Defining Sovereignty and National Interest on Cyberspace: National and Supranational Paradigms

A dissertation
Submitted to the Graduate Program of
University of Macedonia, Faculty of International and European Studies
In partial fulfilment of the requirements for the degree of
M.A. in International Public Administrations

Emmanouil Koulas
Thessaloniki, Greece

May 2019

«I hereby declare, that all the data used in this work, have been obtained and processed according to the rules of the academic ethics as well as the laws that govern research and intellectual property. I also declare that, according to the above mentioned rules, I quote and refer to the sources of all the data used and not constituting the product of my own original work»

Emmanouil Koulas

Abstract

This dissertation examines, within the operational framework of state sovereignty and national interest, the transformation of cyberspace in the 21st century. Focusing on the rising trend of conflictual interests being promulgated progressively into the cyber sphere, this dissertation parses that cyberspace has well and truly transformed into a battlefield increasingly employed and manipulated by both state and non-state actors. This tactic is unveiled in the way States have been forced to adapt to this new reality by building new capabilities and frameworks. States by focusing on the employment of state sovereignty and national interest principles, this dissertation examines how those aforementioned principles are operationalized in specific national and supranational paradigms.

Keywords: cyber security, cyber space, national interest, sovereignty

For my grandmother

Contents

1. Sovereignty 7
1.1 Introduction 7
1.2 Evolution of the concept of sovereignty 7
1.3 The Four concepts of Sovereignty 9
1.4 Sovereignty and the United Nations 10
1.5 Towards the cyber era 12
1.5.1 Sovereignty 13
1.5.2 Internal Sovereignty 15
1.5.3 External Sovereignty 15
1.5.4 Violation of sovereignty 16
1.5.5 Sovereign immunity and inviolability 18
2. National Interest 19
2.1 Introduction 19
2.2 Waltz's Theory of International Relations and his take on national interests 23
2.3 National Interests: A Historical Perspective 26
2.4 National Interests: A Realist Perspective 27
2.4.1 Morgenthau and national interests 27
2.4.2 Waltz and national interests 28
2.4.3 Mearsheimer and national interests 30
2.5 Comments and remarks 31
3. National Paradigms 32
3.1 Introduction 32
3.2 Belarus 32
3.3 Saudi Arabia 35
3.4 Israel 37
3.5 Comments and remarks 40
4. Supranational Paradigms 42
4.1 Introduction 42
4.2 United Nations 44
4.3 European Union 46
4.4 Organization for Security and Co-operation in Europe 47
4.5 Council of Europe 49
4.6 North Atlantic Treaty Organization 50
5. Conclusions 52
6. References 53

Page intentionally left blank

1. Sovereignty

1.1 Introduction

The genesis of international relations theories goes hand in hand with the birth of the sovereign state. Marxism treats the state as one of the actors in the international system, whereas pluralism accepts the fact that the state is the most important actor in the international system. Realism goes even further by having the state acknowledged as the sole factor in the international system. (Kouskouvelis, 2007)

The state has proven its endurance as not only the highest form of social organization, but also as a very effective and popular one, if one is to gauze the sheer number of States that joined the ranks of the United Nations from its establishment in 1945 (51) to over 190 Member-States nowadays. This does not speak so much of the United Nations ability to draw into its embrace States but rather showcases the reality of an international system which is built upon and defined by the States that form it. (Kouskouvelis, 2007)

A fundamental element of the modern notion of States is sovereignty, understood as a tendentially absolute prerogative of an autonomous and fully empowered collective. Scholars (Núñez, 2013) have questioned the validity of this absoluteness in practice, but it is still undeniable that modern political theory (and state building) is very much in debt with this theoretical absoluteness. It is thus that the concept of sovereignty is of paramount importance for explaining the functions of the international system.

A well-accepted definition of sovereignty is provided by the *Island of Palmas (United States vs the Netherlands)* arbitral award of 1928. It is stated that: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise, therein, to the exclusion of any other State, the functions of a State."

1.2 Evolution of the concept of sovereignty

Suffice to say that a traditional approach to sovereignty understands the same as European 18th century ancient regimes looked at the new constitutions: were they a simple gracious concession of an authority whose ultimate source of legitimation is not questioned (and that as such could be taken back in any moment), or were they the seal of a new normative order recognizing citizens (and humans after 1948) as the original bearers of sovereignty? The first theorist of the concept of sovereignty, Jean Bodin, used the concept as a way to enforce the power of the French monarchs. In Bodin's work "De Republica" (1576) in which he studies the concept of sovereignty (souverainete), he emphasizes the importance of the concept of the

supreme authority (summa potestas), is not subjugated to any other kind of authority. This supreme authority, personified in themonarch was granted with the right to draft, interpret and enforce laws without being subjected to the control of any other form of human power. Since he is not controlled by anyone, according to Bodin he is “absolutus”, thus subject only to the laws of the monarchy, God and natural law. (Kouskouvelis, 2007)

Even though the definition of sovereignty given by Bodin in the 16th Century was broadly adopted by other writers, most of them disagreed with specific points of Bodin's theory, by supporting that a law or a constitution could limit sovereignty. Then, in the 17th century Thomas Hobbes took Bodin's theory one step further, by formulating the opinion that sovereignty was not subject or limited by anything (Snyman-Ferreira, 2006). Thomas Hobbes in his work “Leviathan” (1651) will eliminate the reference to the metaphysical commitments. The “sovereign” is absolute, in the sense that even if he oversteps his authority he is not held accountable, since he is the reason for the formation of the state, the elimination of the natural state situation, or as Hobbes calls it "war of all against all" (bellum omnium contra omnes), and the safeguarding of life and property for every man (Kouskouvelis, 2007). In his work, Hobbes, clearly states that sovereignty is superior to every other right, even that of religion (Snyman-Ferreira, 2006). One can conclude that, in Hobbes’ work, the concept of sovereignty is a legal and political notion that allows the ruler to proceed with decision making processes, in the highest level, without any internal or external restrictions (Kouskouvelis, 2007).

The term “state” in the late 16th century defined a sovereign authority that was applied to an entire people in a territorially defined area. From this time begins a search (philosophical, theoretical) of the nature of state sovereignty and the means used for its exercise. The culmination of these theoretical and political pursuits was the liberal state itself and the assumption that power is exercised through the law and remains subordinate to it. In other words, a definition of the state under these parameters is understanding the, state as the supreme, sovereign power applied to an entire people in a defined territory (according to the law) (Kouskouvelis, 2007).

The concept of sovereignty, although it was originally conceived in order to support the power within the emerging countries and to abolish the control of the monarch or of the remaining feudal lords, was soon utilized to pit one state power against another (sovereign) power/party; essentially, against other States. In this juncture of the discussion, it is no longer about the dominant, supreme power within a state but the sovereign state itself. The state is sovereign because it decides on its own, without being under pressure and without being influenced by external factors (Kouskouvelis, 2007).

This paved the way to Constitutional Law and state theory, and added sovereignty to the arsenal of International Law and International Relations. To sum up, in international law each state consists of a population (people) who reside in a given space (territory) on which (people and territory) one sovereign power is exercised. Sovereignty is a property featuring unique States and is absolute and exclusive: There is within the state of this superior power, while at the same time the state excludes any influence or interference from any outside body inside (Kouskouvelis, 2007).

1.3 The Four concepts of Sovereignty

One of the most influential texts on the concept of sovereignty is Stephen Krasner's Sovereignty: Organized Hypocrisy. In his text Krasner (1999) elaborates on four concepts of sovereignty, namely:

1. Domestic Sovereignty,
2. Interdependence Sovereignty,
3. International legal sovereignty and
4. Westphalian sovereignty.

Sovereignty is a multifaceted concept which expresses itself predominantly in 4 different manners according to Krasner (1999). As Ferreira-Snyman (2006) summarizes, the first manner in which sovereignty is expressed is domestically (domestic sovereignty). It largely regards the level of enjoyment a state has to exercise its own power and the domestic organization of power. Second, the manner in which the state can exercise control relationally (interdependence sovereignty), i.e. border controls. Third, the legal status enjoyed by the state internationally (international legal sovereignty). Last, but not least, is the aspect of the so called Westphalian sovereignty which regards the ability of the state to organize its political life under two axes: the integrity of its territoriality and the ability to structure itself without outside influences.

As Krasner (1999) notes, there is a fundamental difference between authority and control, and even though it is not clearly stated, it is enrooted within the usage of the terms.

> *Authority involves a mutually recognized right for an actor to engage in specific kinds of activities. If authority is effective, force or compulsion would never have to be exercised. Authority would be coterminous with control. But control can be achieved simply through the use of brute force with no mutual*

recognition of authority at all. In practice, the boundary between control and authority can be hazy. (Krasner 1999, 10)

Litsas (2013, 47) observes that:

A liberal democratic regime in not the one and only political context for the state's sovereignty to arise, flourish and be maintained. Sovereignty in not necessarily dependent on ideological components such as those found in democratic regimes and liberal philosophical assumptions. Rather, it seems that, in any socio-political context, sovereignty functions regardless of the type of the political system of the state. Its form of operation is closely connected to the administrative, fiscal and judicial qualities of the state, as well as to the state's performance in the international arena, not the ideological facade it demonstrates to the other members of the international system.

What we observe is that sovereignty is one of the most primal concepts a state upholds, regardless of ideology or social structure. Sovereignty is directly connected with the state's constant struggle for survival.

1.4 Sovereignty and the United Nations

Since the foundation of the United Nations after the end of World War II, the concept of sovereignty has been severely changed and challenged. As it is stated in the preamble and in Article 1 of the Charter of the United Nations, the organization's aim is to prevent wars, maintain international peace and security and promote respect for human rights, as well as justice. In addition to all this, the United Nations, aims to facilitate international cooperation and provides for the use of collective measures.

The first reference to the notion of sovereignty appears in Article 2(1) of the Charter of the United Nations. However, it does not use the term on its own, but rather in relation to States. Specifically, the United Nations "is based on the principle of the sovereign equality of all its members". The principle of equality as described in Article 2(1) fully qualifies as an example of the Westphalian model, since this principle lawfully authorizes the current power relationships on the international system and formally recognizes and affirms the case that all States, regardless of their stature, ought to be dealt with as equivalent. Notwithstanding, the

presentation of the phrase sovereign equality into global law by the Charter of the United Nations demonstrates a critical change in the historical backdrop of the idea of state power.

Furthermore, the Friendly Relations Declaration of 1970 states again that the principle of sovereign equality ensures the right of state to equality in law. As the Declaration proclaims:

> *All States enjoy sovereign equality. They have equal rights and duties and are equal members of the international community, notwithstanding differences of an economic, social, political or other nature. In particular, sovereign equality includes the following elements:*
>
> *a. States are judicially equal;*
> *b. Each State enjoys the rights inherent in full sovereignty;*
> *c. Each State has the duty to respect the personality of other States;*
> *d. The territorial integrity and political independence of the State are inviolable;*
> *e. Each State has the right freely to choose and develop its political, social, economic and cultural systems;*
> *f. Each State has the duty to comply fully and in good faith with its international obligations and to live in peace with other States.*

It is understood, by this article of the Declaration, that the principle of sovereign equality integrates the notions of sovereignty and legal equality.

The Charter of the United Nations affirms that the sovereignty of States is restricted, by recognizing the superiority of international law. On this matter Article 2(2) of the Charter reads:

> *All Members, in order to ensure to all of them the right and benefits resulting from membership, shall fulfill in good faith the obligations assumed by them in accordance with the present Charter.*

In joining the principle of sovereignty with the principles that States need to abide by international law, the Charter of the United Nations unmistakably demonstrates that there is not a logical inconsistency, yet rather an association between state power and respect for international law. The Charter consequently affirms the preeminent idea of international law and portrays sovereignty as power within and subject to international law, and hence as a constrained notion.

Regarding the use of force, Article 2(4) of the Charter of the United Nations clearly maintains that all Member States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state. The Charter

therefore allows the Member States to resort to force only in two cases: First, under the authority of the Security Council and secondly, when States exercise the right of individual or collective self-defense per Article 51.

By prohibiting the use of force the Charter qualifies the classical understanding of sovereignty as absolute authority, which included as a key element the right to engage in war. (Ferreira-Snyman, 2006) According to Fassbender the ban on the use of force by the Charter is today understood not so much as a limitation of sovereignty, but as a necessary prerequisite for a de facto enjoyment of sovereign equality by States. Therefore, a state's sovereign equality depends on a comprehensive prohibition of the use of force and an effective mechanism to implement and enforce this prohibition. (Ferreira-Snyman, 2006)

Last but not least, under the Charter of the United Nations the Security Council is given the power, under Chapter VII, to make decisions that bind all member States and allows it to enforce these decisions. Even though one can argue that Article 39 of the Charter directly contradicts the classical notion of state sovereignty by excluding the Security Council from the principle of non-intervention under certain circumstances, this provision allows the Security Council to identify whether any threat to the peace exists, or to determine if an act of aggression occurs and to make recommendations for the decongestion of the situation or to decide on its actions in accordance with Articles 41 and 42 to maintain or restore international peace and security. In terms of Article 42 the Security Council is allowed to order military intervention which is a clear example of the powers of the Security Council to limit the territorial integrity and sovereignty of States.

In conclusion, the concept of sovereignty within the Charter of the United Nations can be summed up with Chainoglou's (2007, 63) explanation that *"Sovereignty is increasingly interpreted as a Janus double-faced concept, as a source of responsibility and immunity, of rights and obligations; and the challenge is to strike a balance between them."*

1.5 Towards the cyber era

With a dawn of a new era, comes always a rise on challenges that must be addressed. The first challenge that states have to deal with, as Chainoglou (2016) observes, is the borderless character of the cyber domain, which many times places the aggressors outside the territorial sovereignty of states. Another challenge that states have to face, intertwined with the concept of sovereignty, is the attribution of cyber-attacks, due to the complex nature of computer systems. And even if they are successful in attributing the attack, it does not necessarily equal to an attack within the scope of *jus in bello* (Chainoglou, 2013).

