ŞHRMUN'24

UNSC

STUDY GUIDE

Cyber stability,conflict prevention and capacity building

USG; ELİF DENİZ URLU

#FORABETTERWORLD

Table of Contents

LETTER FROM THE SECRETARY GENERAL

Esteemed Participants and Respected Advisors,

Welcome to the Eskişehir Şehir Schools Model United Nations (ŞHRMUN) conference, happening this April at Eskişehir Şehir Schools. As Secretary-General, I'm honored to address you.

ŞHRMUN'24 is our second annual gathering, where students from around the world come together to explore diplomacy, international relations, and how the United Nations works. This year's theme, "For a Better World," aims to spark insightful discussions and find real solutions to global challenges.

Our committee sessions offer workshops led by experts in different fields, providing valuable insights and skills. We'll also delve into various global issues to enrich your understanding.

As we look forward to ŞHRMUN'24, I encourage you to prepare by researching your assigned countries and topics, learning the rules of procedure, and honing your speaking and negotiation skills. Your active participation is key to our success.

I'm excited for the lively discussions, meaningful connections, and memorable experiences that await us at ŞHRMUN'24. Let's seize this chance to inspire positive change and make a difference in our global community.

Warm regards,

Zeynep Turkurkor

Secretary-General

Eskişehir Şehir Schools Model United Nations

Letter from Under Secretary General

Welcome to Şehir College Model United Nations'24!!!

Your MUN Experience Awaits!

Dear Esteemed Delegates,

It is with great pleasure and enthusiasm that I extend a warm welcome to you as the Under-Secretary-General for Şehir College Model United Nations conference. As we embark on this exciting journey of diplomacy, collaboration, and impactful discussions, I am confident that this conference will be an unforgettable experience for each and every one of you.

Our dedicated team has been working tirelessly to ensure that this year's ŞHRMUN surpasses all expectations. From thought-provoking committees to engaging social events, we have crafted an agenda that promises a fulfilling and enriching experience for all participants.

Our team is here to support you throughout the conference, whether you have questions about committee procedures, need assistance with research, or simply want to connect with fellow delegates. We believe in creating an inclusive and collaborative environment that facilitates the exchange of ideas and perspectives.

I am confident that your dedication, passion, and diplomatic skills will contribute to the success of ŞHRMUN. Together, let us strive to make a positive impact and build lasting connections that extend beyond the confines of the conference room

Once again, welcome to Shrmun'24! Your journey with us begins now, and I look forward to witnessing the exceptional contributions each of you will make during this memorable conference.

Best regards,

Under-Secretary-General

Elif Deniz Urlu

Letter from Academic Assistant

Esteemed Delegates,

I sincerely welcome all participants of the Şehir College Model United Nations' Security Council. We are honoured to have you join us as we embark on a crucial journey to address challenges on cyber stability, conflict prevention and capacity building.

In this guide's first chapter "Introduction to the Committee," you will find information about the principles of the UNSC. The second chapter called "Preliminary Information and Key Concepts" on theoretical information that will help you understand the principles of the current international order—with respect to relevant IR concepts that are touched upon during the further discussion and analysis. Furthermore, in the third chapter "Cyber Stability, Conflict Prevention and Capacity Building," first, you will be introduced to the concept of warfare, information warfare and the principles of cyberwarfare. Understanding cyberwarfare is crucial for this agenda as it is the governing key concept. In order to do so, you are provided with a definition of cyberwarfare and some of the contemporary noteworthy examples of cyber operations. Which will lead you to the discussion on security and cyber security—most importantly the concept of deterrence and the international regime of law and institutions. Actors that partake in cyberspace are introduced as understanding their roles in the international order is significant, considering concerns over cyber terrorism as well—which are shown in three cases that changed the way cyber wars are perceived. Then, you will see that the concepts of cyber stability and capacity building are introduced, which are concepts that are interconnected and should be approached from both the theoretical perspective and by analysing real-life cases. The road to cyber stability: cyber conflict prevention and peace-keeping is discussed—concluding with past resolutions. In the last chapter "Questions to be Addressed" you will find the questions that will guide you through the course of the committee that needs to be discussed and eventually addressed.

I believe that this guide provides you with most of the significant information you need to know; nevertheless, cyberwarfare, cyber stability and cyber security are relatively new domains in the realm of IR, and is still developing and evolving—thus, further research and reading can always be done with regards to it, as this guide does not cover everything there is to know about the world. Nonetheless, a friendly reminder: the world is bigger than five.

Sincerely,

Academic Assistant

Mirata Deva

Letter from Academic Assistant

Esteemed delegates of SHRMUN24,

It is my honor to welcome you to the UN Security Council, dear diplomats of the future, great problem solvers, and peacekeepers. As one of the academic assistants of this committee, I can assure you that you are about to face numerous crises that will test your problem-solving skills and your ability to maintain peace by choosing the power of weapons over the power of diplomacy or vice versa. Before I leave you to delve into one of the most detailed and well-written study guides I have ever seen, I would like to express my gratitude to our precious Under Secretary General, Elif Deniz Urlu, for believing in me and supporting me throughout my chairboard career. I also want to thank Mirata Deva for his invaluable assistance during this process, and of course, our dear Secretary General, Zeynep Turkurkor, for bringing together such an outstanding academic team.

I am confident that you will all rise to the occasion and make this conference a resounding success. I look forward to seeing you all there.

Best regards,

Mine Çetinkaya

Introduction to the Committee

1. History of the United Nations Security Council

As World War 2 was about to end in 1945, representatives of 50 countries gathered at the United Nations Conference on International Organization in San Francisco, California to create a peaceful and new organization, the United Nations (UN).

"WE THE PEOPLES OF THE UNITED NATIONS determined to save succeeding generations from the scourge of war, which twice in our lifetime has brought untold sorrow to mankind, to unite our strength to maintain international peace and security, and to ensure, by the acceptance of principles and the institution of methods, that armed force shall not be used, save in the common interest."

The UN Charter establishes six principal organs of the UN: The General Assembly, the Security Council, the Economic and Social Council, the Trusteeship Council, the International Court of Justice, and the Secretariat. The Security Council is central to this architecture for international order.

The Charter grants the Security Council (UNSC) with an impressive range of powers and duties, most notably its primary responsibility for upholding international peace and security. Unlike the General Assembly, the Security Council can make decisions that are binding on all UN members.

2. The Functions and Powers of the UNSC

The Council, under the United Nations Charter, has various functions and powers. These include maintaining international peace and security under the principles and purposes of the United Nations, investigating any dispute or situation that might lead to international friction, recommending methods of resolving such disputes or the terms of settlement, formulating plans for the establishment of a system to regulate armaments, determining the existence of a threat to the peace or act of aggression, and recommending what action should be taken.

Additionally, the Council can call on Members to apply economic sanctions and other measures not involving the use of force to prevent or stop aggression, take military action against an aggressor, recommend the admission of new Members, exercise the trusteeship functions of the United Nations in "strategic areas," recommend to the General Assembly the appointment of the Secretary-General and, together with the Assembly, elect the Judges of the International Court of Justice.

According to Article 23 of the Charter, the Security Council shall consist of 15 members of the UN. Five of these members: China, France, Russia, the United Kingdom, and the United States, are permanent members, while the remaining ten are non-permanent members elected by the General Assembly for two-year terms. The current members of the UNSC, besides the P5, are as follows (with the end of

term year): Algeria (2025), Ecuador (2024), Guyana (2025), Japan (2024), Malta (2024), Mozambique (2024), Republic of Korea (2025), Sierra Leone (2025), Slovenia (2025), Switzerland (2024).

According to Article 27 of the Charter, each member shall have one vote and it requires decisions of the Security Council to be made by an affirmative vote of nine members (equals to a 3/5 majority). The Council's best-known provision is the veto power granted to each of the permanent members (P5), which means a resolution requires the concurring votes of all P5 members. In practice, this provision has been interpreted to mean that a P5 member has to vote against a resolution to veto it.

The Security Council is required to function continuously, whether at UN headquarters or elsewhere. It is free to establish subsidiary organs under Article 29 and to adopt its own rules of procedure under Article 30.

Articles 31 and 32 state that any member of the United Nations who is not part of the Security Council can participate in the discussion of any matter that the Security Council considers to be of particular interest to that member. However, they do not have the right to vote. Suppose a member of the United Nations who is not part of the Security Council is involved in a dispute under consideration by the Security Council. In that case, they can be invited to participate in the discussion about the dispute without the right to vote. The Security Council can establish conditions for the involvement of a state that is not a member of the United Nations, which it considers to be fair.

Preliminary Information and Key Concepts

1. State and Sovereignty

A state is not an equal of a nation, which is the collection of people who share a common culture, history and language, therefore a common national identity. Whereas, a state is a sovereign, territorial entity; inhabited by citizens and governed by national leaders, according to IR scholars. Political scientists argue that A state must be able to exercise internal and external sovereignty; its institutions being recognized as public institutions of the civil society; the state is the exerciser of domination and legitimation; and it is a territorial association. The state is the sole sovereign inside its territories, by definition, yet there are limits of the state exercising its legitimate power.

States by their political nature have the primary concern of establishing security in order to protect their sovereignty and this is the main interest of any and all state, according to Realists. States in foreign policy act according to their interests and engage with other states in *diplomatie publique*, trying to maximize their capacity and capabilities. As the state is an entity that is rationally guided and led by national leaders, national interests are concluded by a cost and benefit analysis. These national interests do not change over time or according to different governments, as they are permanent, which creates the *realpolitik*. States seek for balance of power, in which they often pursue to form and join into alliances to naturalize a possible threat by matching to its power as an alliance and try to promote collective security as the actors of international system. Yet, states in cooperation always worry about the relative gains, as they are concerned about what if the other party gains more advantages from this act of cooperation. Therefore, in interstate cooperation, two state in an agreement always try to gain more than the other, as it is not possible for one state to trust into another's intentions. Nevertheless, as a result of security dilemma, states can never trust or be sure of other states' intentions. Thus, state feels insecure and under a security threat, increase its capacity, build up army and form alliances to prevent getting invaded by another state, which causes other states to do same as well as they feel threatened. The result of security dilemma is power against power (or power balancing), in which individual states try to enhance their power by internal balancing[1] and external balancing[2].

Other than the internal political mechanisms, such as the constitution or regime of the country, there are international agreements that states are signatories or inter-governmental organizations (IGOs) that have binding effects which may shape and limit a state's sovereignty and the way it exercises its authority.

2. International Law and Organizations

One of the main purposes of international law and international institutions is the collective security; when a member state is under risk of invasion, other states go to rescue (such as NATO article 5) or apply collective punishments against the aggressor (economic sanctions). UN has two missions to protect peace: peace-making and peace-keeping. UN peace-making is the process in which UN takes effective role to prevent an outbreak of a conflict, it is done before the war—usually in the scenarios where there are tensions between two ethnic parties and a threat of civil war. UN peace-keeping is done by UN after a civil war, where UN meditates terms for a cease fire and sends a peace-keeping force to stand between warring parties, currently there are 18 missions in total, most of them in the Sub-Saharan Africa.

---

[1] **Internal Balancing:** A state increasing its own power resources—economic, technological, development in defence and military capabilities. (Like how Bismarck unified Germany under Prussia)

[2] **External Balancing:** States enter into security alliances with other states to counter rival and aggressor states.

From a liberal perspective, international law and organizations are significant as they help states to resolve the collective action dilemmas[3], that occur from mixed interests. States are rational actors and would like to maximize their gains, according to their own interest, and creating a platform where states can resolve their issues regarding to trust—transparency, eliminates the chaotic nature of the international system; increasing the collective good and everyone being better-off. The world of international institutions is based on cooperation, with significant incentives for compliance. On the contrary realists argue that international law and organizations are created by and reflect the interests of the powerful states.

International law specifies the rights and obligations states have with respect to other states, actors and their citizens; the universal international law generally applied in the international system is the "law of the UN", which is the UN Charter. In the international system, becoming a part of a "law" or treaty is completely voluntarily done, as there is no universal enforcement of law, unlike the domestic legal system of countries. There are different "islands" of international law that cover different topics, and are not coherently bind with a legal hierarchy—hierarchy of norms and do not intervene within each other's spheres of law. Unlike the Anglo-Saxon domestic legal system, in the international jurisdiction (with the exception of ICC) there is no "precedent decision" or referring back to previous cases. If one party wishes to sue another, the consent of the other part is required.

