Jennifer Welsh, a 2015 article titled "The Responsibility to Prevent: Assessing the Gap Between Rhetoric and Reality". In this paper, Welsh states that it has been long proven that prevention of atrocity crimes is more favorable than responding to them, considering the corresponding human suffering as well as the corresponding economic and political consequences and costs of response (2015, 217). As Welsh elaborates, she argues that a variety of approaches to prevention are possible, from long-term structural support to more immediate preemptive action meant to avert what is seen to be an approaching catastrophe while the same basic premise underlies both sets of policies: that

violence can be prevented, making prevention both more beneficial to global peace and security than post conflict reconstruction (2015, 217). Welsh also mentions that within the United Nation under Ban Ki-moon's leadership, emphasis on the vitality was so much that 2012 was named the year of prevention and the preventive dimension of R2P was emphasized during that year (2017, 219). According to Welsh, there are different risk factors that could lead to atrocity crimes:

> "[T]he presence of war and armed conflict, which creates both a motive and enabling environment for mass killing; economic and/or social instability and crisis, which can both generate both motives for violence and weaken the capacity of state actors to respond; an exclusionary ideology, which facilitates the creation of group-identities along hierarchical lines; an authoritarian government, in which deference towards leaders and elites erodes normative checks on orders to perpetrate violence; and a history of previous atrocity crimes, which heightens perceptions of grievance and threat" (2025, 219).

With all said by Welsh, I believe it is safe to conclude that R2P could be applied to atrocity crime situations that are not considered mass atrocities yet. Now, in the case of Iran, at least three of the risk factors currently exist in the ongoing situation: there is social and economic crisis, alienating ideology, and an authoritarian government. Hence, a lower intensity level of R2P could be considered applicable to the situation in Iran.

3.4. A Few Suggestions: Approaches to the Application of Cyber R2P in the Case of Iran

Regarding the internet outage in times of atrocities, the members of the international community (leaders, individuals, and organizations), under a Security Council resolution, have the opportunity to attempt to prevent such disruptions and disconnections by trying to offer new hardware and software to revolutionaries in the aforementioned country, as a way of protecting the population of the wrongful State against its atrocities. I shall attempt to study the case of Iran's 2022-3 revolution and determine how could offering new technology such as Starlink satellite internet, an almost un-censurable and secure means of communication like

Telegram (as opposed to domestic messengers or government approved messengers which are constantly monitored by the State) to protesting Iranians, or cutting and limiting the access of regime forces and organizations may fall under the realm of the responsibility to protect.

I have three approaches to this matter. One is based on Park and Switzer's work and the other based on Neilsen's theories, and the third a merge of the works of both (groups) of authors, all of which I have previously cited in the former chapter. I would like to start my argument with the work of Park and Switzer. Bear with me for the following pages, until I come to my conclusion (or my senses).

Park and Switzer, as we witnessed in the previous chapter, studied the role of the internet in the prevention and discovery of atrocities. To brush up on our memories, they claimed that CICM and CMS play a precious role in discovering and preventing atrocities – mostly CICM, as CMS have limitations, but are still very valuable. I will bring their arguments here, and merge them into my own case.

3.4.1. CMS and Terrorist Organizations

In my first debate, I would like to draw on Park and Switzer's study of CMS. According to the authors, CMS have limitations, as under the Tallinn manual, coercive use of them against States is verboten, however, it was used against the ISIS by the United States in 2016 (2020, 121). Now, we know that CMS stands for Cyber Material Sabotage, which paralyzes an actor's ability to function (2020, 119). This means that CMS possess the capability to cause tangible damage to "financial or institutional infrastructures" (2020, 120). This is another reason that using this capability against States is a risk and forbidden, as it can affect a society's resilience (2020, 120).

To tie this view to Iran's situation, and how the people can benefit from CMS, I would like to focus on the role of the Islamic Revolutionary Guard Corps (IRGC) in the protests'

crackdown. However, to begin with, let us see what this organization is. The IRGC is in fact the Iranian Armed Forces' main multi-service component. The IRGC's constitutional mission is to uphold the Islamic Republic's integrity, whereas the Iranian Army's traditional role is to defend the nation's sovereignty (Art. 150 IRI constitution). What the IRGC generally does is neutralizing military coups (I believe this is the main reason Khemeini established this organization immediately after the revolution), preventing foreign (mostly the West, as Russia and China freely do their share of "intervention") from interfering with domestic Iranian affairs, and - this one is the role I will be focusing on - suppressing "deviant movements" that threaten the Islamic Revolution's ideological legacy (Tasnim, 2022).