Chainoglou (2013, 202) further notes that:

> *"While certain aspects of cyber-attacks can be reasonably dealt with within existing legal frameworks, it has been said more generally that the 'cyber domain generally falls to be regulated within the established framework of relevant parts of public international law'. [...] In particular, there is a sense of discomfort with the application of jus ad bellum and jus in bello rules to cyber-attacks."*

Since traditional law documents failed to address the issues effectively, new legislature had, and still has to be produced. Besides national legislature, that many countries adopted, there is also the Convention on Cybercrime, adopted by the Council of Europe in 2001, the Tallinn Manual on the International Law Applicable to Cyber Warfare, produced by NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE), in 2013, as well as it's revision Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare in 2017.

The focus of this dissertation will be the Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare (herein after Tallinn Manual 2.0), because it provides the most holistic approach towards the challenges brought about by the cyber era, and it has codified them in a comprehensive manner, applicable to every state. The Tallinn Manual 2.0 has its first chapter dedicated to sovereignty, thus showing the importance it holds, both in its traditional application and on cyberspace.

The five rules regarding sovereignty in the Tallinn Manual 2.0 are:

1. Sovereignty,
2. Internal Sovereignty,
3. External Sovereignty,
4. Violation of sovereignty, and
5. Sovereign immunity and inviolability

1.5.1 Sovereignty

The first rule regarding sovereignty, as stated in Tallinn Manual 2.0 (pg. 11) is that "The principle of State sovereignty applies in cyberspace". This rule acknowledges the fact that sovereignty is one of the fundamental, if not the most fundamental, principle of international law. This Rule also reaffirms the fact that activities on cyberspace and state-sponsored cyber operation are examined under the principle of sovereignty. This highlights the

fact that States can exercise their sovereignty over any cyber related infrastructure and their activities within their territory.

When it comes to state sovereignty, international law recognizes that it is a fundamental principle. In this Rule, the issues that are approached are broad and there is no limitation on the notion of sovereignty over territorial sovereignty as one focuses on cyber-space. Moreover, one must understand that the notion of territoriality ceases to exist in its traditional interpretation. On the contrary, cyber infrastructures are such that national authorities exercise jurisdiction abroad as well, since the persons deemed to be involved in the proceedings are involved in activities beyond the territory from which they carry out an activity. This point is also discussed on Rule 4, which is discussed below.

Moreover, cyberspace is a "global sector" that has no specific boundaries and, while virtual, concerns a global joint action. Cyber activities can have an impact on the physical space of the state and society and may therefore fall under the jurisdiction of several national States (Rule 1, paragraph 5).

Therefore, it cannot be considered that an activity taking place in the Cycladic region necessarily involves a given state or its territory - including airspace, water and land. Now, national international law and national human rights law should be reviewed and a way for international organizations to intervene in these areas can be found. It should be noted, however, that according to international law, the concept of sovereignty is - as discussed - internal and external, inter alia, therefore, international organizations do not enjoy sovereignty.

In this rule the Tallinn Manual 2.0 encompasses within the principle of sovereignty the layers of cyberspace, namely the physical, logical and social. The physical layer includes all the hardware and other components. The logical layer includes the connections between network devices, as well as data, protocols and applications that enable connectivity between the components of the physical layer. Lastly, the social layer includes individuals and groups that operate on the cyber domain.

Last but not least, the International Group of Experts that authored the Tallinn Manual 2.0 agree that no State may claim sovereignty over cyberspace per se. This is due to the fact that a big proportion of the infrastructure necessary for the existence of cyberspace is shared among many States' sovereign territories. The first rule, therefore, focuses on the concept of sovereignty both etymologically and practically and the application it has today.

1.5.2 Internal Sovereignty

The second rule regarding sovereignty, as stated in Tallinn Manual 2.0 (pg. 13) is that "The principle of State sovereignty applies in cyberspace". Under Rule 2, States exercise national sovereignty in terms of government infrastructures, as well as those active in their territory and the electronic activities taking place in their territory, always subject to the rules of international law.

In essence, Rule 2 focuses on the "internal" dimension of sovereignty, allowing States to define the measures and activities they deem necessary to manage a question that arises (Rule 2, 1). Rule 2 broadens the discussion of Rule 1 on the physical boundaries of cyberspace because it recognizes that there are two legal dimensions that need to be taken into account: the first is that cyber infrastructures and activities within it are controlled by the national authorities, and second, that the right of sovereignty of the state in its territory also means the obligation to protect the people, transactions and operations in the cyberspace, but also that cyberspace takes the dimension of "territoriality". Territorial cyber sovereignty exists irrespective of the infrastructure or the nationality of the owner of an infrastructure and so on.

It is also noted that cyberspace is not fully vague or devoid of physical boundaries, since physical infrastructure is needed for its operation such as cables and there is a need for information transmission using a network. The purpose of Rule 2 is to lay down some legal and rational rules for the establishment of a common system which may contain cryptographic protocols or other rules for adequate control of cyberspace and activities taking place within the territory of a Member State and may include both natural and legal persons. Thus, it is possible to criminalize these persons in case of breaches of international or national law.

The question that has been raised is at point 8 of Rule 2 is whether a state, after enjoying internal sovereignty, can also restrict access to cyberspace. At this point, it is stated that international legal standards should always be applied and fundamental freedoms recognized. So, the same limitations that apply in the physical world apply to cyberspace. On the basis of this text, it is noted that States cannot access or transmit data relating to specific areas such as national security issues or persons residing and operating in their territory, unless international law provides for a different rule.

1.5.3 External Sovereignty

The third rule regarding sovereignty, as stated in Tallinn Manual 2.0 (pg. 16) is that "A State is free to conduct cyber activities in its international relations, subject to any contrary rule of international law binding on it". The content of this article is just as complex

as that of Rules 1 and 2 and is a logical continuation of the above. Based on this Rule, anyone, including the States, is free to engage in cyber activities, without prejudice to the rules laid down by international law.

External sovereignty, as a concept, in this Rule arises from national sovereignty as defined in Article 2 of the UN Charter. Therefore, no state has an advantage over the other and there is equality between them in all fields. In this sense, the definition of external sovereignty aims to include the concept of external security and the freedom of the state to engage in cyber activities and is reformulated as long as there is no violation of any principle of international law.

Recognizing the equality of States in cyberspace is an important dimension that can allow protection of the sovereignty of States in general. It also gives freedom to States to choose whether they want to set up special cyber regimes in application of Rule 1.

1.5.4 Violation of Sovereignty

The fourth rule regarding sovereignty, as stated in Tallinn Manual 2.0 (pg. 17) is that "The principle of State sovereignty applies in cyberspace". Rule 4 focuses on the consequences of violating the sovereignty of other States from a Member State into cyberspace. On the basis of this, it is completely prohibited to carry out operations which may jeopardize or challenge the sovereignty of another State, as is also the case in international law.

Rule 4 incorporates the content of Rules 2 and 3 and analyzes the consequences of non-compliance with these Rules. Particular emphasis is placed on cases where there is an exception to the rule of not interfering in the activities of a Member State, but also to the failure to disregard state sovereignty. In this respect, in particular, it is recognized that the competence of UN bodies, such as the Security Council, to approve such violations on the basis of Article 76 of the UN Charter and the right of the State to self-defense on the basis of Article 71.

Similarly, it is noted that this rule applies to international / transnational relations, provided that the Member States recognize the primacy of international law, the equality of national sovereignty of States around the world, and their duty to protect international peace and security. Thus, the state must take measures to curb terrorism and behaviors that can be dangerous to other States, and are thus required to warn other Member States of malicious actions. However, this does not translate into a right to violate the internal sovereignty of other Member States (Rule 4 (2)). Close attention is also needed for the action of non-state actors such as organized armed groups.

If there is a threat to the state and the right to self-defense is exercised or there is an objection to the necessity, then, under Rule 4, paragraph 4, countermeasures and penalties are provided for non-compliance. Since, under Rule 2, the State's sovereignty principle also includes cyberspace, the State is responsible for compensating a third State which has suffered critical infrastructure damage even if there is no damage to other infrastructures (Rule 4 5). More generally, international law on soil, the sea and airspace applies to cyberspace and, conversely, whether there is any impact on the state from activities carried out in the airborne, marine and marine environment. space, then there is corresponding responsibility from that state. The same applies to espionage and violation of other rights and obligations under the rules of international law and customary law.

However, as there is still no full agreement as to what cyberspace, cyber-functions and so on, and there is uncertainty about the evolution of cyberspace, based on paragraph 10 of Rule 5, the evaluation is based on two criteria: (a) the extent of the offense and (b) the direct intervention of the governmental functions. While paragraph 11 of Rule 5 States that the analysis concerns (a) whether there was physical harm, (b) if there was a loss of functionality, and (c) if the violation of national sovereignty leads to a marginal loss of functionality. In both cases the object and purpose of the principle of national sovereignty and the type of offense, as well as whether there was unlawful use of force, physical damage, the impact of damage and the degree of loss of infrastructure functionality, are examined.

Consensus was seen as a difficult task, and for that reason specific criteria were set for the definition of the offense, the consequences for the domestic legal sphere and the international community as well as the individuals, physically and legally, within the state. It is important that there is no violation of the personal data of natural and legal persons, usurpation of national sovereignty and the rights of the state in general.

An example of the complexity of the questions raised concerns those undertakings which impede part or all of the businesses of another State on the Internet or access the Internet. In these cases, the International Expert Group has considered that there is only a violation of the sovereignty of the third state as far as access to infrastructure is considered, although there is a risk of violation of other international law rules at the same time. Thus, the extent of the violations, the type and the consequences differ, and the purpose of the state, the measures and the actions required to deal with them must be considered. It is noted, therefore, that the nature of cybercrime violations is unpredictable and there can be broad social, economic and strategic consequences of activities, businesses and malicious internet activities.

Trust between Member States, respect for international law and rules in force in peacetime and cross-sectoral / international cooperation is required. This is an important addition to the Tallinn Manual 2.0 due to its international relations focus, since all of the aforementioned prerequisites apply to international law.

1.5.5 Sovereign immunity and inviolability

The fifth rule regarding sovereignty, as stated in Tallinn Manual 2.0 (pg. 27) is that "Any interference by a State with cyber infrastructure aboard a platform, wherever located, that enjoys sovereign immunity constitutes a violation of sovereignty".

This rule stresses that, regardless of the setting in which an intervention takes place, the infrastructure or the view from a third country recognized violation of the sovereignty of the Member State in which one violation occurred. In particular, because Rule 5 focuses on objects and functions that enjoy state immunity, it is noted that the examination of the incidents should be extremely cautious. The Paragraph 2 of Rule 5 stipulates the inviolability of state immunity, a right which extends to cyberspace, even given that the infrastructure does not serve national purposes exclusively. After all, national sovereignty and immunity are inviolable and interference is not allowed.

An example given concerns the non-consensual entry naval / military aircraft in the national airspace, in the case of cyberspace, if the aircraft can happen performs activities making use of this infrastructure. In this case, measures can be envisaged to put an end to these activities and countermeasures. Also, based on para. 6, the governmental infrastructure of neutral States may be classified, under certain conditions, as a military target, thus requiring the establishment of a special cyber-operational infrastructure protection system, electronic files and so on in order to avoid a full crisis.

Lastly, it must be mentioned that in the event of an international armed conflict, the principles of sovereignty and inviolability cease to apply, regarding the relations of the conflicting parties (subject to any specific rule of international law to the contrary, such as Article 45 of the Vienna Convention on Diplomatic Relations). This practically means, assets, otherwise enjoying sovereign immunity and inviolability, may be destroyed upon qualification as military objectives or may be seized as booty of war and ownership immediately passes to the captor forces by virtue of capture. Exceptions may apply for assets that are granted special protection by the application of bilateral or multilateral agreements (e.g. status of forces agreements), as well as certain infrastructure and electronic assets that are protected under diplomatic and consular law.

2. National Interest

2.1 Introduction

Tang Lan (2016) vibrantly asserts that in cases such as terrorists organizing online "national interests must be defended, and national sovereignty is necessary to do that. Therefore, any state must be able to decide what measures to take when it comes to defending their national interests in cyberspace." He continues on by underlying how the exigencies of cyberspace prove to be quite problematic when it comes to jurisdiction application and on the application of "state power to protect national sovereignty". While oceans of ink have been spilled on what constitutes national sovereignty when it comes to cyberspace, national interest notably is only mentioned in passing in the foreword by Toomas Hendrik Ilves (2017) in which he laments how the initiatives undertaken to forage to the international law applying when it comes to cyberspace has been "sometimes hobbled by narrow national interest and perspectives" or in the Tallinn Manual itself when it sporadically and sparingly refers to "critical national interests" without defining what qualifies as such.

This lack of definition(s) when it comes to national interests does not limit itself to cyberspace alone. In practice all governments have their own unique definitions and elaboration on what constitutes their national interests and this explanation may offer a correct or a wrong definition of national interests (Burchill, 2005). For instance, most political leaders in the United States define their national interests using broad terms to a degree that almost all events around the world are of interest to the United States (Barnett, 2008). In relation to this is a widely held notion that the United States needs to offer leadership in virtually every conflict and crisis happening in international politics. Such incidences provide politicians with numerous opportunities for engaging to the point of abuse the concept of national interests (Kowert, 2001).

The special category and notion of national interests has in the recent past enjoyed revitalization in certain areas of dialogue on international relations (Nielson & Tierney, 2003). It is the central role that the state possesses and in remaining the authority and foundation where modern international relations and international law is based that this revitalization is based. The main reason for the revitalization of the concept of national interest is a state, in specifics it's an effect of the growing geopolitical thinking in the United States (Lake, 2007; Beitz, 1979). Moreover, the rebirth of this concept is in many ways rooted to the need to redefine the role of America in international affairs with the intention of generating a justification for minimizing that role after the end of the Cold War (Hyde-Price, 2006; Ikenberry, 2012).