The effectiveness of international law and organizations are debated as participation, adherence and compliance with them is voluntary, and they do not have a binding effect; as there is no global enforcer of the law or a central enforcement (with exceptions such as the WTO)—as in the sense that not like the domestic system, and international security and peace is not compulsory especially for major powers, as they tend to break their own international law obligations (such as the illegal invasion of Iraq in 2003 by the US or Russia's invasion of Ukraine) and legitimacy issues, where some international institutions lose their legitimacy with humanitarian tragedies. Liberals argue that democratic states tend to comply and adhere more than the authoritarian states, as they have wider range of veto players in the domestic politics; democratic system requires more consent from the decision makers. An example to this can be given from Turkey, where the parliament is a veto power, and in order for Sweden's application to NATO to be accepted, it had to be voted in the parliament with a simple majority. Implementation and approval of agreements and legal decisions is harder in democratic states, however when its embraced, commitment to these treaties are more faithful; in authoritarian regimes, executives are unconstrained when it comes to non-compliance with international agreements.

International organizations become more effective over time and they provide monitoring in which every member state can monitor compliance, which resolves the security dilemmas. Nevertheless, realists argue that there are only two conditions where a state comply with the international law and treaties voluntarily. First possibility is that there has to be a situation where states are facing with a common enemy; where they form alliances and international organizations and make promises to each other, in this scenario they are more likely to comply and keep the promises made, for example formation of NATO against the Soviet threat. In the second scenario, there is a condition of hegemony, where there is a hegemonic power that creates a mechanism, and most of the time forces members, which is not voluntary in nature, for instance the Soviets creating the Warsaw Pact. According to the realists, great powers comply with the international law as they negotiate these laws to fit their own

[3] **Collective Action Dilemma:** Multiple actors that have relative gains ("selfish-interests") choose not to cooperate, but they are better of all together, as it maximizes gains for everyone. (See Game Theory "Prisoner's Dilemma").

national interests, and will therefore agree to accept its obligations; they create institutions to serve their interests and that why they comply with the decisions of this institutions.

2.1. Global Governance

> "In 1995, the UN Commission on Global Governance published its report (…). It constituted a platform of shared values for both reforming the international institutions (overall, the UN system) and strengthening the international rule of law, according to the liberal institutional perspective. Overall, a more inclusive and democratic form of global governance was envisioned.
>
> For Rittberger, 'global governance' is about transnational organizations, along with nation-states, as participating in the production of regulatory output. (…) Despite the differing interpretations of what global governance is, scholars agree that the modern state faces three challenges, as formulated by Held and McGrew: a 'political deficit' in democracy, regulation, and justice; new political energies and forces which are providing an impetus to the reconfiguration of political power; and a shift from national to cosmopolitan political and ethical frame of reference. Based on these, a "cosmopolitan institutional framework" for global governance is envisioned, where states hold a 'markedly diminished role in comparison with institutions and organizations of regional and global governance'" (Antonova 427-429).

3. Legitimate Use of Force (*Jus ad Bellum*)

The authorization of the UNSC is required for the legitimate use of military force, creating a *jus ad bellum*[4] basis for initiating war. For instance, during the Gulf War as a result of Saddam Hussein's invasion of Kuwait, UNSC authorized the use of force by the US. Nonetheless, during the US invasion of Iraq in 2003, the "evidence" presented by the US Secretary of State Colin Powell was the satellite images of mass destruction weapons made by the Saddam regime, led to the illegal occupation of Iraq by the US/UK coalition powers, in the name of "war on terror," without authorization from the UNSC. It was discovered that Colin Powell was lying at the UNSC about evidences, as there have been no weapons of mass destruction found. Another instance is the extensive use of veto power in the UNSC by Russia (and China, except most of the humanitarian issues) on the US drafts regarding the Syrian Civil War and vice versa, with Russia vetoing a total of 20 resolutions. Other than the UNSC authorized wars, humanitarian intervention and responsibility to protect are arguably cases of *jus ad bellum* as well.

4. Power, Types of Power and Authority

There is always an objective or a tangible outcome, and power in the its broadest sense is the ability to achieve that desired outcome. Power effects the decision-making process, as people who have power influence the process and content of decision. There are ways of influencing the decision-making process: "the use of force or intimidation (the stick), productive exchanges involving mutual gain (the deal), and the creation of obligations, loyalty and commitment (the kiss)" (Heywood 46). During the decision-making process, there is always agenda setting present as well. Agenda setting is the ability to prevent certain decision from being made by setting new agendas or changing the pressing issues, and offering alternatives to the existing decisions. Power is also the ability to influence others and as a form of indoctrination or psychological control, being able to shape what one thinks, and used specifically and intentionally for ideological reasons—as a form of thought control.

---

[4] **Jus ad bellum:** is the right to war, and defines what constitutes as just/legitimate war.

Authority is the legitimate power—"whereas power is the ability to influence the behaviour of others, authority is the right to do so" (Heywood 37). Max Weber talks about three types of authority: traditional, charismatic and legal-rational. In international relations, it one wishes to influence others, their authority's base should be legal and rational, therefore legitimate, taking its power from legal and rational sources. Therefore, authority is based on an acknowledged duty to obey.

4.1. Hard Power:

This type of power is based on resources such as military power, force, sanctions, intimidation, payments and bribes. This type of power makes a state able to achieve its goals via means that create a sense of superiority or subduing others, with a combination of economic and military power. Furthermore, theorist Joseph Nye suggests that others' behaviours can be affected by "inducements ('carrots') or threats ('sticks')" (5). In the basic force model of power, military capacity enables a state to be able to protect its territories and citizens from other aggressor states and be able to pursue its national interests outside its sovereign territories via conquest, expansion or invasion. Therefore, military capability: the size, quality, equipment and means of the armed forces is crucial.

4.2. Soft Power:

This type of power is the "co-optive power" which is the ability to shape others preferences by attraction, rather than coercion as Nye suggests. Soft power largely operates through "three resources: its culture (in places where it is attractive to others), its political values (when it lives up to them at home and abroad), and its foreign policies (when they are seen as legitimate and having moral authority.)" (Nye 11). One example can be the 'American Dream' which had effects all over the world that spread through American cultural influence via Hollywood. Soft power is the ability to influence and effectively determine what others think, want, need and prefer—aligning them with the state's best interest and benefits.

4.3. Smart Power:

Smart power is the combined use of hard and soft power—employment of strategies regarding diplomacy, persuasion and capacity building.

Looking at contemporary political developments around the world, it could be said that the usage of hard power is in decline, owing to the great powers' willingness to avoid direct confrontation, with total war being out of the question. Nonetheless, Russia used hard power in 2022 with its invasion of Ukraine, proving that hard power is still a relevant concept. Soft power is often used by culture giants of the world that produce variety of goods ranging from TV series to artists—the US, Japan, South Korea and China are some of the dominant producers of such goods.

5. Instruments of Foreign Policy

States use strategies to achieve their national interests—strategy is the totality of objectives and instruments designed and divided based on the means available. There can be long-term, short-run or grand strategies to achieve economic, financial or military goals.

5.1. Coercive Instruments:

Economic Sanctions: has the goal of leading a change in the behaviour of a target state's foreign policy. There are various ways a state might press economic sanctions, such as trade restrictions—restricting a country's access to another's market, embargo on goods, financial sanctions and asset freezes.

Covert Operations: are secret operations conducted in foreign territories without letting the target country know.

Propaganda: is the selective use of information or misinformation to effect the target country's foreign policy.

Military Force: is the use of armed forces to engage in direct confrontation, no longer seeking for peaceful means for conflict resolution.

Cyber-Operations: targets the digital infrastructure of a state, with the use of manipulation of information in internet and media to effect foreign policy.

Coercive Diplomacy: happens when the diplomats clearly conceive the message that if the target country does not change their foreign policy, there will be harsh consequences.

5.2 Persuasive Instruments:

Persuasion is to convince or induce things so that the other party can change their behaviour. *Diplomacy:* is to achieve foreign policy goals without going to a war or getting involved in any conflict but use peaceful instruments and benefit from diplomatic expertise.

Economic Incentives: is offered by governments to a country to convince them to a certain path of foreign policy—great powers are often the most persuasive as to what they can offer. The main goal is to lead the target country act in a certain foreign policy path that is 'friendly' and beneficial for the interests of the sender country. Economic incentives can be offered through foreign aid mechanisms and institutions, financial aids and economic agreements or it might be conditional—countries have expectations, and attach certain conditions to the economic or diplomatic relationship they will create.

Cyber Stability, Conflict Prevention and Capacity Building

1. Warfare and Types of Warfare

The clash of interest of states causes conflict due to the nature of the international system. War, in its most generic sense, is an armed conflict—a confrontation and violent meeting of forces, between two or more actors and is goal-oriented, with the objective of winning. With the fall of empires in the 20th century, wars evolved to be fought for national independence. In the modern 21st century, the concept of total war became almost non-existent, with the Cold War becoming the new norm. In the post-Cold War world order, new types and strategies for warfare developed, alongside technology, creating varieties of new methods to be used to achieve the ultimate goal of being victorious.

1.1. Total War:

States mobilize all of its resources to engage in military conflict with the enemy, with the objective of winning the war. The state sees the other parties as the foe or the enemy, with no intention of peace.

1.2. The Cold War:

After World War II, the new bipolar world order, having left the old continental European centre of power behind, was shaped between the USA and Soviet Union, ultimately becoming a clash of ideologies between capitalism-liberalism versus communism, fought mostly in proxy wars and regional conflicts, with no "hot war" between these two super powers.

1.3. Guerrilla War:

Instead of a total war fought between two nation states and their standing army, Guerrilla War is fought between armed groups and the sovereign nation state's army—usually in geographically strategic positions that would favour the smaller unorganized armed groups.

1.4. Civil War:

War implodes internally—within the boundaries of the state, creating armed conflict between politically organized armed groups that used to be a part of the state, competing for sovereignty, on the basis of which party is more powerful.

1.5. Terrorism:

Terrorism is an act of violence or aggression, specifically targeting the civilian population, with the intention of giving harm. Constitutionally, states have the right to identify which political groups are considered terrorists, with a proper justification—any groups that threaten the integrity and stability of the state or the state sovereignty.

2. Information Warfare

In the 21st century, information warfare is extremely influential with vast resources and availability and abundance of resources, with the knowledge being easily reachable. However, control over this information and knowledge, proves to been beneficial for states' national interests as well, since it is the usage of soft power to manipulate information to fit in with various agendas.

> "Rather than give a definition of information warfare, Libicki suggested that the term must be broken down into smaller parts to become understandable and meaningful. He therefore described seven forms of information warfare, shown in Table 1.
>
> As can be seen by Libicki's thoughts on information warfare, the term is extremely broad. It can include denying battlefield commanders information, keeping sensitive messages secret, spreading propaganda, traditional hacking and so on.

Table 1 – Libicki's seven forms of information warfare (Libicki, August 1995).

Form	Description
Command-and-control	Attacks on command centres, or commanders themselves to disrupt command effectiveness
Intelligence-based	Increasing your own situational awareness while reducing your opponent's
Electronic	Use of cryptography and degrading the physical basis for transferring information (e.g. radar jamming)
Psychological	Use of information against the human mind. Propaganda to demoralise troops or influence civilian populations
Hacker	Exploitation of viruses, logic bombs and trojan horses to attack computer systems
Economic information	Possessing and being in control of information leads to power
Cyber	Information terrorism, semantic attack, simula-warfare, Gibson-warfare

Dorothy Denning provides an alternative definition of information warfare, stating that it 'consists of offensive and defensive operations against information resources of a winlose nature'. From Denning's perspective information warfare can be seen as a game, played between defenders and attackers who are in direct competition. Defenders perform defensive operations to protect information in any form, seeking to maintain its confidentiality, integrity and availability. Attackers perform offensive operations, seeking to damage that confidentiality, integrity and availability. Denning argues that information warfare can occur in a number of domains such as crime, individual rights and national security. Similar to Libicki, the description of information warfare offered by Denning is broad. Kopp states that the aim of information warfare is to: 'corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity and availability of one's own information'.

Taking these definitions of information warfare, it is clear that the term can be used to describe a very wide range of activities that include but also go beyond cyber space. The question of whether cyber warfare is simply a form of information warfare is unclear" (Robinson et al. 72).

