Ankara Hacı Bayram Veli Üniversitesi
İktisadi ve İdari Bilimler Fakültesi Dergisi 23/3 (2021) 681-698
E-ISSN 2667-405X

Distribution of Capabilities and Anonymity in the Digital World: A New Balance of Power in the International System

Kürşad Şeyhmus TURAN[1] Mesut ASLAN[2]

Geliş Tarihi (Received): 12.10.2021 – Kabul Tarihi (Accepted): 01.11.2021

Abstract

Information technology has evolved to the extent that there is now a digital world where all participants in the physical world are also present and interact with each other, including the states and international relations. Many theories provide explanations for the behaviour of states and their relations. One of the prominent approaches is the systemic approach of Neorealism which focuses on the distribution of the capabilities among states. We argue that states' physical and digital capabilities must be analyzed separately to provide better explanations from the Neorealist perspective. The interactions between these two worlds are limited due to the reduced cost of gaining more power and higher anonymity provided by the digital world. There is a considerable difference in the distribution of capabilities that cause significant changes in the polarity of the international system in the digital world, and the great powers of the physical world no longer enjoy the same level of security in the digital world.

Keywords: Neorealism in the Digital World, Cyber Warfare, Cyber Balance of Power, Digital Threats, Anonymity in the Digital World

Dijital Dünyada Kuvvet Dağılımı ve Anonimlik: Uluslararası Sistemde Yeni Bir Güç Dengesi

Öz

Günümüzde bilgi teknolojileri, devletleri ve uluslararası ilişkileri de içeren, fiziksel dünyadaki tüm katılımcılarının bir arada ve iletişim içerisinde olduğu dijital bir dünyaya doğru evirilmiştir. Uluslararası İlişkiler disiplininde birçok teori, devlet davranışı ve devletlerin birbirleriyle olan ilişkileri hakkında açıklamalar sunmaktadır. Bu teorilerin önde gelenlerinden bir tanesi, devletler arasında kuvvet dağılımına odaklanan ve dolayısıyla sistemsel bir yaklaşıma sahip Neo-Realizmdir. Bu makale, Neo-Realist bir perspektiften, bilgi teknolojileri, devlet davranışı ve devletlerin ilişkileri arasındaki bağın daha iyi anlaşılabilmesi için devletlerin fiziksel ve dijital kuvvetlerinin, ayrı ayrı analiz edilmesi gerektiğini iddia etmektedir. Fiziksel ve dijital dünya arasındaki etkileşim, dijital dünyanın daha az maliyetle güç ve anonimlik artışı sağlaması nedeniyle kısıtlıdır. Dijital dünyada, kuvvetlerin dağılımı, uluslararası sistemin kutupluğunu önemli ölçüde değiştirebilecek kadar farklıdır ve fiziksel dünyanın büyük güçleri, dijital dünyada artık eskisi gibi yüksek bir güvenlik ortamından faydalanamamaktadır.

Anahtar Kelimeler: Dijital Dünyada Neorealizm, Siber Savaş, Siber Güç Dengesi, Dijital Tehditler, Dijital Dünyada Anonimlik

[1] Doç. Dr., AHBV Üniversitesi, İ.İ.B.F., kursad.turan@hbv.edu.tr, ORCID: 0000-0002-7622-5412
[2] Arş. Gör. Dr., AHBV Üniversitesi, İ.İ.B.F., aslan.mesut@hbv.edu.tr, ORCID: 0000-0003-0299-0928

Introduction

The repeatedly utilized cliché "We live in the digital age" is generally misinterpreted. While everybody agrees with the primary notion, which is "the digital sphere is widening and encompassing all areas of our existence," we tend to think of the digital world as an extension of the physical one. The fact is, the digital world is not an extension; instead, it is another realm altogether. For example, in 2018, humankind globally created 33 zettabytes of digital data. (Armstrong 2019) However, this number does not mean anything without bringing it into perspective. As a thought experiment, Mark Lieberman calculated that all human speech, every word ever spoken by every person, since the beginning of history could potentially be recorded, in 42 zettabytes *as sound*. (Lieberman 2013) In other words, we created virtually our entire spoken history worth of data in a year. The digital age introduced a new form of society complete with an economy and culture all its own. (Castells 2010, p. xvii) In the last decades, the digital world sometimes expanded or improved upon but mostly replaced the physical one. Communication, media, commerce, even transportation, and tourism (Guttentag 2010, p. 640) are influenced by the digital world. Naturally, from infrastructure to policy and voting systems, governments also have an alternative presence in this new world. (Marchionini *et al.* 2003, pp. 25–26)

The digital world carries its own issues and threats, and it is changing the very nature of society. (Castells 2010) In this sense, the threats of the digital world must be faced at their own merit. If the digital world influences our perception, culture, finances, governance, and much more, it can threaten our security without necessarily posing a physical threat. We must focus on intangible, digital identities and digital assets at risk, as much as the individuals themselves against digital threats. Since the digital world has even more or at least the same level of impact on an individual's welfare, social life, and security, we must consider it not an afterthought or supplement of the physical world but as fundamentally different and equally important.

In this line of thinking, if there is a new realm in which individuals operate, influence, and interact with each other, naturally, other actors of the physical world such as interest groups, companies, radical factions, NGOs, and of course, states themselves have to participate in this realm. While there is much to say about these agents' actions, relations, threats, and advantages in the digital realm, this paper focuses on the relations and impact of the conflicts between states and state-backed groups.