Going back to the beginning it is easily perceivable that national interest as a concept predates the concept of national security and is currently assuming its proper position in the United States political discourse (Lake, 2007; Burchill, 2005). To realise this change, it is vital for these changes to be put in context in relation to the Neorealist theory of international relations. This thesis investigates various issues around the international relations theories that are tied to the concept of national interests, especially the one of Neorealism, as applied in the current world.

The concept of national interest is very important in the Neorealism paradigm of international relations theory as it determines a nation's foreign policy and ultimately its ability to secure its sustainability from an international perspective. From the analysis of the concept of national interest as positioned by various Neorealists and also illustrated in real international relations issues, it is evident that national interests are not self-evident and are generally not national in nature, in the sense of the state and domestic preoccupation, but they originate from the numerous interactions between the main actors of the international system, in our case the States.

Various interest groups in the international system greatly influence national interests and therefore, Neorealists believe that effective focus on national interests should be externally driven and not internally developed and implemented externally. Neorealist also believe that identification of the national interests is not as important as identifying the various actors and elements and their levels of influence on the national interests of a country.

Generally, from a Neorealism theory perspective, national interests are granted to a nation the emphasis on the effects of international system on a country's security. Consequently, security is the most significant national interest of any country and the ultimate determinant of an effective foreign policy of any nation.

Many Neorealists would argue that effective focus on national interests should be limited to focusing on international issues that are within the capability of a nation. In the concluding remarks of this thesis we would like to employ an expressive example of the above assertion, that is the enjoyment by the United States of a unipolar system of affairs in international relations in its most recent history. Reviewing its recent activities illustrates a contrasting perspective to the beliefs of Neorealists, as the country has done in the recent past, focusing on increasing its global influence in a speed that is too fast and threaten to overstretch the American resources and hence collapse of status lead actually to today's multi-polar world.

Theorists in international relations focus on policy relevance as a benchmark of value supplementary to scientific truth. However, very little is said by Neorealists about national

interests as much as it is classified as a key aspect of the theory of international relations (Hyde-Price, 2006; Burley, 1993; Goldstein, 2007). In particular, the silence by Neorealists is clearly notable as Waltz (1974), the founder of the Neorealist theory of international relations argues that the idea of a nation pursuing its national interests or seeking its own preservation is only stimulating if the specific national interests that a country should focus on are identified. The above explains the silence about the concept of national interests by current Neorealists since it's mainly due to its low levels of interest as compared to other (more easily explorable) concepts.

As Waltz (1974) suggests, Neorealists find the concept of national interests monotonous since they have failed to determine the specific national interests that need to be explored by a state. Even though self-preservation can be considered as a perfect response to Waltz question, in-depth analysis of Waltz theory highlights the emphasis on what a country needs to do from the perspective of national interests (Goldsmith & Posner, 2005). Furthermore, it is the realist, Morgenthau, who further postulates that self-preservation is a necessary but insufficient rejoinder to this issue (Sagan, 2012; Burchill, 2005).

Morgenthau wanting to contribute and provide an explanation of the definition of power in terms of national interests, highlights the imperativeness of space and time without which the idea of international relations is non-existent (Rittberger, 2004). Morgenthau argues that the particular types of interests that influence a political action in a specific historical period is dependent on the cultural and political context within which the formulation of foreign policy takes place (Jackson et al., 2012; Krahmann, 2005). Consequently, the increasing silence of the Neorealists with regard to the concept of national interests might illustrate a point of theoretical malaise.

The concept of malaise explains the methodological pluralisms that emanated from the critics of Neorealism in the 1980s. Even though many theories of international relations often use the same words, they do not generally communicate because they do not speak the same methodological language-in other words, they have no common methodological basis to discuss their differences-to the point they became unintelligible to each other. (Lake, 2007)

Due to this intellectual anarchy, a serious after-effect is how research programs that lack enough funding are being crowded out. Unmarketable approaches and methods are therefore shutdown or downsized or acquired by distant paradigms. The last issue especially concerns currently numerous theoretical practitioners that elaborate on the intellectual mergers that take place due to epistemological issues that emanate from their integration (Taylor, 1992; Bieler, 2001).

A direct result of the above approach results in the creation of an almost market place on ideas related to the theory of international relations that is threatened by the propensity to evolve from monopolistic competition into oligopoly where research studies left after consolidation are the major consumers of new intellectual commodities (Sagan, 2012). They therefore control the market place and can influence the specific technical characteristics. The worst outcome of this situation is that the capacity of translation and dialogue among multiple traditions in the discipline is currently being lost (Collard-Wexler, 2006).

With relation to practicing theorists, the source of this behavior is even deeper as compared to the diverse conceptions regarding the research methodology. This is mainly as a result of the effects of real world observance and undertaking of analysis. Some approaches that emerged as a result of the Cold War remain valid but their universality has declined. But how all the above apply to our search for understanding when it comes to the analysis of the concept of national interest?

For instance, the idea of neoliberal institutionalism if founded on a study of the economic interactions between industrialized States (Jackson et al., 2012) in retrospect makes it incompatible with emerging and developing economies. For instance, the position of Russia as the leader among equals in the former Soviet Union complicates the applicability of models that existed during the reign of the Soviet Union (Taliaferro, 2006). The splitting up of the Soviet Union into different States as well as the existing ethnic divisions in the new States complicated furthermore the theoretical issues (Caporaso, 1992). It is in this way that the new independent States of the former Soviet Union are a clear case point. The need to delineate the concept of national interest in the former soviet cannot be equated to the United States case where the overt dialogue on national interest is much deeper than the general idea of national preservation (Sagan, 2012; Wohlforth, 2008).

Numerous States, including the United States, are seeking ways of defining their national interest as a basis of foreign policy formulation. Such an approach naturally makes the issue have more than just transitory relevance, especially since the case in hand is having the majority of the States around the world not being governed by well institutionalized bureaucratic structures while they do in fact have monopolized the exercise of physical force over an adjoining territory as is the case of most of advanced economies in the world (Collard-Wexler, 2006; Taylor, 1992; Al-Rodhan, 2007).

2.2 Waltz's Theory of International Relations and his take on national interests

Structural realists endeavor to expound on the nature of international relations through splitting the state level, whereas Waltz defines national States within international relations as units at system level within the structure.

Waltz believes not only that it is possible to establish results formulated for the subsystem by considering them at the system level (Waltz, 1974), but also that all States are, in the end of the day, security seekers and anarchy exists at the global level (Shain & Barth, 2003). Therefore, the concept of neorealism as positioned by Waltz highlights the concepts of anarchy, structure, capability, power distribution, polarity and ultimately national interests (Waltz, 1974; Taliaferro, 2006; Blyth, 2003).

The first two concepts, being structure and anarchy, -as it is going to be illustrated below-, are entangled. Another axiom is that the structure of the international system is considered to be anarchic. A small clarification at this point would be that the concept of anarchy as used in this context does not refer to the presence of disorder and chaos. It only refers to the lack of a global government (Waltz 1979; Risse-Kappen, 1996).

Recapping the previous axioms all together is it concluded that without a central global authority that offers stability and security in international issues, global politics is not hierarchically and formally organized. Consequently, international politics is structured by anarchy which is the opposite of what happens in domestic politics, that are themselves hierarchically structured (Taliaferro, 2006; Williams, 2004). The International system is therefore defined on the basis of an anarchical international structure (Banks, 1984). According to the literature on the issue, operating in an anarchical structure has two major implications.

Firstly, every player in international systems is only looking after itself which makes an international system a self-help system. The international system is therefore made up of self-regarding elements whose major emphasis is survival (Hobson, 2001). Secondly, taking into consideration that national States are the only actors of international relations that have a centralized and established legitimate authority to employ force when protecting their interests (Jackson et al., 2012; Barkdull & Harris, 2002), makes them (sovereign States) therefore the main elements that make up the international system and main actors in global politics.

Accordingly, the organizing standard utilized in international structure is anarchy and this structure is defined with reference to individual States. Moreover, national States continually feel threatened by the potential of attack by other States (Checkel, 1998). As Waltz (1979) illustrates, due to the lack of global commanding authority, no single country is obliged per se to obey another in international relations. Since each nation persistently feels insecure,

each country must be in a position to fend for itself. This culminates to the aspect capability as another concept influencing international relations. It is Capabilities that have been found to be instrumental for countries in order to guarantee their survival.

An assessment, and in a way attempted definition, of capability from a neorealist perspective is influenced by five major criteria, including its demographic, economic, technological, and military capacity as well as its natural resource capacity (Sagan, 2012; Taliaferro, 2006; Collard-Wexler, 2006). But it is not only the absolute capacities of a state that makes up its capability assessment. The focus on survival motivates States to focus especially on the aspect of relative gains. Relative gains signify the relative amelioration of a state's capability in relation to another and how much more important is, for ensuring one's state survival, to always ensure that their relative gain is well above another's-even in the occasion that absolute gains are decreased. Moving forward, it's presumably without difficulty to understand that each state has a different level of capability, making nations States easily distinguished based on their capability level in the international system. For the above reasons, Neorealists attempt to paint a national picture of each nation's capabilities at any given time. This notion is generally referred to as the relative capability of a state (Slaughter et al., 1998).

Connecting all the above concepts leads to the understanding that, since States are constantly insecure, they unendingly wish to acquire higher capabilities. This dynamic originates what constitutes one of the most magnificent enigma of international politics, the so called 'security dilemma'. The security dilemma is the outcome of the combination of the States tendencies that have been previously described. Specifically, 1) in an endeavor to attain sufficient security from a potential attack, nations are forced to acquire more capabilities as a way of evading the effects of capabilities of other nations (Baylis, 2001). 2) This makes other nations more insecure compelling them to prepare for any eventuality (Good, 1960; Burchill, 2005). 3) Since no single nation can feel entirely secure in the global environment that is filled with competing units, this competition guarantees a vicious circle of capability and security accumulation (Krahmann, 2005). 4) As countries compete for security, they realize varying levels of capabilities resulting to unequal distribution of capabilities across the units of global system. 5) Based on this perspective, the ranking of nations depends on the components of relative capability. 6) Consecutively, a moment arrives in which augmenting one's (state's) capabilities might well decrease its own security because of the increased fear (and immediate reactions) that the augmented capabilities will cause to the other States in the international system. The above analysis of the way these capabilities are distributed is generally formed in the Neorealism paradigm of international relations.

Another notion that is significant in our analysis is the notion of polarity that is also key to positioning national interests as illustrated in Neorealism theory. The polarity of the international system is influenced by how capabilities are distributed across units in a given time (Behr, 2010; Cowles, 2003). This approach further facilitates the separate typification of the given environment in the international system. Based on existing information about polarity, it is possible to distinguish between three forms of polarity, namely, unipolarity, bipolarity, and multipolarity (De Mesquita, 2006). Unipolarity exists when a single country in the system is superior in relation to other nations in terms of economic, demographic, technological, and military capabilities. The current state of international system tended/tends to be unipolar as the United States maintained and in many ways still maintains technological, economic, and military supremacy in the world. There are however opposing views that believe that our system is currently multi-polar. Bipolarity exists in situations where capabilities are distributed among two nations as illustrated during the cold war era where the United States and the Soviet Union represented the two poles of global power (Humphreys, 2007; Newman, 2010). Multipolarity on the other hand happens when more than just two nations possess equivalent relative capability. This was evident in the global system in the periods that followed the First and Second World Wars.

Having explained and elaborated on all the above concepts will hopefully help in illustrating the concept of national interest, which is admittedly elusive in nature. Some attempts to define what constitutes national interests arises from the previous descriptions of the current situation in the international system. For example, as countries strive for security, they seek to expand their capabilities to align with those of their rivals. Thus, it can be said that promoting economic, military and territorial security are key ingredients of what constitutes the national interests of a state (De Mesquita, 2006). At the same time, as we very explicitly illustrated above, the capability of a state as compared to others equips or constraints States to pursue such interests. Hence, it can be also concluded that the ambition and scope of a nation's interests are actually controlled by its capability levels (Krahmann, 2005).

Using the aforementioned attempted definition, within a neorealist conceptual framework, States national interests can be attempted to be understood when analyzed with reference to their capability ranking. In general, however, it has to be admitted that Waltz's consideration of national interests is rooted on the idea that national interests are taken as a given (Burchill, 2005; Houghton, 2007).

Consequently, when aspiring to attempt a comprehensive analysis of national interests within the Neorealist paradigm, questions that logically follows pertain to such things as the source of

national interests and the process through which these interests are formulated as well as the consideration of the motives of the actors behind actions they describe to be their actual national interests (Cox, 1981).

2.3 National Interests: A Historical Perspective

The concept of national interest has diverse interpretations among the theories of international politics. However, research studies published by Beard Charles in the early 20th century provides a clear picture of the roots of the concept of national interests as represented in various historical theoretical perspectives. According to Beard's publications, the concept of national interests as practiced in the United States is heavily influenced by the economic interests of various societies and groups in the nation (Németh, 2009; Goldsmith & Posner, 2005). These societies and groups focus on ensuring their specific interests forms part of the national interests of the country. He concluded that national interests are derived from particular group interests.

This conceptualization of national interests naturally goes against of core assumptions of the Neorealist paradigm of International Relations such as the identification of certain interests that transcend classes and specificities and thus form a unified, state-wide, conceptualization of the national interest. But in order to continue in the same vein as a historic analysis dictates and to clearly position the concept of national interests as illustrated by various studies that Beard conducted about the international politics of United States, we see that in those he demonstrated and affirmed that two major interest groups influenced the understanding of the concept of national interests in the United States (Németh, 2009; Adigbuo, 2007).

The first group assigned importance of the local development and market in the country's international relations. According to Beard, this group claimed that the United States needs to prosper locally to and should not be concerned about the rest of the world (Good, 1960). The other interest group were interested with international trade and manufacturers activities. This group argued that United States needed to care for international issues if they affected its safety and prosperity.