3. Defining Cyberwarfare

Cyber war is "the use of digital or network-based technology to disrupt the activities of a state or organization, usually for strategic or military purposes" (Heywood 713). Cyber operations can be an example to smart power as the usage of both soft and hard power is possible. Often cyberwarfare is used as a means of coercion, with the threat of destruction of technological infrastructure of a target state or leak of governmental data to the public. Naturally, coercive diplomacy is also a part of this process, with the party that conducted the cyber-attack using the leaked information as a leverage and means to force the hand of the target government to follow policies in their own interests. Propaganda and cyber-attacks are usually seen to be used together, with the data and information gathered from cyber operations used as means for propaganda to influence the general public or politicians' decision making process to shape the foreign policy of the target country. Therefore, it is possible to state that cyberwarfare is an example to usage of smart power, and combination of usage of various coercive instruments of foreign policy. Therefore, cyberwarfare is a technological and informational warfare, that is to happen in the cyberspace[5].

[5] **Cyberspace:** "(…) cyberspace is more than just computers and digital information, and that there are four aspects of cyberspace that a definition should reflect:

- An operational space—People and organisations use cyberspace to act and create effects, either solely in cyberspace or across into other domains.
- A natural domain—Cyberspace is a natural domain, made up of electromagnetic activity and entered using electronic technology.

"The term cyber warfare is one that is used in mainstream media and as with information warfare, there are many differing definitions. In 2001, Alford defined cyber warfare as:

'Any act intended to compel an opponent to fulfil our national will, executed against the software controlling processes within an opponent's system.'

This definition from Alford reflects the view that cyber warfare is something that states will engage in to advance a national agenda. It can be argued, however, that modern warfare does not always aim to advance such an agenda. Religious beliefs and ideologies that are not tied to a national agenda can arguably be the aim of modern warfare. It therefore seems unwise to confine a definition of cyber warfare to having the purpose of advancing a national will.

Jeffrey Carr offers another definition of cyber warfare:

'Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood.'

In comparison to Alford's, this definition avoids attempting to define the motivation of the fighting parties. However, the suggestion that cyber warfare will not spill blood must be questioned. A cyber-attack on critical national infrastructure, such as the power grid may result in loss of life. Colarik and Janczewski agree with this point, arguing that cyber warfare cannot be seen as bloodless. (…)

Arquilla and Ronfeldt do not define cyber warfare, but instead offer a definition of cyberwar: 'Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the balance of information and knowledge in one's favour, especially if the balance of forces is not. It means using knowledge so that less capital and labour may have to be expended'

Arquilla and Ronfeldt see cyberwar as a battle for control over information and communication flows, with the ultimate aim developing an advantage over an opponent. In this respect, there are similarities with the ideas of information warfare. The definition does however face the same challenge as Carr's, in that attacks intended to cause physical damage are not accounted for.

Another definition of cyber warfare is put forward by Cornish et al.: 'Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target

---

- Information based—People enter cyberspace to create, store, modify, exchange and exploit information.
- Interconnected networks—The existence of connections allowing electromagnetic activity to carry information.

To reflect these four aspects, Kuehl offers his own definition of cyberspace: 'A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies'" (Robinson et al. 71-72).

could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target.'

This definition raises the idea that non-state actors may be involved in cyber warfare, an interesting idea that other definitions miss. The use of 'can be', 'could' and 'various ways' make it a general definition that would benefit from being more distinct. It also highlights that cyber warfare may be unpredictable and imprecise in its effects e an idea that is missing from other definitions" (Robinson et al. 72-73).

4. Cyberwarfare and Cyber Operations

Developing technology has eventually caused cyberwarfare to become a new area for states to compete over superiority, and has introduced new strategic vulnerabilities that non-state actors endeavour to exploit and leverage. Targets of cyber-attacks include states, businesses and social media platforms. The number of cyber-attacks targeting governments has seen a significant increase in the past years. "In just one of those data breaches, almost 14 million records of current and former government employees, including their social security numbers, were obtained. The Director of U.S. National Intelligence has labelled cybercrime the top threat to U.S. national security—ahead of physical weapons and terrorism" (Atrews 18).

Some weapons and means used in war are often at the monopoly of the state—such as nuclear weapons (ICBMs). Nevertheless, even though such resources are reserved for state use, non-state actors may possess the capability to utilize means typically exclusive to the state, like military force—in the form of unorganized armed forces or guerrilla tactics—to pursue their interests. However, their resources are limited and often cannot compete with the sovereign state's power and capacities. Yet, cyberwarfare diverges from these traditional methods due to the accessibility and availability of the tools required to conduct such harmful actions. Thus, cyberwarfare is not only a means used in wars but is also accessible to private individuals—who might not be considered non-state actors with set agendas but use it as a way of moneymaking or blackmailing. Therefore, many states categorize cyber operations as not only a form of cyberwarfare but also a type of cybercrime.

It could be said that -unofficially- there is a consensus that cyber operations that target the state and government facilities are means of cyberwarfare and occur as a result of political agendas and interests, whereas ones that target businesses are cybercrimes with financial aims. "Cybercrime in the U.S. has led to annual losses of nearly $300 billion, whereas estimates for worldwide losses have been in the range of 1 percent of global income. To combat this growing threat and mitigate losses, organizations will spend more than $101 billion on cybersecurity in 2018" (Atrews 18). On the other hand, social media is often the target of cyber-attacks as it is easy to reach to targets using these platforms. Spread of misinformation using social media platforms is an important and widely used as a means in information warfare and a tool for propaganda, making it the centre of cyberwarfare targeting the general public.

There are key defining factors of the cyber world and cyber operations, which are basic principles[6] that could be applied to various cases:

"*Lack of Physical Limitations*

Physical limitations of distance and space do not apply in the cyberworld. In cyberspace, physical distance is neither an obstacle nor an enabler to conducting attacks. A cyberattack can be executed with equal effectiveness from the other side of the Earth as

[6] Further reading can be done on the article called "Principles of Cyberwarfare" doi: 10.1109/MSP.2011.138.

from the next room. In kinetic warfare, attacks are carried out by physical objects that must traverse a distance. (…)

Kinetic Effects

Cyberwarfare must have kinetic-world effects. It is meaningless unless it affects someone or something in the real world. Cyberwarfare can directly affect objects in the physical world, such as the opening of a dam spill-gate or shutdown of an electrical substation. Cyberwarfare in its most subtle form can affect the minds of decision-makers. (…)

Stealth

People can take active steps to hide in the cyberworld, but everything we do is visible. The question is whether someone is looking in the right place at the right time. The cyberworld is an artificial one, created by human beings using hardware and software. Any actions combatants take in that world require data movement or manipulation—some bit in some data stream is changed to reflect their presence and actions. (…)

Mutability and Inconsistency

In the cyberworld, nothing can be taken for granted in this way. The cyberworld, as an artificial construct built by humans, is imperfect. It can and does change in ways that seem chaotic. (…)

Identity and Privileges

Most of the steps in any cyberwarfare attack are intended to simply assume the identity of the entity that can perform the desired action. (…)

Dual Use

Attackers and defenders in cyberwarfare use the same tools. Attackers use vulnerability scanners to look for exploit opportunities as part of an attack. Defenders use the same vulnerability scanners to look for weaknesses in their own systems. (…)

Infrastructure Control

This means that neither the attacker nor defender controls 90 percent of the infrastructure used in the course of its activities. Thus, both parties are vulnerable to attacks on third-party infrastructure. (…)

Information as Operational Environment

In cyberwarfare, it's the information itself that constitutes JIPOE[7]. The communication connections, computer network maps, personnel rosters, websites, links, emails, postings, and every other aspect of the target is already information in cyberspace—there's no conversion from physical measurements to information" (Parks et al. 32-34).

4.1. Cyberwarfare Attacks, Operations and Systems

The number of cyber-attacks and operations have been rising and expanding their ranges from simple hacking to cyberespionage. These are some of the contemporary cyberwarfare systems that are noteworthy:

[7] Joint information preparation of the operational environment

4.1.1. Flame

Flame, also known as Flamer, sKyWiper, or Skywiper, emerged around 2010 as a sophisticated cyber weapon attributed to Israel, aimed at spying on computers across the Middle East, notably in Iran. With capabilities for taking remote screenshots, audio recording, keylogging, and data erasure, it demonstrated advanced cyberespionage functionalities. Its discovery followed anomalies in data handling on infected systems, revealing its complex nature distinct yet related to Stuxnet, suggesting a nation-state's involvement. In 2014, Flame 2.0 appeared with enhanced encryption, complicating analysis. It shared roots with Stuxnet, and despite efforts to eradicate it, Flame 2.0 showed resilience and innovation in cyber warfare techniques (Atrews 19-20).

4.1.2. Disttrack/Shamoon

Disttrack, or Shamoon, likely originating from Iranian cyber efforts, first appeared in 2012, targeting the Middle Eastern oil and gas sectors, notably Saudi Aramco, erasing data on tens of thousands of systems. It resurfaced in 2016 and 2018, targeting various entities within the energy sector, showing enhanced capabilities in data destruction and spreading. Its evolution demonstrated continued threats to global energy infrastructure with sophisticated, destructive cyberattacks (Atrews 20-21).

4.1.3. DarkHotel

Active since 2007, DarkHotel has targeted guests in luxury Asian hotels, expanding its operations globally. Utilizing spear-phishing and P2P attacks, it has compromised high-profile individuals through exploiting zero-day vulnerabilities, indicating possible nation-state backing. Its methods have evolved, focusing on political figures with refined social engineering and malware deployment strategies (Atrews 21-22).

4.1.4. Equation Group

Linked to Stuxnet and Flame, the Equation Group has been known for its sophisticated cyber arsenal, capable of infiltrating and persisting on targeted systems, including rewriting hard drive firmware. Its tools facilitate data exfiltration and surveillance across various sectors worldwide, highlighting advanced capabilities likely backed by a nation-state (Atrews 22).

4.1.5. Duqu

Duqu malware, associated with high-level geopolitical espionage, initially targeted international security meetings. Its evolution to Duqu 1.5 showcased increased sophistication in delivery mechanisms and command execution, underscoring ongoing advancements in cyber espionage tools (Atrews 22-23).

4.1.6. Snake

In 2020, cybersecurity experts identified a new ransomware, named Snake by ICS security firm Otorio, believed to have originated in Iran. This ransomware encrypts files and programs, targeting specifically those involved in industrial control systems, effectively halting manufacturing processes by encrypting vital operational data and erasing backups. Initial assessments pointed to Iran as the source, though further investigations suggested Russian hackers might have executed the attacks while posing as Iranian to misdirect blame. Further research is required to conclusively identify the perpetrators (Atrews 23).

5. Impacts of Cyberwarfare and Cyber Security

Nations states realize the effectiveness and importance of cyberwarfare in the international arena and therefore unable to ignore the threats it creates both internally and externally. In terms of politics, leaders and intelligence agencies of nation states participate in cyber-war-making to protect their national security, gain intelligence on their rivals via cyberespionage and to protect their national

interests and prestige. One example to this is when "U.S. President Barack Obama addressed North Korea's alleged hacking of Sony Picture Studio in anticipation of Sony's release of a film depicting the assassination of North Korea's leader, Kim Jong Un" (Atrews 24). With the growth of cyberwarfare as a new sector of war making, states and national leaders are ought to build-up their cyber arsenals and capabilities.

Nonetheless, the reach of cyberwarfare is not limited with political conflicts as the economic effect of cyberattacks and cyber-crimes is estimated to be way more destructive. "In a study conducted by McAfee, it was estimated that global cybercrime has cost the world's economy an estimated $600 billion; 0.8 percent of global Gross Domestic Product (GDP) is lost every year. (…) In the U.S., cybercrime has cost the U.S. economy between $24 to $120 billion (USD) annually, which is approximately 0.2% to 0.8% of the U.S. GDP" (Atrews 24). In a globalized world with growing interdependence of economies, the financial and economic effects of cyber-attacks seem to be prior to political interests—the MNCs that dominate the global economy are *de facto* more effective than the national leaders.

6. Security and Cyber Security

In foreign relations, states seek to achieve their interests, maximize their capacity, and ensure their national security. Therefore, their actions reflect the principle of *Raison d'État*, as they pursue international policies that primarily serve their benefit, with security being of the utmost importance. Joseph Nye defines security as "the absence of threat to core values. Security involves many dimensions beyond just the absence of physical damage or bodily harm. It means the ability to live by constitutional and humanitarian values that are central to our identity. Fear can lead us to damage those values" (Valdés-Ugalde 198).

> "The International Telecommunications Union (ITU) defines cyber security as follows:
>
> Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:
>
> - Availability
> - Integrity, which may include authenticity and nonrepudiation
> - Confidentiality" (Von Solms et al. 97-98).