The IRGC has been having a very active role in suppressing the protests in Iran. This has been to the point that in February 2023, thousands of members of the Iranian diaspora rallied in Paris as a way of pressuring the European Union's member States into recognizing and enlisting the IRGC as a terrorist organization (VOA, 2023). In April 2023 the United Kingdom subjected over 70 members of IRGC to tougher sanctions in accordance with the United States and the European Union", including "four IRGC commanders 'under whose leadership IRGC forces have opened fired on unarmed protesters resulting in numerous deaths'" (France 24, 2023). I would like to take this, and connect it to CMS. As I mentioned before, CMS has a precedent of being used against ISIS. Now, I would like to argue that if the European Union, in accordance with the United Kingdon and the United States recognize and enlist the IRGC as a terrorist organization, using CMS capabilities against this entity would hardly be illegal any longer, as it is not a "State", but a terrorist organization. By doing so, the financial assets of this entity would be unavailable, henceforth, funding crackdown operations would be realistically extremely difficult to virtually impossible. On the other hand, paralyzing other infrastructures also can help save people's lives. For instance, altering or deleting the footage of traffic cameras, deleting costumer data from applications known to cooperate with

the IRGC (Snapp, for instance, which is an online taxi and food delivery service, or Digikala, Iran's number one online shopping platform are known to do so) can keep protestors safe from being recognized and targeted. This is one of the ways that cyber R2P can be applied to the case of Iran, by Cyber Material Sabotage of the assets of the perpetrator. But that is not all, and there are other ways as well.

3.4.2. CICM and Crisis Mapping

Another case in Park and Switzer's article I would like to appeal to, which serves to partially build up towards the answer to my research question, is CICM. As I mentioned before, the Cyber Information Collection and Manipulation allows individual citizens and journalists to record and document atrocities first hand, using their smartphones and the help of ICTs (2020, 123). This could be of notable assistance with early warning and mobilization, like they did in Egypt in 2011, providing evidence and drawing the attention of international policymakers to the ongoing situation (2020, 123). It's worth noting that in this case, documentation on websites and different internet based portals plays a key role. This one is quite self-explanatory. When, while committing acts of brutal violence and atrocities against protestors, a regime cuts off or limits access to the internet, it prevents the people from mobilizing, and from real-time documentation of events. This way, unifying and notification of events is difficult to impossible for protestors, and there will be very little to zero evidence of what actually happened, which could make proving the claims of victims harder in a court of law, and provides the regime forces to build their own narrative through propaganda.

This is very close to what we read as part of Neilsen's argument as well. If my readers remember, in the previous chapter, Neilsen mentioned that a realistic and "near real-time" image of the situation is produced by the crisis mapping of "mass source data" (2023, 304). This approach allows any witness to an atrocity to record and submit the incident over the

internet on a specified website. The purpose of humanitarian technologies, according to Neilsen, is to help communities acquire crucial information which can be utilized in the direction of saving their lives.

3.4.3. A Motivation Killer

Speaking of Neilsen, I would like to appeal to another case I brought up in chapter two. As we read, cyber interventions could secondarily target (potential) criminals' motivations for committing crimes through what the author refers to as "targeted teaching campaigns" (2023, 306). Amongst the techniques she suggests, the first three which were mentioned in the previous chapter are similar to what has been discussed in the present chapter. However, I would like to go over the last point she made: Specific educational initiatives. According to Neilsen, who quoted Mollie Zapata, an alternative to cutting off the perpetrator's access to internet or social media, is "instrumentalizing social media for peaceful purposes", which, instead of paralyzing the perpetrator's means, targets their motivation for committing atrocities (2023, 311). Neilsen is a firm believer that most people do not naturally possess the intention to kill, henceforth they shall only take part in committing the atrocity if there is a strong enough incentive to do so. One method to reduce, if short of stopping, the trend towards violence is to challenge the ideology and language that inspire people to take part in crimes (2023, 311). In a nutshell, Neilsen's argument here is that an effective measure to prevent atrocities is appealing to people through the internet, especially social media, and countering criminal propaganda with education.