Following this particular conceptualization of national interests, it is needed to address the issue in a wider understanding and employment. In particular, if interests and ideas are reviewed as inseparable and interests are understood as entailing human interpretations and perceptions as research has also established (Pham, 2008), then this implies that interests have been found to not only be very subjective but also limited to specific social settings.

As Beard illustrated, interests are expressed through ideas which in most cases have material things in mind and are also linked to social relationships (Ikenberry, 2012). Consequently, by a historical point of view in might well be impossible to develop national interest from an objective point of view.

Furthermore, the contrast between interests and ideas that are nevertheless intertwined cannot be easily clarified, especially since both are necessary for any realistic view of global issues. Therefore, when interests are mentioned, the ideas attributed with the interests and their premises must be provided as well (Németh, 2009; Ray, 2003).

As much as these thoughts were developed over 50 years, before being revisited by constructivist and liberals in the 1990s, they have been vital in positioning the concept of national interests in international relation theories (Risse-Kappen, 1996). No matter the fact that the approach adopted by Beard in exploring the concept of national interests was historical and lacked a theoretical positioning (Checkel, 1998) it is of interest for this thesis to explore the concept of national interests even in that way so as to better demonstrate the contrast with specific reference to Neorealists' perspective.

2.4 National Interests: A Realist Perspective

2.4.1 Morgenthau and national interests

Morgenthau was focused on theorizing the sphere of international politics when he formulated the concept of national interests as the pole position of classical realism. This culminated to the emergence of the debate about the concept of national interests in the mid-20th century (Keohane, 1989). Morgenthau offered a summary of the fundamental principles of realism seeking a way of positioning and explaining away global politics.

According to Morgenthau, national interests are an instrument for researchers as well as a decision makers' guide on issues pertaining global relations (Hopf, 1998; Smith, 2000). This position was based on an assumption that objective laws influence international politics processes and are not dynamic. The aforementioned position is key to realist's approach to the study of the world. As Morgenthau supposed and tried to illustrate, objective laws emanate from human nature and the most significant law is that thoughts and actions of Statesmen are based on the interests that are defined as power (Ikenberry, 2012; Morgenthau, 1951).

This idea has been significant to realists while developing an understanding of international politics as well as during the formulation of theoretical postulations about international relations. Morgenthau affirms that interests as defined by power has been

significantly determinant of historical political decisions and actions making it not only an objective category but also universally valid. Thus, Morgenthau believes that interests as an idea is an essence of politics (Hollifield, 2000). However, the proposed resilient relationship between nation-state and interests cannot be assumed to last forever if one takes into consideration the context of historical occurrence it takes place in. It is therefore highly subjectable to change in the future when the significance of nation-States cannot be assumed to just continue to be same (Németh, 2009; Finnemore, 1996).

Consequently, what Morgenthau ultimately does is to raise the level of consideration of the fact that interests are inseparable from cultural and political context in which decisions on foreign policy are founded. Even though Morgenthau appreciates the imperativeness of cultural context, he as well just assumes that each nation clearly knows its interests. Therefore, according to Morgenthau every nation pursues its own interest through accumulation of power used in realization of said interests.

Based on this position, Morgenthau considers national interest to be non-problematic as a concept and does not provide information about the sources of these interests (Shell, 1995; Payne, 2007). However, several critics on Morgenthau postulations have emerged pointing out that developing an understanding of national interests based on this perspective does not provide an individual with information about the behavior of nations in international politics (Pham, 2008).

2.4.2 Waltz and national interests

As highlighted above, Waltz is among the founders of the paradigm of Neorealism. His research was based and developed on exploring the weaknesses of classical realists including Morgenthau. His criticism was founded on his very different take and very different key assumptions as compared to those postulated by Morgenthau (Waltz, 1996; Finnemore, 1996). Waltz argues that the classical realists were focused on interests, power, judgement of Statesman and human nature without exploring an international politics system inherently (Good, 1960; Pugh, 2004).

He States that Neorealists have been successful in addressing the limitations of classical realism by separating international and internal demesnes of politics. This made it possible for Waltz to formulate an international relations theory that explained away many occurrences that realism just assumed as self-explanatory. As Waltz affirms, Neorealism advances the idea of system structures which at an instant constraint the domains that learners of international politics struggle with by enabling them to visualize how a system structure and its internal

variations influence the interacting units and the results generated (Keohane, 1989; Copeland, 2000).

Waltz believes that an international system is decentralized and anarchic as illustrated above. This state of international system is based on the fact that international politics work in settings where the government and other agents that have system-wide authority are non-existent. In such a system the principle of self-help prevails making system units, which in this occasion are the States, to focus on promoting their individual survival (Taylor, 1992). Waltz postulates that survival is a precondition in the process of realization of all other objects of a nation making every nation to divert its efforts in defending its survival.

Accordingly, Neorealists' perspective of the concept of national interests is rooted in the survival of the state (Baylis et al., 2013). According to Waltz, the idea of a country acting in accordance to its national interests implies attempting to meet its security requirements after an analysis and assessment of the current situation. Based on this position, Waltz affirms that nations often formulate policies based on their current situation and implement their policies carefully to ensure their existence is not threatened (Waltz, 1996; Finnemore, 1996). Based on this perspective, Neorealists consider national interests to be actual products of the international system structure. Based on these reasoning, national interests for nation States are provided by the developments taking place at any given moment internationally wide and therefore it's not possible to enumerate basic principles from which they derive from, as postulated by Neorealists at least. Thus, from a neorealistic perspective, analysis of the approaches through which the national interests are achieved is the most interesting phenomenon (Guzman, 2002).

As much as this understanding of national interests is persuasive, it has been criticized to be very narrow in the sense that by being based on the survival of the state perspective, it is impractical to explain numerous issues that current international actors content with (Good, 1960). For example, this perspective does not provide explanations about disintegration of States and the role of international organizations and multinational companies in international politics. Consequently, this consideration of national interests as postulated by Neorealists is assumed by many not to be well developed to address the sophisticated nature of international relations and how they affect national interests (Keck & Sikkink, 1998). Thus, as a final attempt to comprehensively analyze the specific aspects of national interests as postulated by the Neorealist paradigm, it is important to examine the concept of power as well, as an aspect of national interests.

2.4.3 Mearsheimer and national interests

Mearsheimer perspective on the concept of national interests is an illustration of recent advancements of Neorealist perspectives on national interests (2001). His undertaking positions national interests with the emphasis on the focus on promoting the persistence of the state. Specifically, in his essay entitled "America Unhinged", which is well grounded in the Neorealist perspective, he emphasises on the imperativeness of focusing national interests on promoting security and sustainability though avoiding unnecessary international relations activities (Williams, 2005; Shain & Barth, 2003).

Specifically, Mearsheimer is frustrated by what he perceives as liberal imperialists and non-conservative hawks that dominate the United States foreign policy despite their various failures related to the decisions to go to war in the Middle East (2011). Mearsheimer proceeds to affirm that the United States unfounded claims of strategic aspects of countries is exposing the country to violence in the international relations; hence limiting its focus on its actual national interests which is protection of the country's security and economic interests in the global environment. Mearsheimer wrote this article when the United States was still deeply involved in internal affairs of Egypt and Syria with claims of these nations being vital to the United States national interests.

As Mearsheimer affirms, there is nothing essential in Egypt and Syria that United States cannot survive without. Clearly, Mearsheimer approach to Neorealism is rooted to restoring the paradigm of Neorealism in the development of strategic decisions involving international relations as it allows the events in the international environment to present national interests to the country and not the country to enforce its national interests in an environment that they are incompatible and unacceptable.

In general, Mearsheimer believes that the focus on liberalism in development of foreign policy in the United States has resulted to it implementing strategies that do not reflect their actual national interests in global affairs and ultimately tainting the image of the nation in international relations (Waltz, 2000; Rathbun, 2008). Consequently, Mearsheimer believes that as much as the United States has a history of successfully dealing with worst tyrants, it has never been threatened by anti-American populists as the current society imagines it to be.

According to him, a Neorealism's view of international relations is mainly dependent on geography which is vast in the United States and therefore threats that emanate from insignificant Middle Eastern political instability issues do not warrant to form part of the appropriation of national interests. Consequently, the meddling and overambitious foreign policy of the United States is more harmful to the country's political values and ultimate

national interests (O'Neill et al., 2004). Specifically, a nation that cultivates its national interest with the focus on lying to its citizens, the contempt of the rule of law, increasing secrecy and the massive invasion of privacy clearly illustrate reversed national interests that can be corrected if the Neorealists approach is considered in the country (Mearsheimer, 2013).

Based on the position taken by Mearsheimer, power is the most important factor in identifying national interests with relation to foreign policy. The ability of the United States to successfully manage the effects of the Cold War illustrated the success that can be attained if a nation's foreign policy can be centered on building its power (Sagan, 2012; Jørgensen, 2004). Recent efforts by the United States that have emphasized on demonstrating power rather than developing power have not been in the national interest of the nation as Mearsheimer postulates. Consequently, Neorealists have developed a strong link between power and national interests.

2.5 Comments and remarks

Throughout this chapter, the significance of each state's national interests has been highlighted. The main issue encountered is the lack of literature giving in-depth analysis of national interests. Even the lack of a commonly accepted definition adds to the complexity. On top of that, the cyber domain, with its special characteristics further adds to the complexity.

However, even though there is no commonly accepted way to define national interests, it does not mean that states do not project and protect them. It is anticipated that states protect vital national interests on cyberspace. In the authors firm belief that the neorealists approach towards national interest, will become the foundation upon the analytical norms for the correlation of national interest and cyberspace will be built.

3. National Paradigms

3.1 Introduction

This chapter aims at including examples from countries apart from those who are full member States of either the EU or NATO. The selection has been made on the basis of necessity, relativity and significance of an elaborate analysis for each example and has been based on the overall literature review completed by the researcher throughout the course of his studies in the MA program for which this thesis has been drafted. The main criteria taken into account are (Solana, 2003):

1) The characteristics of each nation state, including its geography, overall status as powers in their region, strategic importance and exposure to threat.
2) The legal, administrative and executive patterns and systems applied by the States that have been considered.
3) The level of risk for these countries and them being or not targets of transnational criminal and terrorist organizations which will mean that they will have to be forced to tackle an immediate and large-scale attack to their cyber-spaces.
4) Other relevant issues that are being faced by the societies of those member States that can impact the fight against terrorism, such as fundamentalism, social unrest, lack of democratization etc. (Yesilyurt, 2010)

Considering all the aforementioned areas, the dissertation shall focus on a critical analysis and review of four specific case studies, that will be used as typical examples of countries that fulfil all the above criteria and can add to the value of the paper. The core scope of this analytical critique is to identify the key priorities of countries that need to act individually and are neither neoliberal or forced to follow a "joint" approach with other countries, at least to the extent that EU-NATO members do and discuss the measures their governments have taken in order to protect their sovereignty and cyber-spaces, either proactively or in the wake of an attack (Conway, 2017). Those countries are: Belarus, Saudi Arabia, and Israel.

3.2 Belarus

In order for one to be able to elaborate on the Belarusian example as a case study, it would be crucial to begin by including some key introductory information on the country. According to the CIA World Factbook (Central Intelligence Agency), then, for 2018:

- Even though Belarus attained its sovereignty from the Soviet Union as early as in 1991, the process of stabilizing the institutions and ensuring the democratic function of its national institutions is still ongoing. Therefore, the country is considered the only non-liberal nation state in the European continent and has been the center of attention by international relations analysts and political leaders, international organizations, academics etc. for the past three decades.
- The government of the country tends, then, to use authoritative strategies to tackle its security issues and the people enjoy rights to a limited extent, only.
- Belarus is a land-locked country, located at a region of major strategic interest for the international society, sharing borders with both the EU and Russia, as well as major energy paths.
- Although, before 1990, the country has been rather well-developed when being part of the USSR, nowadays, it is less economically and technologically advanced than its neighbors in the Baltic region. The economy is highly nationalized and the government uses almost dictatoric mechanisms to control it.
- At the same time, the country is dependent to Russia for its energy imports and maintains, as a key national goal, to maintain its national sovereignty.

Cyber threat and cyber terrorism for Belarus are constant threats, as what happens in any other modern country. The fact that there is an extremely strict framework applied to ensure that all information published and shared by the mass media in the country, and that the communications in Belarus are monopolized by the public company "Beltelecom", it is clear that internet remains rather open and is more difficult to be monitored by the government (Ponomarev, 2010).

In particular, the Ministry of Communications (MIC), in collaboration with other stated owned companies and national institutions such as the State Center for Information Security (GCBI), Top Level Domain (TLD) and the Belarusian Domain Name Service (DNS) aim at fully monitoring all types of exchange of data and information and protect the national sovereignty, the interests of the States as well as the power of the authoritative government. Particular emphasis is being given at a national level at (Geers, 2011):

- Monitoring the elections and minimizing opposition through "muzzling" all alternative opinions. Particularly, on March 19th, 2006, the media have gone as far as to declare that Mr. A. Milinkevich, the opposition candidate, has died before the elections. During the same period, various websites have been made inaccessible to the public.

- The government systematically uses internet filters to maintain order and regulate the state.

However, the EU, as an organization that has been created with an aim to share liberal values in the continent, has not ignored Belarus from its agenda to tackle and repress cyber-threat and cyber-terrorism. On the contrary, the EU institutions and the leaders of its member States have been particularly clear about their position and have pointed out the need to democratize the Belarusian system. Also, it has been pointed out that, violating the right to freedom of expression and opinion in the country not only violates international law but, also, makes the country more likely to experience a wide national crisis due to the rise of radical political groups, fundamentalism or crime, as a response to governmental abuse of power and systematic suppression of the right of the citizens. Particular emphasis has been given on media liberalization and proliferation of internet usage as first steps towards an improvement of the situation in the country. However, Mr. A. Lukashenko, the "unofficial dictator" of Belarus since 1996 does not appear willing to comply with those strategies and recommendations (Bosse, 2009).