6.1. Issues Regarding the Definition of Cyber Security

> "Notably, none of the resolutions discussed in the UNGA contained precise reference to what it is to be understood by cybersecurity. Though present in other documents issued by the UNGA or other UN bodies, security in the cyberspace did not come to be defined until the issuing of ITU's 'Overview of cybersecurity'. One important event preceding this document was the distributed denial of service (DDoS) attacks that paralyzed Estonia for three weeks, between 27 April and 18 May 2007, which may have precipitated the introduction of an operational definition. The 'Overview of cybersecurity', which was approved on 18 April 2008 by ITU-T Study Group 17, also contains a taxonomy of the security threats from an organization point of view.

> Accordingly, cybersecurity was understood as 'the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets', and this was officially acknowledged for further incorporation in activities pertaining to the building of confidence and security in the use of ICTs in the 2010 ITU Resolution 181. This document acknowledges that 'the definition of cybersecurity may need to be modified from time to time to reflect changes in policy'" (Radu 12-13).

6.2. Deterrence and Cyber Security

Traditional or classic deterrence is based on traditional military capacity; army, air force and navy, used for deterring any attack on the territories of the state. Nuclear weapons, on the other hand, are a different kind of deterrent—they are not used in warfare as the purpose of a nuclear weapon is not to use it, and rather pursue a policy of deterrence or threat of retaliation. States use nuclear retaliation to deter any attack to itself. An important concept of nuclear deterrence is "mutually assured destruction," which is the understanding that no state can win a nuclear war as it has heavy costs, meaning that if a nuclear war happens between two nuclear states, it will destroy both of them. Stability is established in the international system by the possession of nuclear weapons by the superpowers, and their nuclear capability.

> "Today, in the arena of cybersecurity, scholars have begun to consider whether the strategies used for nuclear weapon deterrence might apply to the present conflict in order to fill the gap betwee3n real cyber situations and academic research. This concept derives from the idea that any country that possesses a weapon, they are able to come under the control of an enemy, which ensures the security of the country, an idea born during the Cold War. (…) In deterrence theory, global political stability can be accomplished because countries know that the costs of using nuclear weapons are greater than the gains. In addition, the idea of mutually assured destruction serves as a base for the offense-defence theory, which is an essential Defensive Realist theory. Defensive Realism argues that nations support the status quo to maximize the power of their political and military forces. For alliances, a nuclear umbrella is a safeguard against a non-nuclear allied state. The core idea of deterrence theory is that nations should prepare for threats and defend their allies. Despite the problem that the origin of a cyberattack cannot be known for certain because of the use of Tor, which is an anonymous modification application that disguises IP addresses, the core idea of nuclear deterrence remains the same for cyber deterrence. In both the theories of deterrence, mutually assured destruction serves as a base for the offense-defence theory, smaller allied countries can receive benefits by depending on big countries and all cooperate to ensure the safety of cyberspace: cyber-developed countries engage in capacity building for the sake of less developed countries. (…) This desire to deter is a result of feeling threatened. Countries that foresee the possibility of the compromising or even destruction of their infrastructure or financial institutions or fear cyberwar ally with one another to prepare for such attacks" (Watanabe 226).11

6.3. International Legal Regimes and Institutional Frameworks

Since the Cold War's end, cyber-threats have emerged as a concern in global security, rivalling the significance of nuclear weapons. Nations now prioritize cybersecurity (CS) following the growing cyber-attacks and crimes, leading to international efforts and frameworks aimed at mitigating these risks. The 2001 Council of Europe Convention on Cybercrime (CoECoC), effective from 2004, symbolizes

such collective action, garnering widespread support. Despite these initiatives—including contributions from the UN, the Internet Governance Forum (IGF), which is a UN-mandated global multi-stakeholder policy forum, the International Telecommunication Union (ITU), which is a UN specialized agency dealing with information and communication technology issues, the Internet Corporation for Assigned Names and Numbers (ICANN), regional development and security organizations such as the Shanghai Cooperation Organization (SCO), and the Association of Southeast Asian Nations (ASEAN)—the development of effective international cybercrime laws and frameworks is still in its early stages (Kshetri 53-54). The need for international norms and *corpus juris* remains active in the international community.

> "The CoECoC is the only multilateral treaty focusing purely on cybercrimes. As of December 2014, 44 countries had signed as well as ratified the Convention in accordance with their national constitutional or legal requirements, making it enforceable. Nine additional countries had signed the CoECoC but had not ratified. Some argue that a key problem of the CoECoC is that it has adopted vague definitions of cybercrime and related concepts that are subject to different interpretations by different states. Many nations that have ratified the CoECoC have done so under a number of reservations. (…) All these have reduced the scope of cybercrimes covered by the Treaty and led to obligations that are less demanding and lack uniformity across countries. A National Research Council study concluded: '[A] signatory nation may decline to cooperate with its obligations under the convention on fairly broad grounds, and the convention lacks an enforcement mechanism to assure that signatories will indeed cooperate in accordance with their obligations.'
>
> Nations have also relied on the global intergovernmental organizations such as the UN to address cybercrime related issues. For instance, in the first meeting of the Intergovernmental Group of Experts of the UN Crime Prevention and Criminal Justice Program held in January 2011, the Chinese delegation, citing statistics of the China Ministry of Public Security, complained that the country was suffering from foreign-originated cyber-attacks. (…)
>
> Formal standards-setting international institutions such as the ITU have also become a venue where these issues are being discussed and debated. For instance, while governments of the U.S. and the EU economies have argued that the ICANN[8] should continue to be the central organization, governments of some of the major economies such as China, Brazil, South Africa, India and several Middle Eastern economies such as

[8] "The ICANN is governed by US laws and is accountable to the US Department of Commerce asper agreement. However, it is not merely the technical infrastructure of the domain name system (DNS) that ICANN operates. It also formulates policies on the type of new top-level domains, the registries and their operations, copyright issues, privacy issues, cyber security and a whole range of other issues. It is a transnational institution—a private one—that not only operates the technical infrastructure but also makes policies that are in the sovereign domain of nations.
Many nation states have long been sceptical of ICANN's autonomy. Initial calls for the democratisation of global internet governance were made at the World Summit on Information Society (WSIS) in 2005. The Tunis Agenda that emerged out of these discussions mandated that the 'international management of the Internet should be multilateral, transparent and democratic'. But the Internet Governance Forum (IGF)set up on the recommendation of the Working Group on Internet Governance (WGIG)has proved to be ineffective. At the same time, internet governance is being increasingly discussed in other international forums such as World Conference on International Telecommunications (WCIT) by International Telecommunication Union (ITU), and World Telecommunication Policy Forum (WTPF) by Internet Society (ISOC)" (Bajaj 583).

Iran and Saudi Arabia want to move the internet management system under the ITU. The economies in the latter group also want to define Internet governance more broadly to include issues such as spam and illegal content as opposed to the ICANN's narrow technical mandate, management of the DNS. Since the ICANN is a U.S.-based organization, many governments do not like the fact that ICANN's central role in governance would put the U.S. in a position of power to regulate and oversee the Internet. These governments think that the U.S. may have exploited its advantage to create Internet malware such as Flame and Stuxnet, which attacked sovereign nations. In the World Conference on International Telecommunications (WCIT-12) was convened by the ITU in December 2012 to amend the International Telecommunication Regulations (ITRs) treaty, which was adopted 56 3 Cybersecurity in National Security and International Relations in 1988. Of the 144 countries with the voting rights at the WCIT-12, 89 countries signed the revised ITRs, which included many countries in Africa and the Middle East, Brazil, Mexico, Argentina, China, Indonesia, Iran, and Russia. Fifty-five countries including Australia, India, EU members, Canada, Japan, and the U.S. did not sign the treaty (ITU 2012). The U.S. considered the ITU and the ITRs as inappropriate international institutions for dealing with CS issues.

New regional multilateral exclusive groupings established for politico-security arrangements such as the SCO have also dealt with CS. The SCO economies' approach to CS differs in several important and fundamental ways from the CoECoC signatory countries. The two groups differ in the definition and assessment of the scope of the problem. One such difference is that SCO economies consider it important to focus on the broader problem of information security rather than the narrower CS. In 2008, the SCO Agreement in the field of International Information Security emphasized on and expressed concerns about the 'digital gap' between the West and the East. These economies have been particularly concerned about the West's' monopolization in ICT products such as software and hardware and less developed countries' dependence on the West.

Finally, military, political and economic organizations such as the North Atlantic Treaty Organization (NATO), the EU, the Organization for Economic Co-operation and Development (OECD), the ASEAN and Asia Pacific Economic Cooperation (APEC) have also addressed CS issues. For instance, in an attempt to enhance the NATO's cyber defense capability, the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) was established in 2008. As of April 2014, sponsoring Nations of the NATO CCD COE included Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, the Netherlands and the U.S.

The U.S. and EU countries have also established deep and strong collaborations and partnerships. For instance, the Italy-based European Electronic Crimes Task Force, which has dedicated personnel from the countries involved to investigate and prosecute cybercrimes, provides a forum for law enforcement agencies, the private sector, and academia from the U.S. and EU nations. In the same vein, a virtual forum for ASEAN CS is being formed to develop a common framework to coordinate exchange of information, establishment of standards and cooperation among enforcement agencies" (Kshetri 56-57).

6.3.1. Strategic Policy Decisions

Regarding different issues in the global political order, members of the international community either follow the flow of the international decision-making process and ratify treaties, agreements and conventions, or decide to remain outside the existing international order and the world making process **(Table 1)**.

Table 1: "Strategic responses to cybercrimes, cyber-attacks and cyber-warfare involving economies with different categories of relationships" (Kshetri 64)

Nature of relationship	Some examples	Strategic responses
A. Membership in formal multilateral frameworks related to CS (e.g., CoECoC)	Signatories of CoECoC	• Local capacity building and institutional development
Lack of membership in formal multilateral frameworks related to CS		
B. Cooperative, strong, close, favorable and stable diplomatic and economic ties	Relationships of most CoECoC signatories with India and Indonesia	• Local capacity building and institutional development • Harnessing the power of successful regional organizations that are internally cohesive and have security as a key focus • Providing opportunities for developing economies' voice and participation.
C. Formal diplomatic and economic ties characterized by periodic tension and distrust	China-U.S. Russia-U.S.	• Working on areas of common interests • Help and encouragement to integrate with the West • Establishment of a high level working group made up of policy makers • A 'bricolage' approach to CS
D. No formal diplomatic and economic ties	U.S.-North Korea U.S.-Iran Japan- North Korea	• Development of offensive and defensive capabilities tailored to specific threats.

6.3.2. Criticism of the International Regime

Many states criticize the CoECoC for being western-centric and argue that the definitions it provides on cybercrime and cybersecurity is neither enough nor satisfactory—especially the BRICS states being non-signatories, limits its effectiveness and widespread acceptance as the global norm on cybersecurity matters. Some of the mechanisms of the convention is also a concern as of its violations of national sovereignty and security. In international law, the principle of *Égalité Souveraine* holds that all states have equal sovereign rights. Thus, since it is argued that the convention serves the interests of the Global North and violates the sovereign rights of the states of the Global South—this is the reason for developing countries and BRICS states rather not to sign the treaty. Nevertheless, it has been observed that even countries that have ratified the CoECoC have not been able to prevent cyberattacks originating from their territories, nor have they been successful in controlling, convicting, and prosecuting those responsible for such cybercrimes.

> "The need for democratisation of internet governance has been re-ignited by the PRISM programme revelations that social media servers that are predominantly located in the US expose the data of global users to US surveillance. (…)
>
> India's proposal for a Committee on Internet Related Protocol (CIRP) in June 2011 and the Shanghai Cooperation Agreement promoted by China and Russia have created a degree of consensus in the GGE that existing international law applies to cyberspace with regard to: critical infrastructure protection; the rights of states and human rights going together, with privacy of citizens being part of their human rights; nations using non-state actors to launch cyber-attacks against others; and capacity building to help less developed nations. This debate started afresh after the Snowden revelations. (…)
>
> The multi-stakeholder model promises participation of governments, their respective agencies within the UN, users, civil society and technicians, as well as academia and corporates. It sounds similar to the present multi-stakeholder model, except that the ICANN will be Geneva based, just like the ISOC, and the IANA function will not be under US government alone. It amounts to taking a UN approach, without being the UN. Any talk of multilateralism and internationalisation instead of 'multi-stakeholderism' and globalisation is, however, frowned upon. Obviously, the status quoists are pushing hard

to retain control over sovereign policymaking, through the mechanism of making the say of all stakeholders on a par with sovereign governments. (…)

Some of these issues were discussed in the EastWest Institute (EWI) Cybersecurity Summit held at Stanford University from November 4–6, 2013. It was acknowledged that there is presently a lack of trust in the US global leadership of the internet. A Strategic Analysis specific suggestion made by a senior Hoover Fellow was that the US should limit itself to solving specific problems and not address all dimensions such as freedom of expression and content regulation. Cyberspace has to include the countries that do not have the same level of freedom as the US. (…) There is a need to develop cyber security standards and implement and monitor them, to criminalise certain activities and prosecute the criminals. Cyberspace requires treaties that are similar to those related to finance and energy." (Bajaj 584-586).