We argue from a systemic approach that this "new world" is intrinsically different from its physical equivalent. Neorealist thinkers such as Kenneth Waltz and John Mearsheimer posited a well constructed and prominent international relations theory mainly focusing on the *structure* of the system and the capabilities of its actors. Terms such as the balance of power or security dilemma are defined or redefined mostly based on the *capabilities* of the actors and the choices they have based on the structure

of the international system. This study's main aim is to show that the system's structural restraints are different regarding the distribution of capabilities in the digital world with some example cases and demonstrating Neorealism still has significant explanatory power in the digital era. We must carefully implement the correct parameters for the digital system structure and its constraints. Since this is a "digital world," there are fundamental differences in restraints set forth by the structure of the system. Actors have almost identical capabilities relative to their physical capabilities, and the structural constraints are much more lax in the digital world thanks to the unprecedented anonymity it provides. These differences bring a plethora of changes forward which will be studied under the relative capabilities of actors and restraints placed by the system regarding anonymity.

This study relies on two arguments. In the digital world, power distribution differs significantly, and second, anonymity is considerably higher than the physical world. First, we will review the traditional approach from a systemic perspective towards the distribution of capabilities in the physical world. Afterward, power distribution in the digital world will be studied with some examples from recent aggressions between states and state-backed groups, including the attacks aimed towards great powers from the middle powers, since the frequency and complexity of these attacks are increasing, while the number of potentially capable actors is also increasing by the day. Subsequently, we will discuss the second argument and try to demonstrate that actors can get away with aggression in the digital world more easily than the physical one thanks to anonymity. In conclusion, we suggest that these variations are strong, prevalent, and broad enough to influence the structure of the system in terms of the distribution of capabilities and polarity of the international system in the digital world.

1. Distribution of Capabilities in the Physical World

Waltz suggested that a structure of a system is defined in three respects. The first is about its order, the second is about the functions of the units within the structure, and the third is about the distribution of capabilities among the units. The first point is undisputedly recognized as anarchy instead of hegemony from a neorealist perspective. The second point is disregarded in anarchic systems since all units are alike and there are no specific functions attributed to a single unit. (Waltz 2010, pp. 100–101) This leaves the third point, the distribution of capabilities, the distribution on the state level influences the structure of the system, and the system, in turn, affects the interactions between states.

Neorealism characterizes power in a way that avoids concentrating on forcing others to do what they wish but instead emphasizes the distribution of capabilities among the actors in the system. Because in international politics, even the most powerful states sometimes end up with unintended results. (Waltz 2010, p. 192) The distribution of capabilities or relative power perspective provides an instrumental framework for assessing power dynamics without worrying about control over the other actors or

intended outcomes. Thus, Neorealism analyzes the relative power of the states within the system. If a state's level of power is meaningful in international politics, it must be compared to others. According to the neorealist theory, there is limited distribution of capabilities in the system. On the one hand, power in the international system is never held by a single actor globally, or "there has never been a global hegemon." (Mearsheimer 2001, p. 41) Conversely, power is always held by a handful of states. Thus the international system has almost always been a small-number system. (Waltz 2010, pp. 192–193)

International politics is defined by the few major actors consisting of states that hold the status of great power. (Waltz 2010, pp. 94–95) This does not mean that great powers are free to do as they wish, of course. They are still bound by both the structural restraints and other relatively big powers. In essence, according to Neorealism, great powers are the only participants whose actions truly matter in terms of systemwide adjustments. Otherwise, states are all similar actors in terms of challenges they encounter or achievements they desire. (Waltz 2010, p. 96) Analyzing the system through this lens, assessing states' relative power, and counting the number of major actors to ascertain the *polarity* of the system is a frequently used method in international politics. While some argue the multi-polar systems are more stable[3], others suggest bipolar systems establish the stage for stability[4]. The emphasis is that they all agree that the polarity of the system influences the decision-making processes of actors significantly.

We must consider the purported capabilities that give a state its power and consequently determine the system's polarity. While there is no consensus on deciding the importance of different forms of capabilities, most of the spotlight is focuses on military capability. However, the other categories, such as economic, demographic, or geographic advantages, are not neglected. Mearsheimer considers these as potential capabilities which could turn into military capability in the future. (Mearsheimer 2001, p. 45) In essence, we would argue that since the capabilities are regarded relatively, any materialistic capability could be considered a source of power for neorealists. Power is considered an instrument rather than an intrinsic goal. Any useful toolset may be viewed as a capability, as long as it provides a potential or imminent application towards the states' goals. Waltz argued that being strong in one category, such as military, economy, or resources, is not enough. We must consider all aspects of power such as population, territory, military, economy, and many more. (Waltz 2010, p. 131) Considering that the balance of power does not change rapidly in any of these categories, one cannot separate these powers. If a state does not rank high in every category, the actions taken in one category can be used against her in the weaker areas. States always try to gain more power, whether it is direct military capacity or latent auxiliary areas, there is a constant struggle for power in the international system.