Geers (2011) has identified a number of key examples to discuss the development of cyber security and the role of the internet in the country, among which:

1) On September 9th, 2001, it has been revealed that Beltelecom systematically and officially blocked access to several political websites, making use of the, so-called Internet Service Provider's (ISP) network router, to censor information and communications. As a result, numerous other websites became unreachable and particular users (hackers) created "mirror" domains to allow citizens to reach the information available on those sites.

   This is a proof that, despite governmental efforts, Belarusian citizens still used internet as an alternative channel to access information and communicate in and outside the country's territory with other users and to express opinions and alternative views. Analysts and academics have used such proof as an indication that change might be possible in Belarus and that there is potential in the EU-Eastern partnership (Bosse et al, 2009).
2) On January 20th, 2004, the Distributed Denial of Service (DDoS) attacked the Belarusian cyber-space to locate various offensive websites, including networks associated with international crime and, i.e. trade of pornographic material, as well as activities taking place outside the country's borders. The DDoS compromised

more than 55.000 IP addresses, in a course of three weeks and, allegedly, accused persons for their involvement in trading child pornography or threatening the cyber-security of the country, with little or no proof at all. Many researchers criticized these actions as an attempt to abuse power in order to minimize opposition (Zhang et al, 2012).

3) On April 26th, 2008, several street protests took place in the capital of the country, with the citizens accusing the government for the lack of appropriate protection of their rights and data in online / digital spaces. That same day, the DDoS attacked open radio stations in the countries with attacks coming from computers outside the country, indicatively the Middle East and Asia. The size of the attack and the apparent lack of counter-mechanisms on behalf of the country to deal with the offenses effectively, revealed that the government was neither able or prepared to safeguard the sensitive data of the people and the companies operating in the country.
4) On the other hand, the, so-called "97 Charter", a pro-democratic website operating in Belarus with an aim to promote freedom of communication and expression ("Charter'97, n.d.), has managed to effectively counter a DDoS attack on it during June 8th, 2009 that took place during a tented period for the Russian-Belarusian relations. The technical staff of the Charter '97 neutralized the attack and proposed the "Free Internet" project to sufficiently tackle similar offences in the future ("Charter'97, n.d.).

3.3 Saudi Arabia

Cyber-threat and cyber-terrorism are problems faced not only by non-Muslim countries, as many assume. On the contrary, all countries, regardless of their political or administrative systems are potential targets of terrorist organizations and transnational criminal organizations. As a note, here, it must be then, added, that the theory of realism in international relation already clarifies that all nation States act as rational "players" in the international system and aim to promote their interests in order to maximize security and minimize exposure to risk. Therefore, it has to be made clear that, in any case, terrorism may use religion and ideology as "causes" but, in fact, their aims expand much further beyond those areas (Solansky et al, 2009).

Following the same pattern for the second case study, in this paper, as in the first (Belarus), when it comes to the country profile (Central Intelligence Agency, 2018):

- Saudi Arabia is not a liberal democracy. On the contrary, the country is governed by the male descendants of the Saudi (and Kuwait) royal family.
- The official religion of the country is Islam and the country follows the religious law, despite the fact that, during 2015, King Abdallah has made considerable efforts to modernize the legal and administrative system of Saudi Arabia.
- The country is one of the global leaders in the energy market, being very rich in resources.
- Also, it has a considerably high GDP per capita and is considered as a centre for business activity.

When it comes to indicative examples that can be included, in this part of the paper, to Geers (2011):

- The Saudi government uses arguments such as the need to protect the morality, the culture and social wellbeing of the citizens to justify the imposition of a firewall that forbids all users nation-wide to access websites that are considered to be potentially threatening to the interests of the state.
- The firewall bans the access of users to Internet Service Providers (ISPs), disrupts communications, monitors users' activity, censors material, forbids chatting and the distribution of pornography.
- Some partial progress has taken place since 1994, with the opening of the internet to websites that are not purely used for academic or research purposes.
- Even mail and transactions are monitored by the KACST, an institution that acts much like a national digital post-office, and even has access to passwords, personal data and communications, to fully control all users' activities.
- The KACST also uses an elaborate content-filtering system to apply a strict framework to locate potentially threatening content, such as offensive words and expressions.
- The Saudi government, when allowing the connection of the public to the internet in 1999, also created the "Secure Computing's software" that is called "SmartFilter" and is used to block more than twenty thousand (20.000) popular websites, including sites that are associated with pornography, gambling and online chat.

For the Saudi government, then, the following comments have to be made:

- the ideology and religion cannot be put aside. On the contrary, the country is administered using a rather "mixed system": on the one hand, male citizens are being granted a wide number of rights, and, on the other, there is an active firewall that exists and blocks "inappropriate" content and websites anywhere within the borders of the country (Geers, 2011).
- As a consequence, there is only partial freedom of expression and there is need for further liberalization and democratization of the country's institutions in order to protect the cyberspace and personal data of citizens. For the country, additionally, since it is one of the most competitive environments for the creation and expansion of multinational companies, activities and cooperation, it has to be made sure that
- Since Saudi Arabia borders countries in the Persian Gulf and the Middle East that face multiple crises, it has become one of the most active leaders of a 34-nation Islamic Coalition that was created in 2015, to tackle problems related to terrorism. Nowadays (June 2018), the Coalition includes 41 nations. Also, the country, since 2017, is part of the Global Center for Combatting Extremist Ideology (Etidal) following the initiative of King Salman that aims at reducing gender bias and has granted additional rights to women. These strategies have led to a further liberalization of the country.
- Saudi authorities distinguish between "passive" and "active" threats on their cyber-security. In particular, as "passive" they characterize propaganda and sabotage and as "active" terrorist and criminal activities. What is to be noted is that the county, since the 2013-2016 "heated" period of constant attacks, has managed to update its system and increasingly uses "soft power" to minimize threat (Madhian and Majed, 2017).

3.4 Israel

Again, using the information of the CIA World Factbook (Central Intelligence Agency, 2018), the following information can be included to create a short and comprehensive country profile for Israel:

- Israel, in its short history, has been part of several armed conflicts with neighboring countries such as Egypt (1979) and Jordan (1994) as well as the notorious conflict with Palestine, leading to severe loss of lives and wellbeing for the citizens.

- Israel owns important resources, making it a competitive actor in the international market and retains, therefore, despite the various problems related to under-productivity and low workforce, a rather important position in the international markets.
- Also, it is a regional power with one of the most equipped armies, applying a system of mandatory service in the army for all male and female adults, regardless of religion.

Coming, now, to an analysis of past, present and future threats for Israel, when it comes to cybersecurity:

- Israel is a country that has been created in the middle of the 20th c. in the aftermath of the second world war and has been widely accused of defying international law and using official state's propaganda to promote the national interests of the state. In particular, the international attention has been turned on the country, particularly to discuss how and why the country tries to censor material and to use its public diplomacy by supporting websites that use hate speech and offensive content to "win" the war against Palestine in Gaza. This means that Israel is both a target and an offender and special attention must be given in the analysis when it comes to this country (Saad, Bazan and Varin, 2011).
- Notably, two major attacks against the Israeli cyber-space have to be highlighted: the first regards an attack coming from various sides, located in the US, in 2016, targeting Israeli hospitals. Four hospitals have been attacked and important data have been exposed (Kuperwasser, 2017). According to reports of the Reuters, in 2018, there have been several efforts of international criminal and terrorist organizations to target the Israeli bank system. Among those, there have been cases of fishing, fraud and systematic attacks to the overall administrative and financial system of Israel, that aimed at proving the country's inability to protect its cyberspace, and, at the same time, lead to economic profit for the penetrators ("Cyber attacks on Israeli banks rose in last six months", 2018).
- Israel is one of the main targets of Hezbollah, a terrorist organization that openly declares as one of its main goals the destruction of the country. This means that there is high probability for it to become a key target of several individuals or groups of individuals or sister-organizations to Hezbollah. This entails a risk for the stability of the whole Middle East and, even, the international system itself. After all, the Israeli government has been allegedly linked with lobbies and elite parties

acting abroad such as in the USA, Canada, Australia, Germany and the UK. This means that the small country can, actually, disrupt the regional balance and, regardless of the outcome of a potential large-scale crisis, a power vacuum in the Middle East with unmeasurable consequences, will be created (Saad et al., 2011).

- The Israeli mass media are not completely uncensored or free. On the contrary, there have been allegations of the country using social and digital media to promote ideas related to Israeli revisionism, religious fundamentalism and motivation to hate (hate speech) against the Palestinian people. This means that the government, itself is, officially, accused for abusing the internet to manipulate public opinion and change perspectives for their own benefit (El Zein and Abusalem, 2015).
- "Op-Israel" is one of the most notorious examples of systematic attacks aimed at the cyberspace of a particular country and is not led by any particular group or individual. A massive attack took place during April 7th, 2013, at the same day that the world celebrated the Holocaust Remembrance Day, to target all types of state-monitored and administered websites, including educational, medical and commercial databases. This attack has been linked to the organization "Anonymous" but was supported by various groups at a global level. The government was warned before and there has been no physical damage. However, the attack has managed to disrupt the system of administration in Israel, caused public unrest and led to massive delays ("Anonymous launches massive cyber assault on Israel", 2013).

Responsible for the protection of the Israeli cyber-space is the state itself. In particular, Israel has prioritized cyber-security, recognizing the ever-evolving nature of the internet and the communications system. the main priorities of the country include (Kuperwasser, 2017):

- Limit the online propaganda used by terrorist through locating offensive content published on social media, particularly Twitter and Facebook.
- Use a wide variety of methods and mechanisms to further secure the national cyberspaces.
- Monitor the "jihadi chatters" and blogs to achieve an early prevention and countering of potential threats.
- Locate terrorists and potential offenders by systematically locating uses of specific vocabulary, and symbols and, then, identifying the user, using his or her IP to successfully prevent a terrorist act.
- Inform the public and disseminate information on cyber-security.

- Co-operate with other countries to further enhance protection.
- Use a robotic system to protect critical infrastructure and databases.

3.5 Comments and remarks

Having completed the analysis on the regulatory framework across the so-called "West" to tackle, repress and reduce cyber-attacks and cyber-terrorism, it has been made clear that, complex as it is, the problem of expansibility and constant magnification of international criminal networks that aim at terrorizing the public and disrupting public order, requires equally flexible and successful counter-measures. Particularly, it appears that international organizations such as the EU or NATO, are more competent to act against terrorist groups and threat of all types, including cyber- ones. This happens due to the fact that the member States are able to exchange know – how, infrastructure and technologies and increase their capabilities and defense against internal and external threat (Liang, 2015).

On the other hand, though, the researcher has also highlighted that, in several cases, it is required on behalf of specific nation States to take individual actions to protect their cyber-spaces. National databases, the personal data of citizens, the balance sheets of multinational companies as well as strategic plans and sensitive data, are among the most vulnerable types of information that the countries should be able to safeguard. Otherwise, the impact on the States will be major, with them experiencing a loss of status, power and credibility at an international level. Even worse, terrorist and criminal organizations can take advantage of the information they gain access to, to threaten the lives and wellbeing of the citizens and the function of the institutions. Most commonly, even if an attack is not specifically "terrorist", criminals, at an individual level or as part of groups, may sell the data to third parties and, therefore, the attacks can come from multiple sides and have similar outcomes (Ariely, 2007).

Through an elaborate discussion of the data and material related to the above, the following must be highlighted:

- The countries that have been studied still retain the ideology the governments used during the Cold War. This means that emphasis is given on foreclosure, retaliation and active protection. Thus, in several occasions, there have been minor or major violations of the international law at an official level to protect public safety and security (Hennesy, 2003).
- At the same time though, all those cases indicate that the countries seek to advance their technological systems and secure their cyber-spaces, realizing that the new types of threats, that include cyber-attacks, need a targeted intervention. This

includes constant training of staff, exchange of knowledge and expertise and cooperation with third countries (Posen, 2002).

- The priorities of the governments must and *do* include initiatives to plan counter-measures, coordinate actions, informing the public, doing forensic research, screen and search the cases and, engage at a systematic research to achieve maximum capability, adaptability and flexibility, as well as to intervene before the attack takes place (FEMA, 2016).
- Countering cyber-terrorism can become a complex political issue. Especially in non-liberal countries, ideology is used to promote stability and impose rule. Therefore, it must be made certain that the government does not suffer a loss of power as a consequence.

4. Supranational Paradigms

4.1 Introduction

The modern state, apart from the apparent problems with regard to the protection of its citizens against the infinite, uncontrollable internet, has more challenges to face in the present time of rising Islamophobia and due to the overall crisis, a crisis that does not only have to do with financial instabilities but is far deeper- a crisis of democracy and values. All those set an additional barrier in the efforts of protecting people and, especially, the country's wellbeing against all forms of cyber-crime (Marini, 2015). Some countries, such as the member States of the European Union, have tried to regulate their legislation and the treatment of cybercrime through a development of specific codes of conducts, setting strict framework with specific provisions against offences and defining terms widely used to describe crimes that take place in the digital environment, such as that of "cyber terrorism". However, the situation is particularly complex and, as such, so are the challenges that emerge in the process. The fact that efforts at a national level are unsystematic and lack strategic planning in combination with the other, most significant problem, of the impossibility of tackling cybercrime individually but only through tight international cooperation, further justify why the actions have no significant output. At the same time, increased awareness of the risks associated to the lack of cybersecurity and the wide of the internet raise public concern on the violation of, interestingly, not only their individual rights offended *when* offences occur but also about fact that, as part of the efforts of the state to protect them, their fundamental civil rights, such as that of freedom of expression are violated (Capon, 2015).

Ironically, despite prioritizing the tackling of cybercrime and systematizing efforts towards it, no universal definition of the term exists. Generally, academics tend to use various definitions- others too brief and others too extent. Of course, in the process of designing and implementing a specific strategy on behalf of States at either national or regional or international level, specific descriptions and explanations as to what each act covers *does* provide with an overall idea of how the term was conceptualized and on what it concerns. In that way, these descriptions can potentially be used, however, technically, the lack of a common international agreement acts as an additional barrier to the effective protection of what we call "cyberspace" in an adequate way (Kshetri, 2010).