7. Actors of Cyberspace, Cybersecurity and Cyberwarfare

Especially in contemporary issues regarding modern problems, it is not possible to talk only about the importance of the state as the only actor in IR that is able to influence the international system and world making process. Non-state actors are increasingly influential, as liberalists suggest, in cyber issues as well. Therefore, the responsibilities and consensus of states is not enough to neither control the international cyber regime nor prevent cyberwarfare and cybercrimes. An international legal document or institution with such aim, must take into consideration the role non-state actors and other stakeholders play. Starting from 2002, UN resolutions, international treaties and organizations are aiming to increase their capacity to include all possible actors in the process of cyber conflict prevention and other hostile cyber activities.

"Partakers in the cyberspace are explicitly identified and mentioned in the following order: 'Governments, businesses, other organizations and individual users who develop, own, provide, manage, service and use information systems and networks ('participants').

Once identified, the partakers are also attributed responsibility; according to the 2002 Resolution, the participants 'must assume responsibility for and take steps to enhance the security of these information technologies, in a manner appropriate to their roles'. At the same time, each state is empowered to 'determine its own critical information infrastructure'. In what concerns the phrasing of the 'ethics' principle presented in the annex of the same resolution, Yannakogeorgos asserts that it is 'founded on utilitarian grounds in that each participant is expected to respect the interests of others and to avoid inaction that will harm others.'

In the UNGA resolution 58/199 of 2003, the term 'stakeholders' is used for the first time, implying more leverage for inclusion in the decision-making processes. The ITU Resolution 174 from 2010 extends this further, to 'Member States and relevant ICT stakeholders, including geospatial and information service providers'. Resolution 64/211 of 2010 acknowledges the mandate of the IGF, 'reiterating that all Governments should have an equal role and responsibility for international Internet governance'. The 2010 Report of the GGE brings up 'cooperation between states, and between states, the private sector and civil society', making a first explicit reference to civil society as an equal player in the global governance of security in the cyber environment. The report also talks about 'threat actors', pointing out that 'of increased concern are individuals, groups or organizations, including criminal organizations, that engage as proxies in disruptive online activities on behalf of others'. (…)

A reaction to this understanding of threats comes under the form of a letter to the UN Secretary General for the introduction of an 'International code of conduct for information security'—a proposal advanced by the representatives of Russia, China, Tajikistan and Uzbekistan in September 2011 to be discussed in the following UNGA meeting(s). The most controversial part of the document states that the signatories of the code 'endeavor […] to prevent other States from using their resources, critical infrastructures, core technologies and other advantages to undermine the right of the countries, which accepted this Code of Conduct, to independent control of information and communications technologies or to threaten the political, economic and social security of other countries'. While this resembles a reassessment of the non-interference principle in the cyberspace, by redefining the responsibilities of the international community and individual member states, it can also be perceived as a way to counterbalance the gain of additional powers by ITU, following its attempts at modernizing itself after the 18th Plenipotentiary Conference" (Radu 14-16).

8. Concerns Over Cyber Terrorism

Cyber terrorism is a great threat for cyber security and national security of states, as well as the cyber stability of the international system. As a result of the availability of the means for producing and conducting cyber-operations and therefore cybercrimes and cyber terrorism, non-state actors can use the wide spread use of cyberspace to their leverage and might even put pressure on states or MNCs. Not only non-state actors, nation states also might use cyber terrorism via offshore hacker groups and cyber anonymity to conduct operations on their opponents such as the incident of the Stuxnet.

"In the USA critical infrastructure is defined as 'the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof'. Infrastructure that delivers electricity and water, controls air traffic, or supports financial transactions is seen as 'critical life sustaining infrastructures' and all directly depend on underlying communications and network infrastructure. The protection of such critical infrastructure forms an important part of cyber security and is included as an important national imperative in national cyber security strategies. Cyber terrorists or enemy specialists may target a country's critical infrastructure via cyberspace. This could either be indirectly, for example by influencing the availability of information services using denial-of-service attacks or, more directly, through an attack on the national electricity grid. In the case of attacks against such critical infrastructure, the loss entails not only of that of the integrity or availability of information resources, but also that of access to such critical services. In this case, it is neither the information itself nor the individual information user that is at risk, but rather the wellbeing of society as a whole. A good example of such attacks is the attacks on Estonia in April/May of 2007. These scenarios deal with a specific aspect of cyber security where the interests of a person, society or nation, including their non-information based assets, need to be protected from risks stemming from interaction with cyberspace. This serves to highlight the difference between information security and cyber security" (Von Solms et al. 100).

9. The Stuxnet

The cyber-attack conducted by the Stuxnet had significant consequences on the Iranian government as it was a huge blow on their prestige and nuclear programme. Iranian government was late to realize that their facilities and computers has been infected and they were unable to detect who was behind this cyber-attack, therefore could not retaliate. Iran was still under embargo and had limited resources with an already building up pressure on their budget, thus, the delay on production of enriched uranium, damaged the centrifuges, caused the production process to be ineffective—need to take action to ensure the cyber-security of government facilities requires significant financial investment as well—probably contributed to the economic pressures.

> "In 2010, the Stuxnet worm was discovered in an Iranian computer. The piece of malware surprised computer experts due to its sophistication and the use of four zero-day exploits. (…) The target of Stuxnet appears to have been the Iranian nuclear plant and uranium enrichment site in Natanz. (…) Iran uses IR-1 centrifuges, a European model from the late 1960s and early 1970s, which are both inefficient and now obsolete. These centrifuges are also fragile and an abrupt change of speed could cause damage or even breakage. The creators of Stuxnet were aware of this flaw and exploited it. The nuclear plant of Natanz has an air gapped and closed computer network, which means that it does not have a connection to the Internet or other networks. Therefore, it is highly probable that Stuxnet infected the network through the vector of a removable USB-drive. This means that the creators of the worm required a person to deliver the worm and infect the network.
>
> Several antivirus experts asserted that only a state could have developed Stuxnet because of its level of complexity, resource investment, and the fact it seemed to be specifically designed to target the centrifuges of Natanz. (…) The Iranians accused the West and more precisely NATO of being behind the attack. Nevertheless, experts claimed that the evidence, and the motive pointed to the USA and Israel as the perpetrators. There is speculation as to whether Israel was involved in the development of the malware, with experts from Symantec claiming they saw some evidence of its involvement in the coding lines. (…)
>
> Richard Clarke, former US National Coordinator for Security, Infrastructure Protection and Counter-terrorism, argued that if the USA had developed Stuxnet, Israel might have helped in the project by providing a testing site with a similar sample to the IR-1 centrifuge. The New York Times journalist, David E. Sanger, reported in his book that the USA had conducted a covert cyber-campaign, named Operation Olympic Games, against Iranian nuclear facilities. It is said that Stuxnet would have been one piece of malware developed and launched in the context of this operation. The campaign would have begun in 2006 under the Bush administration and would have been intensified by US President Obama. The operation was unlikely to have been limited to cyberspace. The assassinations of Iranian scientists in 2010 and 2011 that were attributed to the USA and Israel suggest that Stuxnet was only one piece in a larger operation aimed at slowing down or stopping Iran developing nuclear technology. It is also believed that the covert cyber-operation was an agreed concession to avoid an Israeli airstrike on Iranian nuclear facilities. (…)
>
> It would also have been possible for Russia to be the perpetrator of the attack. Russian workers had access to nuclear facilities in Iran as they were working with them on the nuclear site of Bushehr. Apart from the fact that Russia has the capabilities to develop such malware, its motive might have been to prevent Iran from enriching its own uranium

by damaging the nuclear sites with Stuxnet. In consequence, Iran would have had no other choice than to buy enriched uranium from Russia" (Baezner et al. 4-8).

10. The Case of Edward Snowden

The actions of Edward Snowden embody the claim that in the cyberspace besides nation states, individuals and non-state actors are highly influential and capable of performing cyber-actions that can compete with state's cyber capabilities.

> "In June 2013, Edward Snowden, a twenty-nine-year-old former National Security Agency (NSA) contractor without a college diploma, executed the single largest leak of classified intelligence in modern American history. (…) By revealing highly sensitive cyber tradecraft, Snowden exposed an even greater pool of state and non-state actors to some of America's most sophisticated tools and techniques, thereby decreasing the United States' relative cyber power. (…) Snowden's actions succeeded in removing the anonymity associated with American cyber power. States and non-states derive significant cyber power from obfuscating their operations because it complicates cyber defence and deterrence strategies, but also yields an unparalleled freedom of manoeuvre compared to other domains. (…) Furthermore, the United States' ability to attribute other states' operations in cyberspace is equally critical to amassing cyber power. In this respect, Snowden's actions compromised not only the United States' anonymity in cyberspace, but also, and perhaps more importantly, its ability to attribute other states' cyberspace operations for the purpose of cyber defence and ultimately, deterrence. (…) Prior to Snowden's leaks, the United States derived significant credibility on cyber issues from its legitimacy on a range of policies and practices. Moreover, it possessed a highly regarded reputation for leadership on Internet governance topics and, mainly due to the general illegitimate standing of other cyber powers, the United States enjoyed widespread support to pursue its policy objectives in international forums. But in the wake of Snowden's revelations, the United States' international credibility on these issues plummeted" (Weinstein 4-8).

11. American and Russian Cyberwarfare

11.1. The US Presidential Elections of 2016

In democracies, especially in representative democracies like the US, elections have the utmost importance for the health and effective working of the government. Elections are instances where the people express their will freely and change their governments and head of state. *De jure*, elections yield and create legitimacy for the elected and ruling government. Nevertheless, most of the elections in the modern world resemble *plebiscites*, with the people generally lacking information about the decision-making process and or candidates—thus, propaganda and misinformation play significant role in determining the fate of the elections. Manipulation of elections is first and foremost against the Westphalian norms of the international community—non-interference. Nonetheless, it is the usage of smart power to shape and influence the domestic policies of other states *vis-à-vis* the national interests of the acting state, aiming to sway the elections in favour of a government or candidate that is more beneficial for a certain foreign policy path.

> "The systematic state use of cyber as a weapon is a modern version of disinformation and propaganda tactics long used by Soviet and Russian security services. The idea of using cyber-attacks as part of a new 'hybrid warfare' strategy may be attributed to Valeryi

Gerasimov[9] (…) The ideas in this 'Gerasimov Doctrine' were implemented under Defense Minister Sergei Shoigu, with considerable resources allocated to cyber tools. Russian authorities began recruiting talented hackers using a variety of means. In addition to advertising on social media such as VKontakte, the Ministry recruited at leading universities and made cyber service an alternative to prison for cyber criminals. The strategy involved the creation of 'research squadrons' for information technology defense and offense, along with other scientific and technical aspects of defense (navy, air force, and medical). (…) The establishment of these IT squadrons mirrored US Defense Secretary Ashton Carter's creation of a special Defense Digital Service in 2015.

Russia's broad-spectrum flexible approach to conflict was realized in the government's reaction to Ukraine's EuroMaidan movement. Beyond the little green men in Crimea and support for separatists in Ukraine's southeast, Russia has used sustained forms of cyber warfare against Ukraine's internet, media, finance, transportation, electrical grid and cellular phone networks. In late 2016 Ukrainian President Petro Poroshenko claimed Russia had launched 6500 cyber-attacks against his country in just 2 months, targeting finance and defense ministries, the state treasury, and Kiev's power grid. Significantly, the pro-Russian group CyberBerkut hacked into Ukraine's electoral system prior to the May 2014 presidential elections in an attempt to discredit the process by reinforcing the Kremlin narrative of fascists and nationalists dominating Ukrainian politics. (…)

The best-known examples of interference are the purported Russian hacks into the Democratic National Committee's (DNC) Web site during the 2016 US presidential election, and the hacking of John Podesta's emails. The declassified version of the US intelligence agencies' report on Russian hacking claimed with a high degree of confidence that:

'Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton and harm her electability and potential presidency. We further assess Putin and the Russian government developed a clear preference for president-elect Trump.'