[3] See. (Kaplan 1957, Deutsch and Singer 1964)
[4] See. (Waltz 1964, Mearsheimer 2001)

There are different explanations for the states' unquenchable thirst for power within Neorealism. Specifically, Waltz focuses on "preserving power" and protecting the *status quo*, while Mearsheimer takes a more offensive approach and argues "maximizing power" is the best recipe for security and survival. (Mearsheimer 2001, pp. 21–22) For this study's scope, we will be focusing on the distribution of power instead of how power should be utilized or why states pursue it. States can focus on internal resources and try to gain more power, or they can focus on the other states and take an offensive approach since their power is meaningful in relative terms. We do not believe these aspects are irrelevant and should be disregarded, but they work in both the physical and digital worlds, and both perspectives have some explanation power depending on the case they are applied. Defensive or offensive, states are always interested in their relative position with others regarding the distribution of power. Although they are in constant strife, the international system remains a small-number system in the physical world. The reason behind this is the obstacles that are in the way of gaining more power.

There is a rising barrier against becoming one of the great powers. Developing modern offensive and defensive military systems requires both tremendous economic strength and leaps in science and technology. (Waltz 2010, p. 181) For example, the United States (US) has been developing various missile defense programs for more than fifty years. (Walker et al., 2003) These programs have a history of years of international and internal cooperation of various governments and branches of the US government relying on vast pools of resources. Hundreds of individuals from different backgrounds poured their time and efforts towards creating various defense systems against intercontinental ballistic missile threats for the US and her allies. However, there are still grave concerns about the effectiveness, feasibility, and costs of such a system. (Fetter et al., 2000) This shows that developing robust military apparatus is an expensive, intensive, and complex goal that only the great powers can achieve in the long term. There is a big gap between states in terms of technology and economic resources. Thus, while all states struggle for power, only a few can gain great power status.

A system consists of a structure and the interrelationship of its parts. While these concepts relate to each other, they are not synonyms. (Waltz 2010, p. 80) The international political system involves interrelationships between the states and the structure and their influence on each other. While Waltz cautions us that the structure is not the aggregate of the interacting parts, he also argues that there is a mutual interaction between the two. (Waltz 2010, p. 99) In Figure.1, we show these forces at play in a hypothetical bipolar international system.

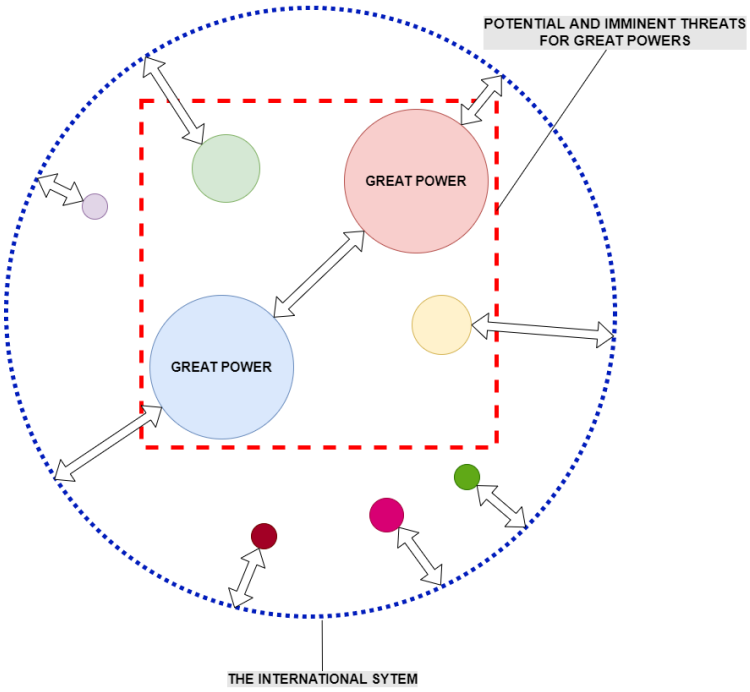

Figure 1 – Hypothetical Bi-Polar International System in the Physical World

Each circle is a state, and the sizes of circles demonstrate their relative powers. The double-arrows show the reciprocating external influences or restraints. While all states influence and being influenced by the system, great powers are only directly concerned with other great powers apart from the system, but they must also keep an eye on the other significant powers even if they are not directly bound by them. Great powers must carefully ponder the intentions or possible reactions of their counterparts first, but they also give some thought to the states within the dashed red box before making significant decisions since even though they are not a direct threat due to the power disparity, but they hold enough power to sway the outcomes of their actions.

In conclusion, Figure.1 shows why Neorealists argue that the great powers are not entirely free to do as they wish. Also, why Waltz believes the small-number systems provide more stability than the big-numbers of the multi-polar world. In essence, if states are never certain of others' intentions, the fewer states within the red box, the better. (Waltz 1964, 2010, p. 173) As mentioned before, there are other views even within the Neorealists, especially Deutch and Singer (1964), who argue the opposite by focusing on balancing, alliance dynamics, and flexibility with the more, the merrier approach. However, as we will discuss in the following sections, anonymity in the digital world makes it much harder to balance against threats.

In the physical world, it is almost impossible for a state to rapidly jump inside the red box due to the barriers mentioned earlier. States within the box enjoy a relatively predictable world as long as they do not misjudge the few states' intentions or capabilities. They know which states pose imminent threats and their relative capabilities. However, we argue this organization is going through a significant change in the digital world. The obstacles of the physical world do not apply to the digital capabilities, so the distribution of power is much more equal. Measuring the relative powers of others is much harder, and threats are posed behind a veil of anonymity in the digital world.