3.5. How Could Cyber R2P be Applied to the Case of Iran?

Now that I have made my appeal to Park and Switzer, as well as Neilsen, I believe it is due time for me to draw my main argument from it. I would like to argue that providing internet, and in my specific case study, providing internet to the protestors in Iran, could be considered

a form of cyber R2P. Allow me to elaborate on this. What I have just cited from Neilsen includes education via social media and the internet, and it is more than obvious that such an agenda would be completely fruitless, if not impossible, to push if the target audience does not have access to (global) internet. Henceforth, a pre-requisition to this type or R2P is making sure that the target audience has access to global, unfiltered internet. The same logic can be applied to the case CICM argued for by Park and Switzer, which Neilsen also made the similar argument of "near real-time image" for. Without safe and free access to global internet, there is almost no way – no safe way, and no guaranteed way – for the individual civilian witnesses and journalists to document their recorded evidence. Yes, the events could still be recorded via their smart gadgets, however, without their concentrated documentation on a safe online platform, the majority of these evidence would be going to waste and rendered useless as accessing every single smart gadget in an area and searching them for data is virtually impossible. Henceforth, I would like to contend that providing internet access to revolutionaries, who are subjected to tyranny by their governing regimes is considered a (modern) form of applying cyber responsibility to protect. States have the opportunity to fund promising individuals, corporations, international organizations, and etc., or to offer their services and servers to the aforementioned entities under the command of a United Nations Security Council resolution.

3.6. Closing Remarks

Some criminals may prefer to carry out their crimes in secret, despite the fact that many may desire to display their atrocities to the public in order to discourage or attract recruits. This may be as a result of their concern for domestic and foreign retaliation. Sometimes, such as during the 2011 Egyptian Revolution or the 2022–2023 Iranian uprising against the Islamic Regime, governments have blocked citizens' access to "global" internet. Having resources

available will aid the populace in spreading the word and, in a sense, counteract official propaganda. Additionally, maintaining contact with the many participating "branches" and organizing mobilizations are both aided. But, in my humble view, access to the worldwide internet is most crucial since it reveals the truth. The reality of what is occurring, the crackdown by the regime and how it treats protesters and those who have been detained, (illegal) arrests, brutality, etc. Such activities might be seen as a kind of support for the Iranian people's quest for liberation from an authoritarian dictatorship that not only threatens its own people (on a global scale if I may say), but also the peace and security of the international community.

Concluding Remarks

In this thesis, I tried to contribute to filling the gap in cyber R2P, with a specific focus on the internet outage and censorship in Iran during the 2022-2023 protests. I started my work by going over debates around R2P in my first chapter, including cited arguments from scholars for and against the matter of R2P. This chapter aimed to give a better sense of R2P to the readers as it would be the center of my arguments in the next chapter, as well as to lay ground to go over cyber R2P in the second chapter.

The second chapter went over the role of cyberspace in international politics and relations. Afterwards, I studied how R2P could be manifested through cyberspace. For the purposes of this chapter, I mostly relied on theories and arguments provided by Neilsen, as well as Park and Switzer. These scholars' works included cases of crisis mapping through mass data through CICM, educational programs as a way of destroying the motivation to commit atrocities, attacking the perpetrator's tangible assets through CMS, and cutting off or limiting the perpetrator's access to the internet, as ways of stopping or preventing atrocities.

My third, and last chapter, is dedicated to studying the case of Iran. My research question is "how can providing internet to the revolutionaries in Iran be considered a case of R2P", and I drew arguments from the former chapters of this thesis to build my own case in answer to this question. First, relying on Park and Switzer, I argued that by declaring the IRGC, CMS could be applicable to it, as a form of R2P. However, this is just a small detour, and my main argument is built on Park and Switzer, and Neilsen. I contended that actions such as crisis mapping through mass data, mobilizing popular movements or educational campaigns or completely dependent on the population's access to global internet. No amount of recording footage of atrocities is useful if they are not to be stored on an online platform, and providing education would be fruitless if people cannot access and benefit from it. At the end of this

chapter, I came to the conclusion that in these manners, providing internet to the people uprising against the regime in Iran could be considered a case of Cyber R2P.