---

9 Back in February 2013, before the current Russia-West political conflict blossomed with the Ukrainian 'Euromaidan' revolution and the annexation of Crimea, Russian Chief of the General Staf General Valeryi Gerasimov wrote an article called 'The Value of Science in Prediction' (…). In it, he warned that:
'In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.'
He went on to describe how a 'perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war'. Subversion, disinformation, and sabotage prepare the ground for eventual kinetic operations, and the 'role of non-military means of achieving political and strategic goals' are now such that 'in many cases, they have exceeded the power of force of weapons in their effectiveness'.
He was channelling the Russian perspective on the Arab Spring and the 'coloured revolution' risings in the post-Soviet states, something persistently blamed on shadowy Western–American–machinations. He was also making the regular military's case for continued relevance (in other words, continued budget priority) in an age of such 'non-military' warfare: essentially their capacity to wipe out any such expressions of Western subversion. The September 2017 *Zapad* military exercises demonstrated this with pyrotechnic extravagance, the first few days being devoted to responding to the incursions of foreign 'diversionary elements' with massive, long-range firepower and close-quarters skirmishes alike" (Galeotti 157).

Distribution of damaging information from the DNC files and personal emails of Hillary Clinton, John Podesta, and other Democrats was largely through Wikileaks, whose leader, Julian Assange, had been highly critical of Hillary Clinton. The leaked information was reported on by the mainstream US media, which focused on the content rather than the original source of the leaks, making the media, as a New York Times story reported, effectively an accomplice in Moscow's efforts to foment discord in the American electoral process.

Given the deep cultural divides evident in the 2016 US election, Russian interference did not create instability, but rather accentuated and exacerbated tensions extant in the American political system. From the Russian perspective, Western democracy promotion, which focuses to large extent on electoral contests, feeds instability in weak states. By encouraging challengers to the status quo (in the form of extremist parties and candidates on the left and right), and by highlighting flaws in the electoral process, Russia can delegitimize democracies. The strategy is in effect a mirror image of Western democracy promotion, or a strategy of reciprocity.

11.2. Russo-Ukrainian War of 2022

As a contemporary event, the Russian invasion of Ukraine that started in 2022 proves that alongside kinetic warfare, cyberwarfare is significant and effective on influencing the outcomes in the battlefield. Russia and Ukraine are actors that are sovereign nation states in this cyberwar—Elon Musk and his Starlink, on the other hand are non-state actors that are capable of determining the outcome of the cyberwar, proving that it is an area of warfare that is the most open to non-state actors, and therefore less stable.

> "An event with far-reaching consequences and coinciding with the complementary cyberattacks against Ukrainian internet service providers and telecommunication services, concerned a cyberattack with yet another kind of wiperware (AcidRain) on Viasat, a major satellite internet communications provider for, among others, Ukraine and other parts of Europe. On the eve of the invasion, hackers erased the hard drives of Viasat's associated satellite internet homebased modems rendering these unserviceable. This resulted in the loss of battlefield communications particularly in the region close to the then seriously threatened Kyiv, making Ukrainian forces virtually blind to Russian troop positions and movements

The cyberattack on Viasat is a good example of how cyberattacks can be targeted and timed in operational support of military operations by disrupting and destroying the technology used by enemy forces. Thanks to the personal relationship between Ukraine's minister for Digital Transformation Mykhailo Fedorov and Elon Musk, the latter's Starlink satellite system quickly filled the incurred gap and restored Ukraine's internet communications.

In spring 2022, Russia withdrew the forces advancing toward Kyiv and redirected these to focus on other regions. Simultaneously, a shift in pro-Russian cyberattacks to the logistics and transportation sector inside Ukraine was observed. At that time, Ukraine's railways and transportation systems transferred weapon systems and military supplies eastward. Refugees used these means to flee in the opposite direction. Russian forces launched both missile-strikes and destructive wiper-attacks on the transportation infrastructure, suggesting a common goal.

In April, hackers targeted the Industrial Control Systems of a critical infrastructure: The Ukrainian power grid. The attacker had modified the previously used (2016) Industroyer malware to attack the power grid and cause power outages. Although similar to its predecessor, this version contained more targeted functionality. In addition, it was accompanied by yet other sets of destructive wiper malware. Late 2022, following Ukraine's military successes in regaining control over southern and north-eastern territory, Russia started kinetically attacking civil critical energy infrastructure. Given the diversity of the target infrastructure and the required access positions necessary for cyber activities, it is suggested that the generic capabilities and quick reaction times favoured kinetic action over tailored cyber actions. With the winter in sight, power and heat infrastructure were hit by numerous missile strikes. Concurrently, and possibly in support of these kinetic operations, wiper malware attacks targeted civilian power and water infrastructure.

In contrast to kinetic military operations, cyber operations can be executed covertly and, hence, are more suitable to be conducted in areas outside Ukraine. Pro-Russian actors used (Prestige) ransomware to attack the transportation sector in Ukraine and Poland, a NATO-member and a logistical hub for supplies" (Arnold et al. 241-242).

12. Cyber Stability

Cyber Stability is a question of creating cooperation and mutual understanding between states, much like any other area of international relations that aim to create a stability in the world order. "International cyber stability can be achieved by generating a platform of resilience, cooperation and transparency, with resilience being the fundamental component and cooperation and transparency providing support" (Kramer 121). Besides states, non-state actors—especially the civil society plays an important role in the establishment of cyber stability in the international system.

"A (…) lesson from Internet norms is that he multistakeholder approach is not optional, but mandatory for success. Norms that are only developed and promoted by a single actor or actor group are unlikely to be successful in this space—implementation will only be possible if there is shared ownership, and ownership usually means some form of participation. In practical terms, this means that previously state-only norm processes must have much stronger engagement with the private sector and civil society to be successful. (…) Multistakeholder approaches that include representatives from civil society organizations, business, technology, and academia might help to increase awareness about norms for cyber stability at different levels of governance, which also raises the likelihood of their being adopted and adhered to. (…) The second part of the solution requires that those "other actors" (such as Internet governance actors like ICANN in particular) be ready to respond when invited to these discussions. But that itself may prove to be a difficult bridge to cross, as many of these organizations themselves are incentivized to be resolutely inward looking and effectively hobbled by their own stakeholders. Multistakeholder processes aim to bring together all major stakeholders in a new form of communication and decision-making on a particular issue. Considering the importance of the normative process for cyberspace governance, it is important to recognize that global norms processes are insufficient, because they are distant from the lower layers of governance in practice. Multistakeholder approaches that include representatives from civil society organizations, business, technology, and academia might help to increase awareness about norms for cyber peace at different levels of governance. (…) An effective governance system for cyber stability that relies on

normative processes requires advancing both the implementation and operationalization of norms" (Klimburg et al. 65).

12.1. Liberal IR Theory

The Liberal theory of IR is not a naïve perception of the world; therefore, it does not deny that the international system is anarchic. Nevertheless, the lack of global governance and enforcement is a reality, which liberals believe it's negative effects can be mitigated. Thus, liberals offer these four propositions:

12.1.1. Commercial Liberalism

Joseph Nye is one of the liberal theorists that suggest this form of liberalism. As a result of globalization—the network of increased economic exchange, and therefore economic interdependence, has a pacifying effect on states, making war unthinkable and diminishing its possibility—preventing anarchy turning into conflicts. Typical cases being the US-Canada and Germany-France. Free trade and investments creates vested interests against armed conflict—actors which benefit from economic interdependence trying to prevent wars. There are examples of geopolitical rivals not fighting because of close economic interdependence that was created during the Cold War era—Greece-Turkey, China-India and South Korea-Japan are some of the cases. Arguing against this claim, Realists state that South Korea and Japan for instance, are the part of the same alliance structure under the patronage of the US, as China seems to be a bigger security threat that causes these states to rather cooperate than become rivals. Another criticism points out to the economic interdependence between Russia and Turkey, stating that there is an asymmetric relationship that favours the more powerful state.

12.1.2. Democratic Peace Theory

This theory is the closest to becoming a law in IR. Democratic Peace theory claims that democracies do not fight with each other. The given reason for this is the mechanisms of democracy—citizens of democratic countries do not wish to fight with other democratic countries' citizens. The root and philosophical origin of this theory is in Immanuel Kant's "Perpetual Peace" in which he argues that republics will not fight each other. Nevertheless, realists criticize this theory stating that this might be empirically true, nonetheless, consolidation of democracy is relatively new and archival research shows that democratic powers came to the brink of war many times, yet, the balance of power was what prevented them from going to war—an example case being the Suez Crisis, in which the UK and France had rising tensions with the US.

12.1.3. Functionalism

Functionalism suggests that the growth of international institutions and legal agreements create a 'link' of peace. States establish international institutions with a particular function, which strengthens and promotes cooperation amongst states, and reduces the possibility of wars, as states tend to discuss their frustrations in a diplomatic environment. Some of the most famous cases—WTO was created to discuss trade disputes and IMF to prevent economic crisis.

12.1.4. Transnationalism/Cosmopolitanism

Transnationalism suggests that citizens and other economic actors of various origin states engage in cross-border activities, which make war unthinkable for them. Cosmopolitanism suggests the creation of a global society—a united global society, as cooperation is by nature. The EU, as a supranational organization, came closes to fulfilling this dream.

Liberals argue that international law[10] and organizations has an important function and mission of helping states resolve collective action dilemma that emerge from mixed interests. States are rational actors and therefore would prefer to maximize their own interests. Creating a platform for states to allow them to resolve their security dilemmas and 'trust issues'—at the same time creating a space for international knowledge exchange, where state can learn from each other—eliminates the anarchic nature of the international system. Via the collective good, every state is better-off as the gains are maximized for everyone. With respect for the international law and transparency among states, collective interests are created, which states can use to maximize their own national interests and gains. In the world of international institutions and cooperation, incentives for compliance is a necessity.

12.1.5. Liberal IR Theory and Cyber Stability

Taking the liberal approach into consideration (especially commercial liberalism), it can be said that states and non-state actors that benefit from free market trade, financial investments and economic interdependence—making a costs and benefits analysis as rational actors, finds war and armed conflict expensive. The same approach is true for cyber-space as well, especially considering that most of the financial transactions and trade actually happens on the internet and related systems. Therefore, cyberwarfare and cyberattacks are expensive, especially when they target world's biggest economies and stock markets—which is a risk no major economy in the Global North would dare to take. Naturally, if such a cyber-operation were linked to a major world economy, MNCs, private banks, private individuals, and the market would exert immense pressure on the acting state—which would not be preferred especially in a democracy, as it could risk causing the government to fall.

Thus, liberals would argue on three main points to prevent and solve the question of cyberwarfare and the establishment of cyber stability. First, democratic countries should not conduct cyber-operations targeting each other's facilities and economic centres as it is undesirable for the free market and trade in the economically interdependent world—both states and non-state actors shall put pressure on each other to not conduct such cyber-operations for the sake of the economic and financial interests. Secondly, the establishment of an international institution or a legal document on the issue of cyber security, allowing the monitoring of state's programmes and actions in the cyberspace would prevent hostile cyber-operations targeting others. It would also allow states to discuss their problems and interests related to cyber security in an international platform that is transparent and creates bonds of trust between member states, and especially the world's major powers. Lastly, in a broader context, establishment and creation of a united global society or a supranational institution would prevent such cyber-conflicts and warfare as in the case of the EU.

This approach might provide an understanding of the reasons for UNGA resolution on protection of cyberspace statements on the frame of protection:

> "Apart from 'information security' and "cybersecurity", the other type of reference made to protection in the cyberspace comes under the form of securing critical information infrastructures, and it was introduced in the UNGA resolution language in 2003 through the Resolution 58/199 of 23 December, 'Creation of a global culture of cybersecurity and the protection of critical information infrastructures', and later on reiterated in resolution 64/211 on 'Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures', adopted in 2010. In this context, critical infrastructures are identified as 'those used for, inter alia, the generation, transmission

[10] The theoretical effectiveness of international law is discussed under sub-title "2. International Law and Organizations"

and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health—and the critical information infrastructures that increasingly interconnect and affect their operations'. The latter resolution had 40 sponsoring countries under the lead of the US and proposed a voluntary self-assessment tool for national efforts to protect critical information infrastructures.