2. Distribution Capabilities in the Digital World

In this part, we will focus on the defensive and offensive *capabilities* of actors in the digital world. The term "*attacks"* is used here to imply actors' unilateral actions with broad implications and great complexity for offense or aggression and "*security"* in the sense of a general suite of defensive applications and methods implemented against said offensive multi-faceted threats in the digital world.

Marcin Kleczynski created a security software called Malwarebytes in 2004 when he was *fifteen years old.* His firm, formally established in 2008, was used to secure more than 250 million computers with about 35 million active users in 2014. In 2019 on average, it was installed 247 thousand times every day on the computers of hundreds of millions of customers, including personal, business, and various agencies. (Tidy 2019) What is illuminating about this example is that a kid who is fifteen can create one of the world's most prominent security software, and this is not an exception. Founder of another world-renowned security firm Kaspersky, Eugene Kaspersky, was twenty-four when he started creating his simple security scripts as a *hobby* while working for the Russian Ministry of Defence. (Schofield 2008) In the traditional world, it is almost unheard of for one individual to create a globally dominant and effective security apparatus with virtually no resources as a pastime. Although these might seem like commercial products for personal use, in the world of information technology (IT), experts use the tools which *work*, meaning the most effective, accessible, and fast solution will be implemented if it is trustworthy. These security solutions have been used either by IT technicians or individual users to protect their devices worldwide. Thus, even individuals with minimal resources can create and implement widely popular security tools for both personal and professional use. In contrast to the physical world, digital security tools are much more accessible.

Digital security systems are neither perfect nor are they always effective. The difference is in the costs of developing and deploying these systems to protect states and their citizens. Digital security is a constant cat and mouse game (Schneier 2004, p. XII), but in the physical world, tremendous advances or investments are needed in many areas of science and technology to create a modern security system of the highest potential. In both worlds, when new threats emerge or the security systems fail, either new systems must be implemented, or existing ones must be rapidly upgraded to provide security. In the digital world, breaches and new threats are as problematic as their physical counterparts, but systems can often be patched much more quickly, and developing alternative systems is relatively straightforward.

Then, one has to ask why governments, businesses, or even individuals struggle with creating secure systems if they are relatively cheaper to develop and deploy? The answer lies in the actual cost of digital security. In the digital world, the actual cost of security is *convenience*. In other words, "Increasing security regularly frustrates end-users" (Schneier 2004, p. XIII), and the digital world was not built for security but ease-of-use. (Nye Jr. 2010, p. 5) There are other costs, of course, every system requires a certain amount of time and investment, but these costs are *relatively* trivial at the state level.

(Nye Jr. 2010, p. 4) One indicator is the US defense budget for 2021. The proposed Department of Defense (DOD) 2021 budget allocates $9.8 billion to the cyberspace domain. In the total budget of $705.4 billion, it is minuscule. Especially when we consider the missile defense systems mentioned before, which are laden with existential problems, have an appropriate budget of $20.3 billion for 2021. (DOD Releases Fiscal Year 2021 Budget Proposal 2020) The US Department of Homeland Security (DHS) budget for the same year draws a similar picture. Around $50 billion general budget and about $1.6 billion for "Securing Cyberspace and Critical Infrastructure." (*FY 2021 Budget in Brief* 2020). After numerous attacks in recent years, such as Russian involvement in the 2016 presidential elections, recent breaches in multiple branches of the US government in 2020, again by suspected Russian attackers (Sanger 2020), and many more. One can not argue that digital security is not an essential agenda for the US. Instead, these numbers show that the problem does not lie in the economic costs for digital security. Research conducted by IBM in 2014 states that "...over 95 percent of all incidents investigated recognize "human error" as a contributing factor." (*Cyber Security Intelligence Index* 2014, p. 3) The takeaway from which we will build upon further in this section is that almost every state can provide an adequate level of security for itself with limited resources in the digital world. The reason behind why this is not generally the case is a whole other subject we will not delve into. What must be noted here is that compared to the physical world, states have much more capability to provide security for themselves and their subjects in the digital world.

The main point here is that *relatively big* powers, not just the great powers, could create somewhat secure systems within their measurable economic and technological capabilities in the digital realm. The technological gaps, decades of research and development, gargantuan amounts of economic investments of the physical world's security approach is not in play in the digital realm. (Nye Jr. 2010, pp. 1–2) There are other obstacles in achieving higher digital security, of course, but being a great power is not necessarily one of them. Since there is no clear and big gap of power distribution between states regarding digital security systems, we should also examine their offensive capabilities.

Similar to security, individuals can wield enormous power in digital attacks. (Nye Jr. 2010, pp. 4–5) An independent research group pointed out how critical US infrastructure, including water distribution and treatment plants, and oil wells, could be attacked easily (Mikalauskas 2020). An actual attacker tried to change the chemical mixture of water supply to dangerous levels in Oldsmar, Florida, one year after the report. The attack was only prevented because a supervisor had noticed the change rather quickly. (Mikalauskas 2021) This is just an example from thousands of similar cases on how individuals can achieve dangerous levels of power. Governments rely on private contractors to develop and manage digital infrastructure, and the responsibility to secure these systems largely falls on to the private sector. (Eichensehr 2016, p. 470) One of the latest breaches in the US demonstrates how governments depend on private contractors for critical infrastructure and how they can spectacularly

fail. Suspected Russian hackers breached the Treasury Department, the Department of Homeland Security, the National Institutes of Health, and other agencies in 2020 because they were all using the same contractor's software for network management. (Geller 2020) The scope of this sophisticated attack and the responsible parties behind it are still being investigated, but it is clear from the level of the complexity of the attack that the perpetrator was a state or state-sponsored group.