Especially when it comes to particularly "sensitive" issues that involve issues such as hate speech and hate crime which require a specific politically incentive and include policy challenges that may reflect on the projection of a particular profile of a candidate and/of a party,

the situation become even more complex. In that respect, there is an observable unwillingness of leaders to engage in a systematic process to define, legislate, enact and apply strict rules and regulate offenses which could potentially threaten their public image or their relationship to elites (including lobbying) (Dodge & Kitchin, 2001). For instance, even in the same country and among US States, laws on cybercrime are applied to various degrees and citizens themselves as well as Institutions choose to respond in different ways to different challenges depending on the particular culture, traditions and priorities of each state. An indicative example can be drawn through investigating how "hate speech" and "harassment" in the internet is treated: California, as a state with a more "progressive" overall governance and culture applies strict rules and includes categories such as gender and sexuality ("U.S. hate-crimes bills/laws California law (Bill SB 1234)", n.d.) while others such Texas and, generally, the American South, having a certain past of bias and prejudice, are more inflexible and hesitant towards taking more effective action. This is a very complex political issue itself, as, as it can be realized, any politician who would like to go as candidate in a Southern state will take into account their "audience" (electoral base) and prioritize electoral success. As a result, they will try to avoid touching upon sensitive issues such as treatment of minorities and strict punishment against racist rhetoric (Carr, 2012).

One can only imagine what happens in international levels. To begin with, cyberspace is part of the ever-changing, constantly evolving digital environment that is the projection of the globalized society which is trying to discover new ways to incorporate external elements of different societies to be able to approach old notions in new manners. The very ideas and logic behind previously "fixed" terms such as "citizenship" and the very boundaries of the state, even the concept of what is the state, are contested in the cyberspace (Capello & Dentinho, 2012). OSCE further points out the complexity of the issues around the protection of cyberspace activities and defense against offenses and violations. In particular, clear mention is given on the risks related to the lack of common agreements and understanding between the States, a problem that further leads in miscalculations, administrative and operational incapabilities and hasten inter-state relations. The citizen is also particularly vulnerable in that process while lack of a common approach and defense strategy with clear calculations, common perceptions and co-operation at all levels can effect transnational relationships and create inter-state tensions (Organization for Security and Co-operation in Europe, 2016).

In that global, border-free, infinite, fictional "space" of the "cyberspace" human and civil rights are constantly threatened as, in reality, the human factor is always there and always absent (European Parliament, 2015). Because if the cyberspace is not a space then what is it?

The user, is immediately assumed to be a "human" being, but, is that always so? Hidden behind their anonymity, users can be both invisible and extremely apparent. Yet, it is important to take actions to protect that anonymity since it gives the internet its full potential- it allows for free speech and expression, accessibility and serve of a particular informative purpose (Kittichaisaree, 2017). That way, it is the responsibility of the State to take actual measures to protect *the user's anonymity* and the user from threats deriving *by anonymity*. As argued, this is impossible to be accomplished through isolated national initiative and requires multi-level international cooperation (Khosrowpour, 2000). This section will analyze exactly how, to what extend and through the use of which tools, regional and international organizations such as NATO, the EU and the UN act towards managing the effective defense of their Member-States' cyberspace.

4.2 United Nations

One of the first United Nation bodies to address the cyber domain was ECOSOC. In its first steps the committee's belief was that cybersecurity and cybercrime should be tackled through a close co-operation between the private and public sector including the participation of stakeholders who represent the civil society to achieve development through cooperation, training and awareness-raising. Also, ECOSOC identified several parameters that make cybersecurity a complex matter, including the need for a constant, rapid and immediate law enforcement, the role of economic inequalities and the lack of a coherent, commonly agreed strategy to prevent cybercriminal and to assist countries to create, as they called it "safe heavens" for developing countries. Especially in the area of protecting children against online crime, Ms. Deborah Taylor Tate, ITU Special Envoy and Laureate for Child Online Protection, made specific recommendations with regard to the need for applying a common strategy to provide children with the necessary tools, media literacy and protection to be able to safely join the "online world" ("Cybersecurity: A global issue demanding a global approach", 2011).

Despite their tendency to avoid actions on issues regarding "high politics" especially due to the need for a consensus and as they tend to "leave" such matters to the Security Council which has a more "military" scope than the majority of their organs, many UN Organizations have, actually, taken initiative in drafting, assisting in, educating about and enforcing regulations and mechanisms with regard to the protection of cyberspace. As a result, in their majority, the United Nations' activities in the field are fragmented and usually need to be approved by the General Assembly (UNGA) or the Security Council (SC). Especially the SC

has not yet passed any mandatory agreement on protecting the cyberspace of the UN member States (Maurer, 2011).

As a matter of fact:

- United Nations Economic and Social Council (ECOSOC) managed to raise awareness on cybersecurity through the organization of a Special Event on "Cybersecurity and Development in collaboration with the Department of Economic and Social Affairs (DESA) and the International Telecommunication Union (ITU) which gained significant attention due to it bringing together public and private sector organizations operating in several member States *and* the civil society. In collaboration with other UN organs it was successful in raising awareness, identifying best practices and talk about the future of cybercrime ("Informal Summary of the Special Event on Cybersecurity and Development", 2011).
- Despite the lack of binding resolutions, draft resolutions on cyber-defense have been passed to the UNGA for voting by the Disarmament and International Security Committee (First Committee), the Economic and Financial Committee (Second Committee) and the Social, Humanitarian and Cultural Committee (Third Committee).
- the First Committee, and, in particular, actors such as U.S., China and Russia have pushed towards the discussions on 'high end' of information security threats from 1998 onwards with actions such as the 2001 Resolution, that regarded the Russian proposal for the establishment of a specialized group of experts on governmental level. The group would include 15 experts from various States, chosen on the basis of their geographic position and would aim at a study to of threats in cyber-security and was called "GGE". The plan was rejected (Tikk, 2012). The GGE and its creation was proposed again in 2009 that resulted at a consensus report and agreeing on future cooperation and coordination, followed by the calling of a third GGE in 2011 with similar outcomes that further affirmed the need for application of international standards and law regarding the cyberspace, which was also followed by a fourth one which finished its tasks in 2015.
- The Second Committee made numerous efforts towards "pushing" the 'creation of a global culture of cybersecurity'. Theses led to the adoption of resolution 57/239 by the UNGA in 2003. The resolution aims at regulating and advancing the national information technology and its functions and includes nine (9) priority-areas:
    1. Awareness
    2. Responsibility

3. Response
4. Ethics
5. Democracy
6. Risk assessment
7. Security design and implementation
8. Security management
9. Reassessment (UNGA Resolution 57/239, 2003).

- The Third Committee of the GA focuses mainly on privacy rights, which proposed measures to tackle cybercrime with respect to privacy and people's rights, with two draft proposals leading to the adoption, for instance, of resolution 68/168 on 'The right to privacy in the digital age' (European Cyber Security Perspectives, 2015) and appointance of a new Special Rapporteur on the Right to Privacy.
- The UN Office on Drugs and Crime (UNODC) also takes initiatives on cybercrime and on ac common international response and has produced, among many, a report on cyber-related research and initiatives ("Comprehensive Study on Cybercrime", 2013).

The United Nations have made efforts for cybersecurity actions, however, we observe that even though they started very active and energetic, they went through a period were the UN didn't take any cyberspace initiative, and after that we go through a period where the UN is starting again to peak their efforts. This lack of continuity, as well as the lack of the lack of proper committees and bodies to tackle those issues have prevented the United Nations of achieving a major breakthrough regarding the cyber domain.

Concluding, the author agrees with the opinion of Chainoglou (2013, 204) that *"the development of any new body of law to address computer network attacks should be a matter for negotiation within the United Nations following a rigorous assessment of state practice in the field of cyber warfare".*

4.3 European Union

According to the official website of the Consilium, the EU has designed and has encouraged its member States to implement a specific "security strategy" to protect the States' and European (in general) telecommunications systems. The proposed strategy includes setting provision to enable a timely response to prevention against disruptions and attacks at the cyberspace. The digital agenda includes the protection of IT systems, of search engines and digital platforms, databases and business' information systems (including online payment services) and risk management ("Reform of cybersecurity in Europe", n.d.).

Cyber-security is also part of the EU efforts to ensure financial stability as it protects the online economy and its function and ensure the implementation of the common international strategy against cybercrime. The main aims, as specified, are to:

- increase cybersecurity and network security of the member States by implementing the NIS Directive.
- strengthen overall impact and capacities of the EU in the field of providing citizens, companies (SMEs included), the public rector etc. advantages and protection of rights (such as the right to privacy).
- mainstreaming the main aspirations and strategies (as well as best practices) of the Union and emphasize on the Internet of Things (IoT).

- develop public-private partnership while tackling problems and risks related to cybersecurity through the NIS Platform (networking).
- further engage in international activities such as working with the EU-US Working Group on Cybersecurity and Cybercrime,
- cooperate with:
  - the Organisation for Economic Co-operation and Development (OECD),
  - the United Nations General Assembly (UNGA),
  - the International Telecommunication Union (ITU),
  - the Organisation for Security and Co-operation in Europe (OSCE),
- join the World Summit on the Information Society (WSIS),
- take part in the Internet Governance Forum (IGF) ("Cybersecurity", n.d.).

The European Union has taken significant steps to set up the proper bodies and frameworks for cybersecurity. It has provided its Member-States with a plethora of tools but we observe that the states have huge differences among themselves when it comes to cyber awareness and cyber preparedness.

4.4 Organization for Security and Co-operation in Europe

Further systematic strategic planning on combating cyber-threat has been done at regional level through the Organization for Security and Co-operation in Europe, for its 57 member States. Their overall strategy, contrary to other similar initiatives such as that of the EU, is more crime-oriented, specifying and clearly stating that their aim is to tackle “cybercrimes and the use of the Internet for terrorist purposes” through creating tools and mechanisms such as the CBMs (Confidence Building Measures) ("Cyber/ICT Security", n.d.).

In detail, the main activities of the OSCE in establishing sufficient and suitable measures that would use international high standards in combating cybercrime and cyber-threat include:

- the implementation of "Decision No. 1202 on OSCE confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of information and communication technologies (ICTs)" (2016) which regulates:
    - Information sharing and exchange
    - Communication and dialogue
    - Future arrangements and things to consider
    - International and regional co-operation.
- the operation of a separate department specialized in ICT/cyber security. For OSCE, ICT (Information Communication Technologies) and the reduction of risks from their use for the participating States and their citizens, is one of the key priorities to achieve communication and cooperation as well as economic and social advancement and growth (Organization for Security and Co-operation in Europe, 2016).
- working close with other regional and international organization. For example, it maintains networks of communication with:
- the Council of Europe (CoE) in a Joint Expert Workshop in applying Council Decision no. 3/04 on "Combating the Use of the Internet and with regard to the "Convention on the Prevention of Terrorism" ("Responses to cyber terrorism", 2008).
- networking and common actions with other organs of the United Nations in order to achieve a better countering of terrorism (especially) and to incorporate other sections and sectors in a common strategic approach, as through co-operation with the Security Council of the UN with regard to the application of Regulation 1373 of 2001 and through the Action Against Terrorism Unit (ATU) within the Office on Drug and Crime of the UN (UNODC) (Tehrani, 2017).
- NATO, especially when it comes to cyber-attacks on particular member States' domains such as Estonia, and on relations with Russia and Ukraine (Tikk, 2010).

The prosperity that Europe has seen the last decades has almost eliminated the need for the Organization for Security and Cooperation in Europe. Without its core objectives being relevant anymore, OSCE has tried to reaffirm its mandate, pivoting to other areas of interest where the organization might be able to have a purpose once again. Whether this pivot will prove successful, remains to be seen.

4.5 Council of Europe

Further elaborating on regional efforts to tackle cybercrime, the Council of Europe (CoE) is one of the most active in not just drafting but actually enforcing acts and measures on tackling online threats. CoE follows the Common Standards set by the Budapest Convention on Cybercrime (2001) which aims to:

- align national and international efforts against cybercrime and cyberterrorism,
- improve existing techniques, mechanisms and methodologies,
- increase transnational cooperation,
- enhance the protection of the sovereignty of the member States,
- set up an applicable standard method of immediately tackling threat.

In addition, CoE, just like the OSCE and the EU, aims for the inclusion of further States despite them being or not its members, such as with the recent accession of Chile to the Convention (2017) or the collaboration with the United States of America (USA) in the project Cybercrime@Octopus (2017) initiatives that enhance international cooperation and a more coherent and targeted approach.

CoE also organizes and fully supports missions and activities, as well as funds specific projects in a variety of domains and regions with a focus on cybercrime, namely, and not exclusively:

- visits in countries in and outside Europe to promote the Budapest Convention and Cybercrime Convention Committee (T-CY), that have measurable effects on creating solid networks of cooperation and encouraging voluntary participation.
- the aforementioned Cybercrime@Octopus project, which also included, apart from the States that took part, Microsoft,
- iPROCEEDS a Joint project of the European Union which includes countries that are in a pre-accession phase and aim at a full EU membership,
- Eastern Partnership projects (Eastern Europe) like Cybercrime@EAP II and Cybercrime@EAP,
- the Global Action on Cybercrime (GLACY+).

The Council of Europe is yet another organization that seeks to reaffirm its mandate and that is the core driver for its cybersecurity involvement. However, the Budapest Convention on Cybercrime (2001) is one of the leading international documents that deals with this issue.