The technologies used to support cybersecurity present an interesting paradox with regards to the international and national levels that Diebert and Rohozinski point out. As they show, there are contradictory movements in the actions taken by governments to address these problems: on the one hand, the measures to achieve greater cooperation at the international level for the protection of critical infrastructure underlie the preservation of a free and open internet; on the other hand, increasing divergence can be noticed in the national efforts against risks through cyberspace, as governments tend to impose—within their national boundaries—measures that limit the potential of global connectivity by filtering, blocking, surveilling content, etc. In a Foucauldian understanding, such high-impact technologies may act in a disciplinary way, as they can allow for constant monitoring of individual activities on the internet; they may also create incentives for identification of online behavior patterns and may impose a degree of self-restraint on the end-user. Such potential has been realized in certain areas around the globe, such as China or Iran" (Radu 13-14).

12.2. Structural Realist and Defensive Realist IR Theory and Cyber Stability

Structural Realism, as an IR theory, looks into the structure of the international system and world order, and determines its effects on the state behaviour. As an extansion of realism, structural realism also argues that the primary aim of a state in the international system is to pursue its interests and achieve to its foreign policy aims, with the main goal being the security and survival of the state within the anarchy of the system. Structural Realism argues that the immitigable anarchy of the system is the cause of conflict and war—this anarchy is permanent and cannot be changed by any actor within the system, without changing the system itself. The state interaction and behaviour is governed by this international structure of the system. Anarchy caused by the lack of global governance and enforcement or an authority is the defining factor of this structure. Other defining factor of the structure is the states' capability and function. The distribution of capabilities—the power of the state is the determinant for its survival. Therefore, cyberwarfare which is defined by a state's cyber arsenal and capabilities are influential in the international system.

Offensive Realists, such as Mearsheimer, argue that a state should maximize its capacity and power—whereas Defensive Realists like Kenneth Waltz states should show caution against power accumulation after a certain point, as it will have negative consequences due to balance of power, as pursuing hegemony is destructive for the state. Defensive Realists argue for "appropriate power," taking into consideration strategic concerns, possible reactions from neighbouring states and the balance of the international system. Therefore, in cyberwarfare, Defensive Realists argues for the effective use of Mutually Assured Destruction principle to prevent cyberattacks and cybercrimes, to ensure there is cyber stability in the international order.

"Cyberspace is also a sector as it is currently being securitized by state and non-state actors; it is a site of contention. (…) There are two stages of securitization: the first is the portrayal of event/issue/person as a threat to the referent object. The second is the need for the public to consent, to successfully convince the audience. We see this happening. First, states perceive that their security as under attack and are doing what they can to exert control. The kill-switch is a firm example of this. Non-state actors see the internet

as being attacked. They are doing their part to securitizing cyber-space as well. For example, hacktivists like Anonymous and Lolzsec see their freedom of speech and expression on the internet under threat. Their activities are a response to what they perceive as an attempt by states and corporations to annex the internet for their purposes.

Firewalls can be found inside hardware such as routers, modems and so on. (…) Without going into much detail, each type attempts to block unwanted users. These function in similar ways, using their source and destination address to identify users. In this way, it is a passive way to deny access to the unauthorized. (…) Viruses and worms can cause economies to slowdown and stop, and sometimes result in loss of life. They usually infect "targets of opportunity" or weak security systems, but can also be sophisticated enough to destroy political targets. (…) unauthorized users can encapsulate data from one area of a database to another using the faculties of the firewall. Once inside, the message is inserted into the network and tucks itself inside the database rendering it undetectable. This way, unauthorized actors can infiltrate, steal or control the database that is supposedly protected by this firewall.

What can be done to avoid this type of infiltration? It is here that I will discuss the proposed virus-wall system. If an attacker infiltrates a database's virus-wall by tunnelling through it, a virus should attach itself onto the attacker, that is, use the tunnel that was created to seek out and destroy the source of the attack. To recall, a virus attaches itself through contact with an uninfected user. If there is no communication, then there is no transmission. There will be no infection if there are no attackers making contact with the infected database. The problem with firewalls is that it is a passive means of defence; after all, the walls of Troy were penetrated by enemy forces. The scheme is to infect the database with the virus without harming the database. Furthermore, the virus should be so aggressive to knock out all the computers within its vicinity. This way, the cost of attack would be so outrageous, no further attacks would be launched. Staying true to Defensive Realism and the assumptions of Mutually Assured Destruction, such a system would minimize the occurrence of cyber-warfare as the benefits of carrying out such activities would be cancelled out by its enormous and unreasonable costs.

There are, of course, moral and ethical issues that must be discussed. Like Mutually Assured Destruction of the Cold War, cyber-deterrence disturbs the lives of many innocent people. I am arguing for a system that seeks to destroy the computers in proximity to the attacker's. An entire state's economic growth and development can be hindered by this proposed system. Is it fair? Of course not, but like the logic of sanctions (the way they are supposed to work) the citizens must confront the initial attacker to prevent any further cyber-attacks. However, there must be an antidote available to the attackers after some time. The antidote would effectively remove the virus from infected computer systems. Before the antidote is given, a second virus-wall will replace the first to continue cyber-deterrence. In this sense, cyber-warfare can be effectively stopped bringing balance to cyberspace.

Currently, there are no laws to punish states who conduct cyber-attacks; there is a definite lack of governance over cyber-space and the internet. As said, states operate within an international system as described by Structural Realism: it is one of the self-help comprising of an anarchical structure. Even with the perpetrators properly identified, it would be very difficult to bring offenders to justice. They would be protected by their

state's borders. Thus, actors may continue their attacks with no fear; only of reprisal. There would be no stability as described by the idea of Mutually Assured Destruction. There should be a mechanism in place to disrupt these activities by making punishment for such indiscretion a reality" (Kassab 64-73).

13. Cyber Capacity Building

Capacity building is a rather realist approach—as a result of security dilemma and balance of power concerns, states seek to increase their relative capacities to ensure their security in the international arena and develop capacity to pursue their national interests. By the nature of IR, capacity building requires the mutually assured destruction principle as well—with respect to defensive structural realism. A state can ensure its survival via developing its capacity to either be unmatchable and become the hegemon of the system -offensive realism- or increase its power to an appropriate level to be able to compete with other states of the international order and defend itself from any hostile and offensive action –defensive realism- either way being able to retaliate is an important defence strategy. "'Capacity building' is a catch phrase from the UN development discourse. In recent years, it has entered the global Internet governance (IG) arena. At World Summit of the Information Society (WSIS 2003), 'capacity building' was identified as a key public policy issue" (Antonova 425). In addition to having the capacity to prevent the occurrence of any cyber-attack or cyber-operation, being able to retaliate in the case of failed prevention is crucial for deterrence.

> "An important condition for the build-up of cyber capacity is whether the country possesses adequate resources to achieve its desired cybersecurity goals. This argument derives from the theory of opportunity and willingness, which suggests that states require both opportunity (capacity) and willingness (interest) to act in a given area. This framework has been employed to explain a wide range of state activity, from international conflict to arms production or military technology adoption. The final set of factors, therefore, relate to the opportunity to develop cyber capacity, which is determined by access to resources. Resources should be critical for explaining the cyber capacity divide between the Global North and South, given the historical inequalities in terms of economic development, industrialisation and knowledge production" (Calderaro 925).

13.1. A Realist Approach to Cyber Capacity Building

"The first set of explanatory factors is informed by realist IR theory which is founded on the idea that states operating in the self-help, anarchical international system are responsive to security threats from other countries and seek to deter aggression and ensure their survival through military build-ups. Capacity building in the cyber domain may also be motivated by a need to deter threats. The ability of states to infiltrate one another's computer networks for strategic gain creates a cybersecurity dilemma, according to Buchanan, which, as realists argue, drives a mutual build-up of capabilities to restore security. The threat posed by the cyber activity of rival actors could promote the development of cyber capacity in preparation for an attack and to build a deterrent capability through either denial or punishment. If states develop cyber capacity to reduce digital threats from their rivals, it follows that states facing more substantial threats or more rivalry should be more interested in building cyber capacity. Security threats can be conceptualised in terms of conventional threats and cyber-based threats. In this analysis, we can assess the effects of both on cyber readiness" (Calderaro 924).

13.2. A Liberal Approach to Cyber Capacity Building

"Liberal IR theory suggests that due to the structural constraints on the executive in democracies, democratically elected governments are more responsive to the demands

of their populations than authoritarian states are. Cyber threats may not actually be more significant in democracies, but democratic governments may experience higher pressure to invest in cyber capacity to avoid suffering negative audience costs. Moreover, regime type may capture the effects of the so called 'cyber-industrial complex' whereby vested economic and political interests push for increased investment in cyber capacity, partly through cyber threat inflation and 'cyber doom scenarios'. This phenomenon may be more likely in a democracy due to societal openness giving interest groups more influence in the political decision-making process. On the other hand, authoritarian states could have higher capacity because of greater efficiency, whereas relatively new democracies, especially in the Global South, may lack the stability to build cyber capacity" (Calderaro 924).

13.3. A Constructivist Approach to Cyber Capacity Building

Constructivists generally concentrate on the identities of the actors, as they see the world as a social place, dominated by human interactions. They argue that human interactions create identities (culture, religion, ethnicity, nationality, history of identity…), which create more identities, and eventually leads to the creation of national identities—national interests change from one country to another. Constructivists argue that social reality is socially constructed—responding to the realist argument of anarchy in the international order, they claim that anarchy is what states make of it; and state that it depends on how the actors interpret it. The interests change from one identity to another, therefore the interests of individuals and other non-state actors are important. The national identity creates national interests—which are decided by the identities within the state -the political elites- who are often influenced by strategic culture, define what is the state's national interest based on their own understanding of their nation's interests. Globalization and the global communication and interaction of actors results with 'shopping' or 'changing' of identities—much like the liberal understanding of transparency creating trust; constructivists argue interaction between states, cooperation and transparency results with transformation of identities in the international system. They argue for normative change—transformation of norms of IR.

"Constructivist IR scholars argue that IGOs can help shape state behaviour through the development of norms that define the parameters of acceptable behaviour internationally. The concept of cyber-norms and the institutions that could promote them in areas such as technological export controls, the non-proliferation of cyber weapons, and restraint from cyber conflict have already been discussed by scholars. Greater membership in IGOs reflects a stronger willingness by a state to engage with global governance efforts and abide by the norms of the international community. Assuming the international community is currently promoting the norm of cyber capacity building, one might expect there to be a greater tendency towards cyber capacity building amongst countries that are in general more cooperative and engaged internationally, in contrast with pariah states such as North Korea that are detached from global governance efforts and less influenced by norms.

Another constructivist-based concept is that of status and prestige. Prior research suggests that states seek military capabilities, including nuclear weapons, as a status symbol, and a similar dynamic may exist in the cyber domain. Countries that consider themselves significant players in international politics may pursue cyber capacity because it befits a state of their status and confers prestige. Major or regional powers, most of which lie in the Global North, may therefore be expected to possess greater levels of cyber capacity" (Calderaro 924-925).

14. Global Governance, Cyber Stability and Capacity Building

It is possible to say that the concept of global governance is an attempt to mitigate the effects of the anarchic state the international order is, and the structure that is created by this type of international system. As realists and structural realists argue with regards to the lack of enforcement and global authority—to regulate, oversee and ensure the *État de droit*[11] causes instability and injustice. The solution to overcoming this structural problem is the establishment of a global governance, reforming international institutions, and strengthening the international law—the *jus cogens* and *jus gentium*. Global governance is also a crucial concept for liberal IR theory, as it is based on the consensus and cooperation of states, embodying an international institution that governs and monitors state behaviour, and enforces international law.

Therefore, the creation of an international institution or reforming the already existent ones, and the enforcement of the international law might create cyber stability. However, the question of global governance must be addressed in order to apply it to the cyberspace. Capacity building can be a solution to bypass the problem of global governance which is a macro issue, and concentrate on cybersecurity as a micro issue.

14.1. Internet Governance and Cyber Capacity Building

> "In recent years, capacity-building has acquired a broader interpretation by focussing on 'the relationship between different organizations, groups and individuals as well as the environment in which they all perform'. This latest interpretation of the concept applies to the global IG case, as by definition a MSH forum's mandate is to allow such relationships to be built, maintained, and to lead to tangible results. Therefore, I would propose that, in the IG context, capacity-building should be defined in relation to the MSH process. The open collaborative process facilitates the accumulation of intellectual capital, skills, and competencies; development of a relational infrastructure for the domain, as represented by stakeholder constituencies, collaborative alliances/dynamic coalitions, and network communities; and emergence of a common global consciousness (realization of stakeholder interdependencies and shifting identities, among others).
>
> Capacity-building was identified in the WGIG Report as one of the public policy issues that are relevant to Internet governance, but it was mainly seen as a matter of national governance: 'Capacity-building: Adequate resources have not been available to build capacity in a range of areas relevant to Internet management at the national level and to ensure effective participation in global Internet governance, particularly for developing countries.'
>
> (…) capacity-building was defined in the WSIS/WGIG discourse in broad terms – ranging from training and evolving human resources to developing and securing financial and technical resources, and all of these were seen as policy issues to be addressed at the global, as well as at national levels. Yet the potential of the MSH process itself to contribute decisively to the creation of knowledge and its diffusion from the global to the local levels was not realized" (Antonova 436-437).