The list of agencies above comprises a massive section of the government, and it is believed that the attack was ongoing for *months,* not a single breach of security, and the Russian government is suspected to be the one who orchestrated it. (Sanger 2020) In order to collect such sensitive information from US government branches at this level, the Soviets were required to run multiple expensive and intensive espionage operations over an extended period during the Cold War.[5] Even then, there were numerous unfruitful attempts, and it was an expensive operation for Soviet intelligence. (Parrish 2001, pp. 109–110) In modern-day Russia, there is no longer the same level of interest nor the capability to spare resources as the Soviet Union did in the field of espionage against the US. However, there have been numerous breaches, leaks, intrusions, and interventions occurring in the US in the last decade, many of them supposedly to have been orchestrated by Russia. (Ashmore 2009, pp. 25–26, Shackelford *et al.* 2017, p. 322)

Russia is by no means the only nation that has the capability to punch above her weight. In this new world, even Estonia has been deemed a superpower (Collier 2007) and she has "...signed agreements on developing training and cooperation in cyber security with Austria, Luxembourg, South Korea and NATO" (How Estonia became a global heavyweight in cyber security 2017)**.** Iran's numerous alleged attacks on Saudi oil companies (Perlroth and Krauss 2018) was dubbed the "most destructive acts of computer sabotage on a company to date" (Perlroth 2012), which puts Iran as a significant player on the map. Sony Pictures was hacked in 2014, and 47 thousand social security numbers of US citizens were leaked online. Along with various threats and breaches of sensitive information, the supposed North Korean hack was sophisticated and long-running. (Musil 2014) Many examples can be given, but in summary, the digital realm shows a broader range of diffusion of power. (Nye Jr. 2010, pp. 1–2) We can conclude that many states are more capable of operating in the digital sphere than they are in the physical realm, and thus they can develop or acquire sophisticated technological capabilities to conduct various attacks according to their agenda. Thus this creates a significant difference in the international system in the digital world, as shown in Figure.2[6].

[5] For the extent and depth of Soviet intelligence activities and infiltration of the US during the Cold War see (Romerstein and Breindel 2014)

[6] Number of states and their relative power is not representative of the current international system. The figure here is used only to show the conceptual changes in the digital world, relative to the hypothetical bipolar world shown in Figure.1.

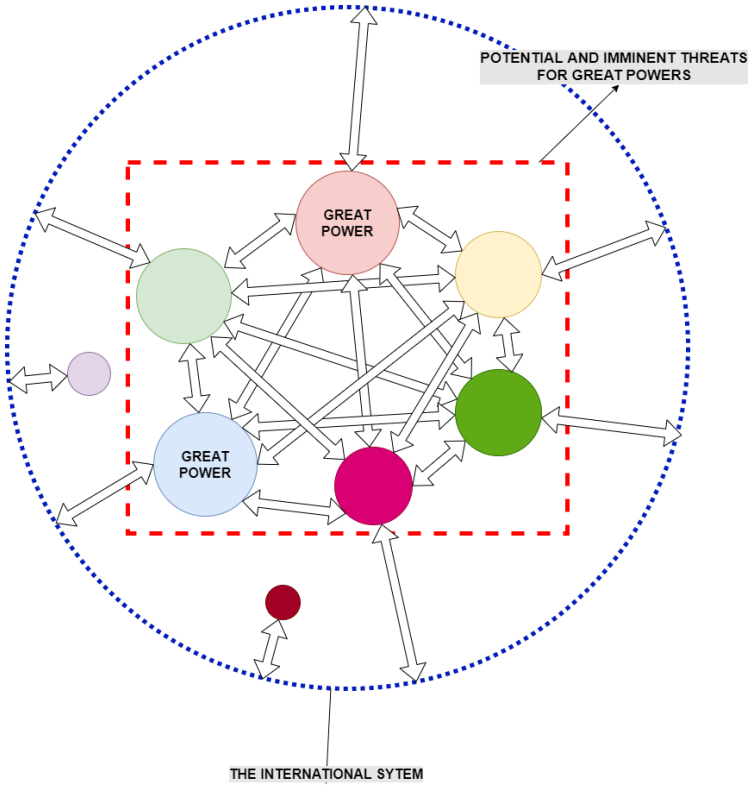

Figure 2 – International System in the Digital World

All the forces and interactions in the physical world are at play in the digital one. We are not arguing against the basic principles of Neorealism. The difference is between the number of highly capable actors. The digital world system is no longer a small-number system. As shown in Figure.2, this creates exponentially complex interrelations. States outside the scope of the great powers in the physical world become significant actors in the digital one. This crowded stage leads to restraining the great powers of the physical world significantly in the digital world.

Today, the distribution of power approach and measuring materialistic capabilities still hold in the physical world, but this new digital era we all face shows that some aspects of power are relatively unimportant. This, in turn, creates a different organization of states in the digital world, as shown in Figure.2.