I suggest that more focus be put on the relationship between the cyberspace and international relations, specially something as contentious as R2P. Considering how wanting international law and relations are when it comes to cyberspace, I suggest more attention to be paid to cyber policies that can broaden the protective umbrella of R2P to internet access for vulnerable communities suffering atrocities. This could be due to the fact that free and safe access to global internet, in a manner which the perpetrator cannot monitor individuals' political activities online, could be a vital and lifesaving asset in revolutionary situations. We should also consider the role that crisis mapping data can play as evidence in a court of law for the prosecution of the perpetrators. More research and policymaking in this area could pose as a breakthrough in the realm responsibility.

Bibliography

1. Amnesty International, Public Statement. "Iran: Urgent International Action Needed to Stop Mass Killings of Baluchi Protesters." Amnesty International, November 12, 2022. https://www.amnesty.org/en/documents/mde13/6193/2022/en/#:~:text=Security%20forces%20unlawfully%20killed%20at,province%2C%20on%204%20November%202022.
2. Bellamy, Alex J. *The responsibility to protect: A defense*. Oxford: Oxford University Press, 2015.
3. Crossley, Noele. "Is R2p Still Controversial? Continuity and Change in the Debate on 'Humanitarian Intervention.'" Cambridge Review of International Affairs 31, no. 5 (2018): 415–36. https://doi.org/10.1080/09557571.2018.1516196.
4. Deutsche Welle. "Iran: Rights Groups Warn of Crackdown in Kurdish Mahabad – DW – 11/21/2022." dw.com, November 21, 2022. https://www.dw.com/en/iran-rights-groups-warn-of-crackdown-in-kurdish-mahabad/a-63827269.
5. Dorr, Noel. "The Responsibility to Protect: An Emerging Norm?" *Irish Studies in International Affairs* 19, no. 1 (2008): 189–207. https://doi.org/10.1353/isia.2008.0007.
6. Evans, Gareth. "R2P: The Dream and the Reality." Global Centre for the Responsibility to Protect, December 3, 2020. https://www.globalr2p.org/publications/r2p-the-dream-and-the-reality/.
7. Fassihi, Farzaneh. The People Executed or Sentenced to Death in Iran's Protest Crackdown". The New York Times, March 31, 2023. https://www.nytimes.com/article/iran-protests-death-sentences-executions.html?auth=login-google1tap&login=google1tap.
8. Graham, Mark. "Geography/Internet: Ethereal Alternate Dimensions of Cyberspace or Grounded Augmented Realities?" *The Geographical Journal* 179, no. 2 (2013): 177–82. https://doi.org/10.1111/geoj.12009.

9. Hirblinger, Andreas T. “Building a Peace We Don’t Know? The Power of Subjunctive Technologies in Digital Peacebuilding.” *Peacebuilding* 11, no. 2 (2023): 113–35. https://doi.org/10.1080/21647259.2022.2154957.
10. Homans, Charles. “Responsibility to Protect: A Short History.” Foreign Policy, October 11, 2011. https://foreignpolicy.com/2011/10/11/responsibility-to-protect-a-short-history/.
11. Hosseinpour, Farzaneh. “,ایسنا .”پیگیر برقراری اینترنت هستیم/ نگرانی مردم را می‌دانم November 19, 2019. isna.ir/xdDHLH.
12. “Iran (Islamic Republic of)’s Constitution of 1979 with Amendments through 1989.” Constiproject, April 27, 2022. https://www.constituteproject.org/constitution/Iran_1989.pdf.
13. Iran International. “‘Anonymous’ Says It Hacked Many Iranian Government Accounts.” Iran International, September 28, 2022. https://www.iranintl.com/en/202209289528.
14. “Iran: ‘bloody Friday’ Crackdown This Year’s Deadliest.” Human Rights Watch, December 22, 2022. https://www.hrw.org/news/2022/12/22/iran-bloody-friday-crackdown-years-deadliest.
15. Motamedi, Maziar. “‘anonymous’ Hacks Iran State Websites after Mahsa Amini’s Death.” News | Al Jazeera, September 21, 2022. https://www.aljazeera.com/news/2022/9/21/anonymous-hacks-iran-state-websites-after-mahsa-aminis-death.
16. Neilsen, Rhiannon. “Coding Protection: ‘Cyber Humanitarian Interventions’ for Preventing Mass Atrocities.” *International Affairs* 99, no. 1 (2023): 299–319. https://doi.org/10.1093/ia/iiac261.
17. Newsroom, Iran International. “UN Rapporteur Slams Iranian Regime’s Brutality during Protests.” Iran International, March 11, 2023. https://www.iranintl.com/en/202303113997.