4.6 North Atlantic Treaty Organization

NATO is admittedly the most active in the field of cyber defense- first of all, collective defense against cyber-attacks is declared as one of its core tasks and also holds itself responsible for the protection of both its own networks and on assisting its member States in reinforcing their capabilities with regard to the protection of their own, national networks, in ways compatible with the methods introduced and used by NATO and with each other. Apart from practical methods of protection of the cyberspace against offenders and crime, the allies are also supported by NATO in further advancing with education, training, prevention and mutual assistance with regard to managing and protecting their cyberspace. NATO, as discussed, maintains vital and active networks of cooperation with other international and regional organization such as the CoE and the EU, recognizing the need for a common approach. Apart from that, specific mention is given to public-private cooperation and the need to include major enterprises ("Cyber defence", 2018).

That strategic focus is justified by the increased risks for the member States with regard to their military security, sovereignty and the need to tackle cybercrime in all its forms as a top priority issue that moves beyond the private domain (protection of intellectual rights and of personal data) which are commonly addressed by the EU (hard politics instead of soft politics). NATO has, indeed, moved towards a more "aggressive" response to what they call a "cyber-crisis" and tries to tackle the problems in their very roots as the Alliance considers cyber threat as a threat to the NATO itself and its function and operations (Fidler, Pregent & Vandurme, 2016).

NATO efforts on cyber security started as early as in 1999, before the majority of organizations began to even consider the potential importance and extent of the need for protection against "digital offences" but it was only after 2007 that it systematized its actions, due to attacks in Estonia that caused increased national and international concern on the vulnerability of the national information systems (Fidler et al., 2016). Since then, NATO continues to take over a variety of actions against cybercrime and provides with all sorts of measures- from training to information sharing, to military defense, storing of information etc (Healey & van Bochoven, 2011). The main policy areas are:

- the NATO Policy on Cyber Defence, endorsed in 2014, that aims to integrate an operational plan to increase awareness and training on processes with regard to cooperation and defense against cyber-attacks, including civil emergency strategic planning and prioritizing the safeguarding of communications systems' systems. The

Strategy is indicative of the main purposes of the Alliance and emphasizes on international cooperation, including state-enterprise common approaches.

- development of the allies' cyber defense capability through the NATO Computer Incident Response Capability (NCIRC), which is part of the Alliance's Smart Defence projects and includes exchange of information and of best practices among its member States.
- Increasing cyber defense capacities with further training of citizens on education, regular projects such as the Cyber Coalition Exercise, awareness-raising activities, the drafting of MOU (Memorandum of Understanding on Cyber Defence, consultation through common initiatives such as the NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE) and the NATO Communications and Information Systems School (NCISS) etc.
- Systematic cooperation with partners towards a common border defense to strengthen the works of the alliance and enhancing security on the basis of a common approach that reflects the mutual interests of the stakeholders.
- Cooperation with the private sector and industry to achieve cyber defense, especially with the NATO Industry Cyber Partnership (NIC), including Computer Emergency Response Teams (CERTs) in national levels and multinational Smart Defense Projects that involve industries ("Cyber defence", 2018).

NATO has been a pioneer regarding the level of involvement it has shown with the cyber domain. However, even though NATO is providing its Member-States with all the necessary information and training in order to adapt to the new challenges, it is observed that the level of cyber awareness is not harmonized with the alliance, as is the case with the European Union.

The author expects that especially due to the interconnection of systems and the ever increasing use of the cyber domain, NATO will push its members to adapt to those challenges. Otherwise security flaws in the infrastructure of Members-States, in addition to non-harmonized frameworks will significantly jeopardize the alliance's capabilities.

5. Conclusions

In the modern era cyberspace is going to become, sooner rather than later, the primary battlefield. The vulnerability of the internet, the reactive nature of cyber defense, the participation of non-state actors and the plausible deniability paint the modern strategic cyber landscape. As Geers (2014) notes "Nations today use computer network operations to defend sovereignty and to project power, and cyber conflicts may soon become the rule rather than the exception.".

States are, and will remain for the foreseeable future, the main actors responsible for countering those threats and providing a safer internet for their citizens. In order to do so, state institutions must adapt more swiftly to this new reality.

This dissertation examines the evolution of the concepts of sovereignty and national interest in cyberspace. Regarding the concept of sovereignty, we have seen that researchers have started to study the issue, especially after the publication of the Tallinn Manual 2.0. States start to include the cyber domain in their core documents, which signals a shift in traditional strategic thinking.

Regarding the concept of the national interest, there is hardly any literature, which means that there is an opportunity for a more in-depth research, regarding the traditional concept of national interest and how it is projected and protected on the cyber domain.

In the third chapter, the author has used the cases of Belarus, Saudi Arabia and Israel to show how sovereign States dealt with cyber issues threatening their sovereignty and national interests.

Finally, in the last chapter, this thesis examined how supranational organizations are actively involved in assisting their member States to develop the cyber capabilities they need. Furthermore, these organizations are actively pursuing the development of frameworks and the establishment of bodies within the organizations that tackle cyber issues.

The overlapping field between cyber space and international relations will become a major field of research in the coming years per this dissertation's conclusions.

6. References

Books

1. Baylis, J., Smith, S., & Owens, P. (Eds.). (2013). The globalization of world politics: an introduction to international relations. Oxford University Press.
2. Behr, H., (2010), A History of International Political Theory. Ontologies of the International, London/New York: Palgrave Macmillan.
3. Beitz, C. R. (1979). Political theory and international relations (Vol. 13). Princeton: Princeton University Press.
4. Burchill, S. (2005). The national interest in international relations theory. Palgrave Macmillan.
5. Capello, R., & Dentinho, T. (2012). Globalization Trends and Regional Development: Dynamics of FDI and Human Capital Flows. Cheltenham: Edward Elgar.
6. Chainoglou, K. (2013). An Assessment of Cyber Warfare Issues in Light of International Humanitarian Law. In R. Barnidge, *The Liberal Way of War: Legal Perspectives*. Routledge.
7. Chainoglou, K. (2016). Attribution Policy in Cyberwar. In J. Kulesza & R. Balleste, *Cybersecurity and Human Rights in the Age of Cyberveillance*. London: Rowman & Littlefield.
8. Dodge, M., & Kitchin, R. (2001). Mapping cyberspace. London: Routledge.
9. Finnemore, M. (1996). National interests in international society. Humphreys, A. R. C. (2007). Kenneth Waltz and the limits of explanatory theory in International Relations (Doctoral dissertation, University of Oxford).
10. Geers, Kenneth. Strategic cyber security. Kenneth Geers, 2011, p. 73-79.
11. Henessy. P. The secret state: Whitehall and the Cold War. Penguin Global, 2003.
12. IOS Press. (2008). Responses to cyber terrorism. In NATO Advanced Research Workshop on Responses to Cyber Terrorism. Amsterdam.
13. Jackson, R. H., Jackson, R., & Sørensen, G. (2012). Introduction to international relations: theories and approaches. Oxford University Press.
14. Keck, M. E., & Sikkink, K. (1998). Activists beyond borders: Advocacy networks in international politics (Vol. 6). Ithaca, NY: Cornell University Press.
15. Keohane, R. O. (1986). Neorealism and its critics. New York: Columbia University Press.

16. Keohane, R. O. (1989). International institutions and state power: Essays in international relations theory. Boulder: Westview Press.
17. Keohane, R. O., & Nye, J. S. (1977). Power and interdependence: World politics in transition. Boston: Little, Brown.
18. Khosrowpour, M. (2000). Challenges of Information Technology Management in the 21st Century. In Information Resources Management Association Conference. Igi Global.
19. Kittichaisaree, J. (2017). Public International Law of Cyberspace. Cham: Springer International.
20. Korab-Karpowicz, W. J. (2010). Political realism in international relations.
21. Kouskouvelis, I. (2007). Introduction to International Relations. Athens: POIOTITA.
22. Krasner, S. (1999). Sovereignty. Princeton: Princeton University Press.
23. Kshetri, N. (2010). The global cybercrime industry. Berlin: Springer.
24. Litsas, S. (2013). State and Sovereignty: Mythical Talos and the Politics of Conventional Rationality. In K. Lavdas, S. Litsas & D. Skiadas, Stateness and sovereign debt: Greece in the European conundrum. Plymouth: Lexington Books.
25. Maurer, T. (2011). Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security? [Ebook]. Cambridge, MA: Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf
26. Mearsheimer, J. J. (2001). The tragedy of Great Power politics. New York: Norton.
27. Mearsheimer, J. J. (2013). Why leaders lie: The truth about lying in international politics. New York: Oxford University Press.
28. Mearsheimer, J. J., & Walt, S. M. (2007). The Israel lobby and U.S. foreign policy. New York: Farrar, Straus and Giroux
29. Morgenthau, H. J. (1951). In defense of the national interest: A critical examination of American foreign policy. New York: Knopf.
30. Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek (TNO). (2015). European Cyber Security Perspectives [Ebook]. Retrieved from http://publications.tno.nl/publication/34616211/SyuTCF/european-2015-cyber.pdf
31. Németh, B. (2009). The Highly Important, Non-Existent National Interest (Doctoral Dissertation, Central European University).
32. Rittberger, V. (Ed.). (2001). German foreign policy since unification: theories and case studies. Manchester University Press.

33. Schmitt, M., & Vihul, L. (2018). Tallinn manual 2.0 on the international law applicable to cyber operations. Cambridge: Cambridge University Press.
34. Taylor, C. (1992). Explanation and practical reason (pp. 179-201). Springer Netherlands.
35. Tehrani, P. (2017). Cyberterrorism: The Legal and Enforcement Issues. World Scientific.
36. Tikk, E. (2012). Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012 [Ebook]. Geneva: ICT4Peace. Retrieved from https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf
37. Walker, R. B. (1993). Inside/outside: international relations as political theory (p. 2). Cambridge: Cambridge University Press.
38. Waltz, K. W., (1979). Theory of International Relations. Reading, Mass: Addison-Wesley
39. Weber, C. (2013). International Relations Theory 4th Edition: A Critical Introduction. Routledge.

Articles

1. Adigbuo, R. (2007). Beyond IR theories: The case for national role conceptions. Politikon, 34(1), 83-97.
2. Al-Rodhan, K. R. (2007). A critique of the China Threat theory: a systematic analysis. Asian Perspective, 41-66.
3. Ariely, Gil. "Knowledge management, terrorism, and cyber terrorism." Cyber warfare and cyber terrorism. IGI Global, 2007, pp. 7-16. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.670.9033&rep=rep1&type=pdf#page=40 [Accessed June 25th, 2018].
4. Banks, M. (1984). The evolution of international relations theory. Conflict in World Society: A new perspective on international relations, 3-21.
5. Barkdull, J., & Harris, P. G. (2002). Environmental change and foreign policy: a survey of theory. Global Environmental Politics, 2(2), 63-91.
6. Barnett, M. (2008). Social constructivism. The Globalization of World Politics, 3rd ed. (Oxford: Oxford University Press, 2005), 260.
7. Baylis, J. (2001). International and global security in the post-cold war era. The Globalization of World Politics, 253-276.

8. Behr, H., & Heath, A. (2009). Misreading in IR theory and ideology critique: Morgenthau, Waltz and neo-realism. Review of International Studies, 35(02), 327-349.
9. Bieler, A. (2001). Questioning cognitivism and constructivism in IR theory: reflections on the material structure of ideas. Politics, 21(2), 93-100.
10. Blyth, M. (2003). Structures do not come with an instruction sheet: Interests, ideas, and progress in political science. Perspective on Politics, 1(04), 695-706.
11. Bosse, Giselle, and Elena Korosteleva-Polglase. "Changing Belarus? The limits of EU governance in Eastern Europe and the promise of partnership." Cooperation and conflict 44.2, 2009, pp. 143-165.
12. Bosse, Giselle. "Challenges for EU governance through Neighbourhood Policy and Eastern Partnership: the values/security nexus in EU–Belarus relations." Contemporary Politics 15.2, 2009, pp. 215-227.
13. Burley, A. M. S. (1993). International law and international relations theory: a dual agenda. American Journal of International Law, 205-239.
14. Caporaso, J. A. (1992). International relations theory and multilateralism: the search for foundations. International Organization, 46(03), 599-632.
15. Chainoglou K. (2007). Reconceptualising Self-Defence in International Law, King's Law Journal, 18:1, 61-94
16. Checkel, J. T. (1998). The constructive turn in international relations theory. World politics, 50(02), 324-348.
17. Collard-Wexler, S. (2006). Integration under anarchy: neorealism and the European Union. European Journal of International Relations, 12(3), 397-432.
18. Conway, Maura. "Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research." Studies in Conflict & Terrorism 40.1., 2017, pp. 77-98.
19. Copeland, D. C. (2000). The constructivist challenge to structural realism: a review essay. International Security, 25(2), 187-212.
20. Cowles, M. G. (2003). Non-state actors and false dichotomies: reviewing IR/IPE approaches to European integration. Journal of European Public Policy,10(1), 102-120.
21. Cox, R. W. (1981). Social forces, states and world orders: beyond international relations theory. Millennium: journal of international studies, 10(2), 126-155.
22. De Mesquita, B. B. (2006). Game theory, political economy, and the evolving study of war and peace. American Political Science Review, 100(04), 637-642.