[11] Rule of law

15. Cyber Conflict Prevention and Cyber Peace-keeping

Conflict prevention is often used together with UN-concepts of peace-making and peace-keeping. Adapting these concepts to the cyberspace creates the "cyber peace-keeping". "Cyber Peacekeeping is defined as cyber conflict prevention, mitigation, aftermath containment and rehabilitation with a focus on conflict de-escalation and civilian security" (Akatyev et al. 131). Therefore, it is possible to understand cyber peace-keeping as the creation of an international system that would monitor and mediate between the warring parties of the cyberspace. "Cyber Peacekeeping works to promote online safety and security with accordance to international laws and agreements in order to protect civilians as its main goal. CPK is a framework to maintain conditions for lasting peace in cyber and physical spaces impacted by possible threats in cyberspace" (Akatyev et al. 131). The aim of cyber peace-keeping is to prevent possible conflicts, while ensuring stability of the cyberspace, when. During conflict, cyber peace-keeping works to stop the ongoing conflict and try to create a diplomatic environment to create a mutual understanding between the warring parties, and once the conflict is resolved it aims to prevent further destructions and enact the recovery process.

> "Currently, international relations are not at a point where truly global Cyber Peacekeeping is possible. Implementation at a regional level is also undesirable since many regions already have organizations that have at least some overlap with Cyber Peacekeeping, as proposed. Instead, already established international organizations, such as INTERPOL or the United Nations, should attempt to fill the identified gaps. The challenge then would be allowing Cyber Peacekeeping to remain agile and responsive while being associated with large, notoriously slow entities. Alternatively, some described aspects of Cyber Peacekeeping could be implemented regionally, such as the concept of a cyberspace safe layer, and information clearing-house. If these are established regionally, or even nationally, then once a global entity for Cyber Peacekeeping does exist, current local implementations and standards could be directly applied" (Akatyev et al. 138).

The *détente* process is crucial for the rapprochement between actors that are involved in a cyberwarfare, in order to protect the cyber security. Unlike kinetic warfare and direct armed conflict, it is easier to go to the *status quo ante bellum* in the cyberspace. With proper mitigation and mediation between actors, with the governance of a powerful international institution or legal framework—process of cyber conflict prevention and re-establishing the order in the cyberspace and ensuring security seems to be possible.

16. Resolutions of the Security Council on Cybersecurity

The UN covers the issue as cybersecurity and new technologies—thus, often with regards to the usage of new technologies by armed non-state actors and terrorist groups, and protection of the crucial infrastructure against terror attacks. The UN and ITU published a guide on cybersecurity called: "A Guide to Developing a National Cybersecurity Strategy, 2nd Edition 2021". The guide simply aims to "guide national leaders and policy-makers in the development of a National Cybersecurity Strategy, and in thinking strategically about cybersecurity, cyber preparedness and resilience" (ITU). This guide is accessible from the website of UN[12].

The UN Security Council in its Resolution 2341 in 2017 on protection of critical infrastructure states:

[12] **The link to the guide is:** un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf

> "Recognizing that protection efforts entail multiple streams of efforts, such as planning; public information and warning; operational coordination; intelligence and information sharing; interdiction and disruption; screening, search and detection; access control and identity verification; cybersecurity; physical protective measures; risk management for protection programmes and activities; and supply chain integrity and security" ("UN").

"8th Review of the United Nations Global Counter-Terrorism Strategy" (A/RES/77/298), Security Council Text S/2015/939 (Madrid guiding principles) and UNSC Resolution 2370 in 2017 takes terrorism as the centre with references to cybersecurity. Similarly, the Delhi Declaration also points out the use of technology by terrorist groups and gives references to cybersecurity:

> "Emphasizes the need for Member States to act cooperatively to prevent and counter the use of new information and communications technologies, and other emerging technologies, for terrorist purposes, including recruitment and incitement to commit terrorist acts, as well as the financing, planning and preparation of their activities and stresses the importance of cooperation with civil society and the private sector in this endeavour" ("UN").

The "Sixteenth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat," mentions cyberattacks in its article 62:

> "Efforts to protect critical infrastructure and vulnerable targets from terrorist attacks continued to be prioritized within the United Nations system. (…) The Executive Directorate, the International Criminal Police Organization (INTERPOL) and the Office of Counter-Terrorism, in close partnership with the Organization for Security and Cooperation in Europe, held a workshop for experts to strengthen capacities and facilitate the exchange of good practices among States in Central Asia on protecting vulnerable targets from physical attacks and cyberattacks" ("UN").

Questions to be Addressed

1. In what ways can the UNSC foster the development of international norms and legal frameworks to regulate state behaviour in cyber operations?

2. What role can the UNSC play in establishing mechanisms to prevent the escalation of cyber conflicts and sustain international stability in cyberspace?

3. Considering its mandate, how can the UNSC facilitate international cooperation to build cyber defence capabilities?

4. How can the UNSC support the development and implementation of effective deterrence strategies in cyberspace, and leverage its unique position to initiate preventive diplomacy aimed at mitigating emerging cyber conflicts?

5. What specific strategies should the UNSC endorse to address the growing threat of cyber terrorism and its implications for international peace and security?

6. What measures should the UNSC recommend to enhance the resilience and response capabilities of nations against recognized cyber threats, and how can it facilitate a coordinated international response?

7. What role should the UNSC play in strengthening international legal regimes to better govern state and non-state cyber activities, and how should the UNSC engage with various cyberspace actors, including private sector and civil society, to enhance global cybersecurity frameworks?

8. How can the UNSC contribute to the development of a universally accepted definition of cyberwarfare to guide international law and enforcement, and promote a standardized global approach?

Works Cited

Akatyev, Nikolay, and Joshua I. James. "Cyber peacekeeping." *Digital Forensics and Cyber Crime: 7th International Conference, ICDF2C 2015, Seoul, South Korea, October 6-8, 2015. Revised Selected Papers 7*. Springer International Publishing, 2015.

Antonova, Slavka. "Capacity-building" in global Internet governance: The long-term outcomes of "multistakeholderism." *Regulation & Governance* 5.4 (2011): 425-445.

Arnold, Kraesten, et al. "Assessing the Dogs of Cyberwar: Reflections on the Dynamics of Operations in Cyberspace during the Russia-Ukraine War." *e R U*: 231.

Atrews, R. A. "Cyberwarfare." *Journal of Information Warfare* 19.4 (2020): 17-28.

Baezner, Marie, and Patrice Robin. *Stuxnet*. No. 4. ETH Zurich, 2017.

Bajaj, Kamlesh. "Cyberspace: Post-Snowden." *Strategic Analysis* 38.4 (2014): 582-587.

Calderaro, Andrea, and Anthony JS Craig. "Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building." *Third World Quarterly* 41.6 (2020): 917-938.

Galeotti, Mark. "The mythical 'Gerasimov Doctrine'and the language of threat." *Critical Studies on Security* 7.2 (2019): 157-161.

Kassab, Hanna Samir. "In search of cyber stability: international relations, mutually assured destruction and the age of cyber warfare." *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. 59-76.

Klimburg, Alexander, and Virgilio AF Almeida. "Cyber peace and cyber stability: Taking the norm road to stability." *IEEE Internet Computing* 23.4 (2019): 61-66.

Kramer, Franklin D. "Achieving international cyber stability." *Georgetown Journal of International Affairs* (2012): 121-137.

Kshetri, Nir. "Cybersecurity in National Security and International Relations." *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies* (2016): 53-74.

Parks, Raymond C., and David P. Duggan. "Principles of cyberwarfare." *IEEE Security & Privacy* 9.5 (2011): 30-35.

Radu, Roxana. " Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace." *Cyberspace and International Relations: Theory, Prospects and Challenges*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013. 3-20.

Robinson, Michael, Kevin Jones, and Helge Janicke. "Cyber warfare: Issues and challenges." *Computers & security* 49 (2015): 70-94.

"UN Documents on Cybersecurity and New Technologies" *un.org*. un.org/counterterrorism/cct/programme-projects/cybersecurity

Valdés-Ugalde, José Luis. "Approaching power and understanding leadership through the lens of Joseph Nye." *Norteamérica* 3.1 (2008): 197-204.

Von Solms, Rossouw, and Johan Van Niekerk. "From information security to cyber security." *computers & security* 38 (2013): 97-102.

Watanabe, S. (2020). States' Capacity Building for Cybersecurity: An IR Approach. In: Kreps, D., Komukai, T., Gopal, T.V., Ishii, K. (eds) Human-Centric Computing in a Data-Driven Society. HCC 2020. IFIP Advances in Information and Communication Technology, vol 590. Springer, Cham.

Weinstein, Dave. "Snowden and US cyber power." *Geo. J. Int'l Aff.* 15 (2014): 4.

Ziegler, Charles E. "International dimensions of electoral processes: Russia, the USA, and the 2016 elections." *International Politics* 55.5 (2018): 557-574.

Bibliography

Amulya, Narem VNSS, and Animi Poornima. "Cyberwarfare, Space Hegemony and International Law." *IUP Law Review* 12.3 (2022).

Chen, Thomas M., and Saeed Abu-Nimeh. "Lessons from stuxnet." *Computer* 44.4 (2011): 91-93.

Cornish, Paul. "The Deterrence and Prevention of Cyber Conflict." *The Oxford handbook of cyber security* (2021): 273.

Egan, Brian J. "International law and stability in cybershpace." *Berkeley J. Int'l L.* 35 (2017): 169.

Fridman, Ofer. "On the" Gerasimov Doctrine"." *Prism* 8.2 (2019): 100-113.

Healey, Jason, and Robert Jervis. "The Escalation Inversion and Other Oddities of Situational Cyber Stability (Fall 2020)." (2020).

Hildreth, Steven A., and Foreign Affairs, Defense, and Trade Division. "Cyberwarfare." Congressional Research Service, Library of Congress, 2001.

Jenkins, Ryan. "Cyberwarfare as ideal war." *Binary bullets: the ethics of cyberwarfare* (2016): 89-114.

Klein, Hans. "Information warfare and information operations: Russian and US perspectives." *Journal of International Affairs* 71.1.5 (2018): 135-142.

Kolovos, Alexandros. "Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict." *Air & Space Management and Control Laboratory, OCCASIONAL PAPER* 3 (2022).

Komninos, Theodoros, and Dimitrios Serpanos. "Cyberwarfare in Ukraine: Incidents, Tools and Methods." *Hybrid Threats, Cyberterrorism and Cyberwarfare*. CRC Press, 2024. 127-147.

Lam, Christina. "A slap on the wrist: Combatting Russia's cyber attack on the 2016 US presidential election." *BCL Rev.* 59 (2018): 2167.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." *Security Studies* 22.3 (2013): 365-404.

Lowe, V., Roberts, A., Welsh, J., & Zaum, D. (Eds.). (2010). *The United Nations Security Council and war: the evolution of thought and practice since 1945.* OUP Oxford.

McDermott, Roger N. "Does Russia have a Gerasimov doctrine?." *The US Army War College Quarterly: Parameters* 46.1 (2016): 11.

Miller, Seumas, and Patrick Walsh. "The NSA leaks, Edward Snowden, and the ethics and accountability of intelligence collection." Ethics and the Future of Spying. Routledge, 2016. 193-204.

Orji, Uchenna Jerome. "The African union convention on cybersecurity: A regional response towards cyber stability?." *Masaryk University Journal of Law and Technology* 12.2 (2018): 91-129.

Pope, Amy E. "Cyber-securing our elections." *Journal of Cyber Policy* 3.1 (2018): 24-38.

Valeriano, Brandon, and Ryan C. Maness. "International relations theory and cyber security." *The Oxford handbook of international political theory* (2018): 259.

Von Solms, Suné, and Renier Van Heerden. "The consequences of Edward Snowden NSA related information disclosures." *ICCWS 2015—The Proceedings of the 10th International Conference on Cyber Warfare and Security: ICCWS2015*. 2015.

ŞHRMUN'24

#FORABETTERWORLD