18. Park, Tina J., and Michael Switzerer. "R2P & Cyberspace: Sovereignty as a Responsibility." *2020 12th International Conference on Cyber Conflict (CyCon)*, 2020, 113–27. https://doi.org/10.23919/cycon49761.2020.9131729.

19. Parent, Deepa and Habibzad, Ghoncheh. "'They used our hijabs to gag us': Iran protesters tell of rapes, beatings and torture by police". February 6, 2023. https://www.theguardian.com/global- development/2023/feb/06/iran-protesters-police-rapes-beatings-and-torture.

20. Pattison, James. "The International Responsibility to Protect in a Post-Liberal Order." *International Studies Quarterly* 65, no. 4 (2021): 891–904. https://doi.org/10.1093/isq/sqab081.

21. Reardon, Robert, and Nazli Choucri. "The Role of Cyberspace in International Relations: A View of the Literature." https://nchoucri.mit.edu/, 2012. https://nchoucri.mit.edu/sites/default/files/documents/%5BReardon%2C%20Choucri%5D%202012%20The%20Role%20of%20Cyberspace%20in%20International%20Relations.pdf.

22. Reuters. "Events in Iran since Mahsa Amini's Arrest and Death in Custody." Reuters, December 12, 2022. https://www.reuters.com/world/middle-east/events-iran-since-mahsa-aminis-arrest-death-custody-2022-10-05/.

23. Saed News. "."رائفی پور: اگر از جانتان سیر شده‌اید و چهره زیبایی دارید به خیابان بیایید December 6, 2022. https://saednews.com/.post/raefi-por-agr-az-jantan-sir-shodhaid-v-chhare-zibaii-darid-be-khiaban-biaiid

24. Smith, Troy E. "The Specter of Cyber in the Service of the Islamic State: The Zeros and Ones of Modern Warfare." *American Intelligence Journal* 34, no. 1 (2017): 54–58.

25. Tasnim. "- خبرگزاری تسنیم ".سپاه پاسداران چگونه تأسیس شد و فرماندهانش چه کسانی بودند؟ Tasnim, April 22, 2017. http://tn.ai/1382738

26. "UK Toughens Sanctions on Iran's Revolutionary Guard over Crackdown on Protesters." France 24, April 24, 2023. https://www.france24.com/en/asia-pacific/20230424-uk-toughens-sanctions-on-iran-s-revolutionary-guard-corps-over-crackdown-on-protesters.
27. United Nations, General Assembly. "Resolution Adopted by the General Assembly on 16 September 2005 [without Reference to a Main Committee (A/60/L.1)] 60/1. 2005 World Summit Outcome." New York: United Nations, September 16, 2005.
28. VOA. "Opposition Groups Rally in Paris Demanding EU List Iran's Guards as Terrorist Group." VOA, February 12, 2023. https://www.voanews.com/a/opposition-groups-rally-in-paris-demanding-eu-list-iran-s-guards-as-terrorist-group/6959879.html.
29.
30. Welsh, Jennifer. "The Responsibility to Prevent: Assessing the Gap between Rhetoric and Reality." *Cooperation and Conflict* 51, no. 2 (June 18, 2015): 216–32. https://doi.org/10.1177/0010836715613364.
31. Xianghui, Zhu. "New Modes of Non-Military Intervention Under the Responsibility to Protect: The Case of the Rohingya Crisis in Myanmar's Rakhine State." Stimson.org, October 30, 2019. https://www.stimson.org/wp-content/files/file-attachments/Zhu%20Xianghui%20- %20New%20Modes%20of%20Non-Military%20Intervention%20R2.pdf.
32. Yiu, Hannah. "Jus Cogens, The Veto and the Responsibility to Protect: A New Perspective." *New Zealand Yearbook of International Law* 7 (2009): 207–54. https://doi.org/10.1163/9789004345911_001.