23. De Mesquita, B. B. (2006). Game theory, political economy, and the evolving study of war and peace. American Political Science Review, 100(04), 637-642.
24. Deutsch, K. W. (1968). The analysis of international relations (Vol. 12). Englewood Cliffs (NJ): Prentice-Hall.
25. El Zein, Hatem, and Ali Abusalem. "Social Media and War on Gaza: A Battle on Virtual Space to Galvanise Support and Falsify Israel Story.", 2015, available at https://www.researchgate.net/profile/Hatem_El_Zein/publication/305719299_Social_Media_and_War_on_Gaza_A_Battle_on_Virtual_Space_to_Galvanise_Support_and_Falsify_Israel_Story/links/579c088808ae80bf6ea346a1.pdf, [accessed June 25th, 2018].
26. Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations:(IR) relevant theory? International political science review, 27(3), 221-244.
27. Federal Emergency Management Agency (FEMA). (2016). National Prevention Framework. https://www.fema.gov/media-library-data/1466017209279-83b72d5959787995794c0874095500b1/National_Prevention_Framework2nd.pdf.. [accessed June 25th, 2018].
28. Ferguson, Y. H., & Mansbach, R. W. (2007). Post-internationalism and IR Theory. Millennium-Journal of International Studies, 35(3), 529-549.
29. Fidler, D., Pregent, R., & Vandurme, A. (2016). NATO, Cyber Defense, and International Law. Journal Of International And Comparative Law, 4(1).
30. Goldsmith, J. L., & Posner, E. A. (2005). The limits of international law (Vol. 199). Oxford: Oxford University Press.
31. Goldstein, A. (2007). Deterrence and security in the 21st century: China, Britain, France, and the enduring legacy of the nuclear revolution. LIT Verlag Münster.
32. Good, R. C. (1960). The National Interest and Political Realism: Niebuhr's "Debate" with Morgenthau and Kennan. The Journal of Politics, 22(04), 597-619.
33. Guzman, A. T. (2002). A compliance-based theory of international law. California Law Review, 1823-1887.
34. Hemmer, C., & Katzenstein, P. J. (2002). Why is there no NATO in Asia? Collective identity, regionalism, and the origins of multilateralism. International organization, 56(03), 575-607.
35. Hobson, J. M. (2001). The 'second state debate' in International Relations: theory turned upside-down. Review of international Studies, 27(03), 395-414.

36. Hollifield, J. F. (2000). The politics of international migration. Migration theory: Talking across disciplines, 137-85.
37. Hopf, T. (1998). The promise of constructivism in international relations theory. International security, 23(1), 171-200.
38. Houghton, D. P. (2007). Reinvigorating the study of foreign policy decision making: toward a constructivist approach. Foreign Policy Analysis, 3(1), 24-45.
39. Hyde-Price, A. (2006). 'Normative'power Europe: a realist critique. Journal of European public policy, 13(2), 217-234.
40. Ikenberry, G. J. (2012). Institutions, strategic restraint, and the persistence of American postwar order.
41. Jørgensen, K. E. (2004). European foreign policy: conceptualising the domain.Contemporary European foreign policy, 32-56.
42. Kowert, P. A. (2001). Toward a Constructivist Theory of Foreign Policy. Foreign policy in a constructed world, 4, 266.
43. Krahmann, E. (2005). American hegemony or global governance? Competing visions of international security. International Studies Review, 7(4), 531-545.
44. Kubálková, V. (2001). Foreign policy, international politics, and constructivism.Foreign policy in a constructed world, 4, 15.
45. Lake, D. A. (2007). The state and international relations. Available at SSRN 1004423.
46. Liang, Christina Schori. "Cyber Jihad: understanding and countering Islamic State propaganda." GSCP Policy Paper 2 (2015), p. 4.
47. Madhian, Bin, and M. Majed. Saudi Arabia's counterterrorism methods: A case study on homeland security. Diss. Monterey, California: Naval Postgraduate School, 2017, available at https://calhoun.nps.edu/bitstream/handle/10945/55569/17Jun_Binmadhian_Majed.pdf?sequence=1&isAllowed=y, [accessed June 24th, 2018].
48. Meyer, C. O. (2005). Convergence towards a European strategic culture? A constructivist framework for explaining changing norms. European Journal of International Relations, 11(4), 523-549.
49. Meyers, E. (2000). Theories of international immigration policy-A comparative analysis. International Migration Review, 1245-1282.
50. Newman, E. (2010). Critical human security studies. Review of International Studies, 36(01), 77-94.

51. Nielson, D. L., & Tierney, M. J. (2003). Delegation to international organizations: Agency theory and World Bank environmental reform. International organization, 57(02), 241-276.
52. Núñez, J. (2013). About the Impossibility of Absolute State Sovereignty. International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique, 27/4: 645-664.
53. O'Neill, K., Balsiger, J., &Van Deveer, S. D. (2004). Actors, norms, and impact: recent international cooperation theory and the influence of the agent-structure debate. Annu. Rev. Polit. Sci., 7, 149-175.
54. Payne, R. A. (2007). Neorealists as critical theorists: The purpose of foreign policy debate. Perspectives on Politics, 5(03), 503-514.
55. Pham, J. P. (2008). What Is in the National Interest? Hans Morgenthau's Realist Vision and American Foreign Policy. American foreign policy interests,30(5), 256-265.
56. Pollack, M. A. (2001). International relations theory and European integration. JCMS: Journal of Common Market Studies, 39(2), 221-244.
57. Ponomarev, A. (2010). A Critical Comparative Analysis of the President's Decree on Measures to Improve the Use of the National Segment of the Internet Network: The Case of Belarus, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1910189. [accessed June 24th, 2018].
58. Posen. B. R. The struggle against terrorism: Grand strategy, strategy, and tactics. International Security, 26. 3, 2002, pp. 39-55.
59. Pugh, M. (2004). Peacekeeping and critical theory. International peacekeeping,11(1), 39-58.
60. Rathbun, B. (2008). A rose by any other name: Neoclassical realism as the logical and necessary extension of structural realism. Security Studies, 17(2), 294-321.
61. Ray, J. L. (2003). A Lakatosian view of the democratic peace research program. Progress in international relations theory: Appraising the field, 205-43.
62. Reus-Smit, C. (2001). The strange death of liberal international theory. European Journal of International Law, 12(3), 573-594.
63. Risse-Kappen, T. (1996). Exploring the nature of the beast: international relations theory and comparative policy analysis meet the European Union. JCMS: Journal of Common Market Studies, 34(1), 53-80.
64. Rittberger, V. (2004). Approaches to the study of foreign policy.Derived from international relations theories.

65. Saad, Sabrine, Stephane Bazan, and Christophe Varin. "Asymmetric Cyber-warfare between Israel and Hezbollah: The Web as a new strategic battlefield.", 2011, pp. 1-4, available at: http://www.websci11.org/www.websci11.org/fileadmin/websci/Posters/96_paper.pdf, [accessed June 26th, 2018].
66. Sagan, S. D. (2012). Why do states build nuclear weapons? Three models in search of a bomb.
67. Shain, Y., & Barth, A. (2003). Diasporas and international relations theory. International organization, 57(03), 449-479.
68. Shell, G. R. (1995). Trade legalism and international relations theory: an analysis of the World Trade Organization. Duke Law Journal, 829-927.
69. Simmons, B. A., & Martin, L. L. (2002). International organizations and institutions. Handbook of international relations, 192-211.
70. Sjursen, H. (2006). What kind of power? Journal of European public policy,13(2), 169-181.
71. Slaughter, A. M., Tulumello, A. S., & Wood, S. (1998). International law and international relations theory: a new generation of interdisciplinary scholarship. American Journal of International Law, 367-397.
72. Smith, S. (2000). International theory and European integration. International Relations Theory and the Politics of European Integration: Power, Security, and Community, 33.
73. Snyder, G. H. (2002). Mearsheimer's World—Offensive Realism and the Struggle for Security: A Review Essay. International Security, 27(1), 149-173.
74. Snyman-Ferreira, MP. 2006, ' The evolution of state sovereignty: a historical overview' , Fundamina, vol. 12, no.2, pp. 1-28.
75. Solana, J. “A secure Europe in a better world: European Security stratefy. World Economy, Ecology and Development (WEED)”. Civilian Perspective or Security Strategy. icinde Klaus Schindler, Tobias v der Hauschild 2003. pp. 52 - 60.
76. Solansky, Stephanie T., and Tammy E. Beck. "Enhancing community safety and security through understanding interagency collaboration in cyber-terrorism exercises." Administration & Society 40.8, 2009, pp. 852-875. Available at http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.953.3246&rep=rep1&type=pdf, [accessed June 26th, 2018].
77. Sørensen, G. (2008). The case for combining material forces and ideas in the study of IR. European Journal of International Relations, 14(1), 5-32.

78. Taliaferro, J. W. (2006). Security seeking under anarchy: Defensive realism revisited.
79. Taliaferro, J. W. (2006). State building for future wars: Neoclassical realism and the resource-extractive state. Security Studies, 15(3), 464-495.
80. Telbami, S. (2002). Kenneth Waltz, neorealism, and foreign policy. Security Studies, 11(3), 158-170.
81. Tikk, E. (2010). Global Cybersecurity–Thinking About the Niche for NATO. SAIS Review of International Affairs 30(2), 105-119. Johns Hopkins University Press. Retrieved May 14, 2019, from Project MUSE database.
82. Waltz, K. N. (1996). International politics is not foreign policy. Security Studies,6(1), 54-57.
83. Waltz, K. N. (2000). Structural realism after the Cold War. International security, 25(1), 5-41.
84. Williams, M. C. (2004). Why ideas matter in international relations: Hans Morgenthau, classical realism, and the moral construction of power politics. International Organization, 58(04), 633-665.
85. Williams, M. C. (2005). What is the national interest? The neoconservative challenge in IR theory. European Journal of International Relations, 11(3), 307-337.
86. Wohlforth, W. C. (2008). Realism and foreign policy. Foreign Policy: Theories, Actors,
87. Zhang, Yanping, et al. "A survey of cybercrimes." Security and Communication Networks 5.4, 2012, pp. 422-437.
88. Zuhal Yesilyurt. G., The European Union at 50: Xenophobia, Islamophobia and the rise of the radical right. Journal of Muslim Minority Affairs, Vol. 30, No. 1, 2010, pp. 35-47.

Websites

1. Accession by Chile to the Budapest Convention on Cybercrime. (2017). Retrieved from https://www.coe.int/en/web/cybercrime/-/accession-by-chile-and-signature-to-the-budapest-convention-on-cybercrime
2. Anonymous launches massive cyber assault on Israel. (2013). Retrieved from: https://www.rt.com/news/opisrael-anonymous-final-warning-448/, [accessed June 25th, 2018].
3. Capon, F. (2015). Facebook's European Head Faces Investigation Over Hate Speech Claims. Retrieved from https://www.newsweek.com/germanyhate-speech-germanyanti-refugee-hate-speech-germanyasylum-seekers-596954

4. Carr, S. (2012). In Southern Towns, 'Segregation Academies' Are Still Going Strong. Retrieved from https://www.theatlantic.com/national/archive/2012/12/in-southern-towns-segregation-academies-are-still-going-strong/266207/
5. CIA World Factbook, Country Profile: Belarus, https://www.cia.gov/library/publications/the-world-factbook/geos/bo.html. [Accessed June 24th, 2018].
6. CIA World Factbook, Country Profile: Saudi Arabia, https://www.cia.gov/library/publications/the-world-factbook/geos/sa.html, [accessed June 23rd, 2018].
7. CIA, World Factbook, Country Profile: Israel. https://www.cia.gov/library/publications/the-world-factbook/geos/is.html, [accessed June 23rd, 2018].
8. Cyber attacks on Israeli banks rose in last six months. (2018). Retrieved from https://www.reuters.com/article/israel-cyber-cenbank/cyber-attacks-on-israeli-banks-rose-in-last-six-months-regulator-idUSL8N1PU09Y. [accessed June 25th, 2018].
9. Cyber defence. (2018). Retrieved from https://www.nato.int/cps/en/natohq/topics_78170.htm
10. Cyber/ICT Security. Retrieved from https://www.osce.org/secretariat/cyber-ict-security
11. Cybercrime@Octopus: Voluntary contribution by the USA. (2017). Retrieved from https://www.coe.int/en/web/cybercrime/-/cybercrime-octopus-voluntary-contribution-by-the-u-1
12. Cybersecurity. Retrieved from https://ec.europa.eu/digital-single-market/en/policies/cybersecurity
13. Cybersecurity: A global issue demanding a global approach. (2011). Retrieved from https://www.un.org/en/development/desa/news/ecosoc/cybersecurity-demands-global-approach.html
14. Informal Summary of the Special Event on Cybersecurity and Developement. (2011). Retrieved from http://www.un.org/en/ecosoc/cybersecurity/summary.pdf
15. Kuperwasser, Y. (2017). Cyber Terror and Security. Retrieved from http://jcpa.org/lessons-israels-response-terrorism/cyber-terror-security/ [accessed June 26th, 2018].
16. Marini, A. (2015). Totalitarian Legacy in the Refugee Crisis. Retrieved from http://www.euinside.eu/en/comments/refugees-ex-communist-countries

17. Official website: https://charter97.org/en/
18. Reform of cybersecurity in Europe. Retrieved from https://www.consilium.europa.eu/en/policies/cyber-security/
19. U.S. hate-crimes bills/laws California law (Bill SB 1234). Retrieved from http://www.religioustolerance.org/hom_hat11.htm

Other

1. European Parliament. (2001). Convention on Cybercrime. Budapest. Retrieved from http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf
2. European Parliament. (2015) The impact of the crisis on fundamental rights across Member States of the EU. Brussels: Committee on Civil Liberties, Justice and Home Affairs
3. Geers, K. (2014). Pandemonium: Nation States, National Security, and the Internet [Paper]. Tallinn: NATO Co-operative Cyber Defence Centre of Excellence. Retrieved from https://www.ccdcoe.org/uploads/2018/10/TP_01.pdf
4. Healey, J., & van Bochoven, L. (2011). NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow [Brief]. Washington: Atlantic Council. Retrieved from https://www.files.ethz.ch/isn/169072/022712_ACUS_NATOSmarter_IBM.pdf
5. Island of Palmas Case (or Miangas), United States v Netherlands (Permanent Court of Arbitration 1928).
6. Organization for Security and Co-operation in Europe. (2016). Decision No. 1202 on OSCE confidence-building measures (CBMs) to reduce the risks of conflict stemming from the use of information and communication technologies (ICTs). Permanent Council
7. Organization for Security and Co-operation in Europe. (2016). Factsheet on Cyber/ICT Security.
8. UNGA Resolution 57/239 on the "Creation of a Common Culture of Cybersecurity", adopted by the GA at 31st January 2003, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/UN_resolution_57_239.pdf.
9. United Nations. (2013). Comprehensive Study on Cybercrime. Vienna: Office on Drugs and Crime.