One has to ask why the great powers of the physical world can not use their superiority by wielding their physical power against digital threats. How can we separate these two worlds? The great powers should be able to punish the digital aggression of a weaker state in the physical world, thus enjoy the same level of security. We argue this is not the case because, apart from the diffusion of power, one other essential difference in the digital world is anonymity. In the digital world, the unprecedented level of anonymity protects actors against possible repercussions, and the interaction of the digital and physical world is limited in terms of reciprocity, as we are going to discuss in the next chapter. While we could not separate the different capabilities in the physical world, the digital one provides this opportunity, at least regarding the costs of gaining more power. Thus, the ranks of great powers are getting crowded by the day in the digital world. (Nye Jr. 2010, pp. 2–3)

In the example cases in this section, the frequent use of the terms “allegedly, supposedly” was a conscious choice by the writers. Even on the individual level, catching and prosecuting perpetrators in the digital world is a tall order at best. Internet Crime Complaint Center (IC3) published a report in 2010 which states that the US Federal Bureau of Investigation (FBI) received 303,809 complaints. Nevertheless, only six convictions were made. (IC3 Internet Crime Report, 2010). Given that these

complaints represent rather severe cases as they were filed with authorities, these figures are eye-opening. On the state level situation is no different, as John Arquilla notes, "Ballistic missiles come with return addresses. But computer viruses, worms, and denial of service attacks often emanate from behind a veil of anonymity." (Geers *et al.* 2014, p. 22) This introduces us to our next point, how anonymity alters the restraints of the anarchic international system.

3. The Veil of Anonymity in the Digital World

States constantly strive to shift the balance of power in their favor, and they only pause when the costs or risks are too high. (Mearsheimer 2001, p. 2) These claims hold for both worlds. However, as shown in the previous chapter, the cost of gaining more power is significantly less than the physical one in the digital world. The costs are internal factors since they involve the state's allocation of resources toward new conducts. However, risks are external since, in most instances, they entail the potential ramifications from other states within the system. Here we are going to study how the risks differ in the digital world for actors.

In the digital world, there is no "return address" for continuous and frequent attacks. Anonymity is an inherent part of the digital world. It is an ongoing debate whether it is the centerpiece of this realm and deserves to be protected under all circumstances or whether it is a calamity and should be restricted and regulated at all costs,[7] but either case does not change the fact that the digital world offers much more anonymity than the physical one, at least for now. This fact alters how actors in international relations evaluate the risks of their actions. The external risk of an attack is the likely counteroffensive action from the target actor, and this is why in determining the strategy for achieving their objectives, states consider both the short-term and long-term consequences of their actions. (Mearsheimer 2001, p. 31) However, when there is a chance of orchestrating an offense without being held accountable, we see more action. State-backed terrorist organizations and proxy wars are prime examples of this. In the physical world, identifying the parties responsible during such operations and presenting tangible evidence is not so difficult as it is in the digital one, so they still present substantial risks and require careful consideration, especially for weaker states. Since the veil of anonymity is much thicker in the digital world, states can take aggressive actions, even towards much greater powers, somewhat frequently, with relatively low risks.

States have different options regarding attacks and counter-attacks between the two worlds. This type of categorization is also used in the physical world, as in seapower, where ships are categorized based on whether they can attack land from sea or directly aimed at controlling seas. (Nye Jr. 2010, p. 5) Figure.2 shows the four possible attack vectors between the physical and digital worlds. The attacks

[7] For further discussion on both perspectives see. (Berthold *et al.* 2000, Davenport 2002, Christopherson 2007)

originating from one world can have targets either within the same world or the other world. In this sense, there are four options.

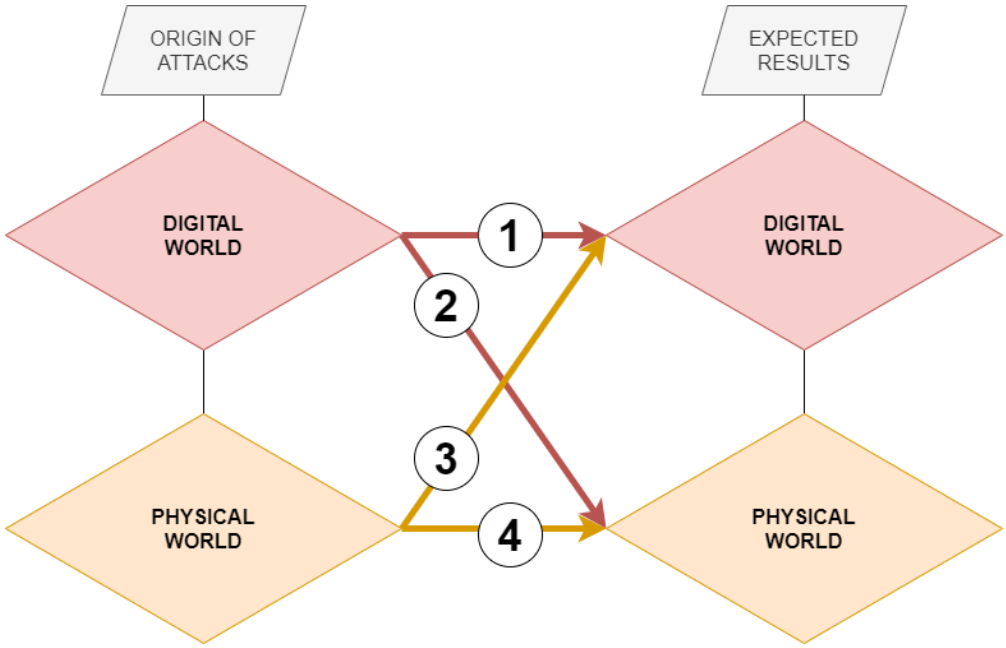

Figure 3 – Attack Vectors by their Origins and Targets Between the Physical and Digital Worlds

These options all have some advantages and shortcomings, but we should categorize the threats or actual attacks to show why some are utilized more than others. The digital to digital attacks (Vector 1) is the most rising and devastating digital threat type in recent years. These attacks target the digital world without direct implications on the physical one. (Nye Jr. 2010, p. 5) Denial of service attacks, ransomware attacks, information leaks, and breaches such as alleged Russian espionage in various US government branches example in the previous chapter, falls under this category. They provide higher anonymity since the perpetuators' intended targets are relatively unknown and dispersed. The information gained by these attacks could be used for various types of future attacks and subversions. The digital to physical (Vector 2) includes digital threats targeted directly to the physical world. Disabling or impeding critical infrastructure is the most common example of these attacks. Attacks against Saudi oil companies or US water treatment plants are included under this category. These provide less anonymity than the second vector since the direct targets provide at least a modicum of information about the possible perpetrators, even if through inference, as discussed below. Vector 3 is the least probable attack type. Attacks are considered under this category when they target infrastructures in the physical world, such as network centers or undersea cables to wreak havoc in the digital world. There is no large-scale example of this vector applied as an attack between states to our knowledge. We will discuss why this vector is practically unusable for great powers to apply their physical power to secure their position in the digital world. The last vector (Vector 4) is the conventional one, direct conflicts originating and resulting in the physical world. Thus, we have this "hourglass" of

attack vectors shown in Figure.3 between the two worlds. The great powers of the physical world have a considerable advantage in vectors three and four, while the distribution of capabilities is significantly balanced in vectors one and two. Attacks originating from the digital world (Vectors 1,2) are relatively anonymous than those originating from the physical world (Vectors 3,4). (Nye Jr. 2010, p. 4,15)

In all of the examples given in the previous chapter, we saw presumed accountability but rarely tangible evidence. This lack of evidence comes from the inherent nature of the digital world. The perpetrators of digital attacks are determined based on a two-step approach, short of a responsible party's statement. First, experts analyze the attack vectors and determine by their sophistication whether an individual or small group could have executed it or whether it is so elaborate there must be a major sponsor behind it. If the latter is true, the second step is based on inference by the intentions and a list of *potentially* capable attackers. (Gusovsky 2016) In the case of Iran's attacks on Aramco oil company, this can be seen clearly. First, experts claim that it was a sophisticated attack. Second, "Security experts said Iran, China, Russia, the United States, and Israel had the technical sophistication to launch such attacks. But most of those countries had no motivation to do so." (Perlroth and Krauss 2018), and it was deemed that Iran was behind the attacks. This approach demonstrates a great deal of ambiguity regarding those who were behind an attack. There are many technical indicators and excellent research on this subject. The claims made by the experts pointing to the responsible parties may be very well primarily valid. However, there are always other possible relatively strong explanations. Since states can never be sure about the intentions of others (Mearsheimer 1994, p. 10) and the intentions can change rapidly (Mearsheimer 2001, p. 31), the process starts on a somewhat subjective basis. Evaluating the capability of the states is a tall order at best in the physical world, even with the aid of satellite imagery, economic indicators, or plain old espionage. It gets orders of magnitudes harder to make a list of capable states who might be responsible for a digital attack with certainty. Experts agree that there might be other explanations and responsible parties behind an attack even in high certainty cases. (Gusovsky 2016) This provides plausible deniability to the perpetrators at an extraordinary level.

Considering that even individuals with limited resources can cause great harm, and even ingenuity or creativity is an asset (Geers et al., 2014, p. 14), the perceived threats of counter-aggression, the external risk, is considerably lower for aggressors. For the target states, the certainty of the actors behind an attack determines the degree of their response. Since the evidence is somewhat ambiguous, they can not use their power to its full extent to counter the attacks. There would be bigger ramifications in the long term for an unprovoked attack on the off chance that they are wrong. Even the great powers are not free to do as they please, and they must consider the risks and costs of their actions. (Waltz 2010, pp. 183–184) Punishing those they *believed* to be responsible for an attack and then proven wrong would cause more issues than it solves. Thus, even when there is a high degree of certainty about the identity of the responsible parties, there is often a relatively tepid response.

Occasionally, the target state considers the evidence that someone was responsible for an attack as convincing and takes action. An example is the North Korean hack of Sony. The US government responded to the attack by imposing new economic sanctions against North Korea. (Acosta and Liptak 2015) Even though it was relatively clear, as far as digital attacks are concerned, who was behind the attack, North Korea repeatedly denied responsibility and demanded proof. (Park and Ford 2015) This demonstrates that states can take the consequences of their digital actions into the physical world, but this is the exception, not the rule. The US has not taken much concrete action against other offenders to this date, and it should be kept in mind that taking action against an already "rouge" state is much less costly and risky. Generally, there are both internal and external forces in play, making it difficult to take action in the physical world against digital attacks. Even there are some exceptions of this, as Waltz puts it, "[...]exceptions fail to invalidate a theory if their occurrence can be satisfactorily explained." (Waltz 2010, p. 20) As stated before, since even the major powers do not operate in a power vacuum, taking tangible actions in the physical world requires both justifying its cost in public opinion internally and contemplating other power's reactions externally.

We pondered before, what happens when a great power is ready to take on the costs and risks and justify its actions domestically and tempted to protect its physical world rank in the digital world? In essence, they can try to secure their position by applying their physical world power to deter or counter the attacks originating from the digital world. However, we argue the hourglass of vectors limits their options considerably. Their physical power enables them to dominate attack vectors three and four. If they choose vector three (physical to digital attacks), the inherent nature of the digital world does not provide a feasible target. Meaning, the internet or digital networks do not follow the political borders of the physical world. In 2012, two undersea cables were damaged in the Mediterranean sea for unknown reasons. This incident directly disrupted services in Egypt, India, Kuwait, United Arab Emirates, and Saudi Arabia while affecting individuals and companies who utilize the services in these countries abroad, from the US to the United Kingdom and Italy. (Severed cables disrupt internet 2008) Incidents such as these show that it is impossible to isolate a digital target for attacks from the physical world. Especially the results will not discriminate between a friend from foe, civilian from military, and even cause issues for the attackers' own subjects. (Nye Jr. 2010, pp. 15–16) Proportionality also would be a huge problem in such a case when The United Nations (UN) considers domestic blocking and filtering of internet access or digital attacks, *regardless of the justification* as a violation of Article 19, Paragraph 3. of the International Covenant on Civil and Political Rights. (Rue 2011, para. 31,52) This is why we argue vector three is not a viable option for deterrence or counter-offense, leaving us with the fourth vector (physical to physical). Would a state have the option of waging war in the physical world against a digital attack? For vector four to be a viable option, multiple issues we raised here must be addressed. First, the responsible parties must be identified with almost concrete evidence, which is close to

impossible, as we discussed above. Second, their connections, backers, and locations have to be brought into the light. Third, the attack must have been devastating to require such a response, which is generally not the case (Nye Jr. 2010, p. 16). Fourth, the responsible parties have to be relatively weaker, so the chance of success high, and the economic and personnel costs of attack is low. Last but not the least, the balance of power in the physical world must permit such an action. In the case of North Korea, surely a digital attack against a US company is not the biggest commited aggression of North Korea, there are many obstacles in the way of waging war against her for the US. So a limited digital attack from North Korea does not provide much more incentive towards vector four on top of the plethora of other current issues already at play. In conclusion, for deterrence or counter-offense against digital threats only viable are the first two which originates from the digital world. Where the ranks of the great powers are very crowded and the physical disparity of power does not apply, and the fog-of-war is significantly thicker.

Thus, in the digital realm, aggression is running rampant relative to the physical realm. Given that both low costs and risks, states can and are taking part in more and more aggressive courses of action toward one another. The thick veil of anonymity provided in the digital world makes finding the responsible parties rather tricky, if not impossible. Occasionally technical analyses supply some fingerprints about the responsible parties, but it quickly turns into finger-pointing. This makes deterrence almost non-existent, especially in limited attacks. There are very few examples of when states decide to counter digital attacks in the physical world because it raises many questions, both internal and external, about proportionality and responsibility, and there no viable attack vectors to wield their physical power to protect them in the digital world.

4. Conclusion

In this work, we argue that today the physical and digital worlds are two different realms. There are strong interactions between the two in many areas. There are both old and new threats in these two worlds, and some attacks are based on only digital gains while others have implications in both worlds. (Nye Jr. 2010, p. 4) However, reciprocity or deterrence is not inclusive of both worlds. The anonymity provided in the digital world and the distribution of capabilities make it challenging even for the traditionally great powers to enjoy relative security provided by their accrued physical power. Since all major powers care about the balance of power, and all compete for supremacy (Mearsheimer 2001, p. 361), this new world will witness both the rise of the numbers of clashes between them and a greater range of attacks in the foreseeable future. The digital world is no different from the physical world in its nature for international politics. On the contrary, it works much the same. The anarchic and self-help system explanation works for both worlds from the neorealist perspective. Changing parameters are measuring the power, deterrence, and power balance in the system. We believe these changes require an adjustment in our perspective while studying international relations in this new era.

There is an increasing trend in the number of attacks in the digital world, while the scope of the attacks is also widening. It turns out that the distribution of power is quite equal in relation to the physical world because more and more states are getting on to the stage with each passing day. (Nye Jr. 2010, p. 9) The distribution of power within the international system is crucial for Neorealism since, traditionally, power was held by only a few states, and the system was relatively stable.

The stability of an anarchic system depends on two main points, first its nature, namely the anarchy, is not changed, and second, the number of main actors is relatively constant. The fulcrum of the changes in the digital world relies on the latter. In the physical world, "[...] no more than small numbers of states have ever coexisted as approximate equals…" (Waltz 2010, p. 132) however, as we saw in the previous chapters, in the digital one, this is not the case. Of course, this does not mean that all actors possess the same capabilities in the digital world, but the number of approximate equals is significantly higher. Considering even individuals or small groups having the capability of causing mayhem without a significant risk of repercussions with relatively limited resources draws a new picture in terms of capabilities in the digital world. Analyzing the system from a Neorealist perspective, we find that we have a multi-polar world in the digital world. This multi-polarity differs from the praised "small numbers," which provide stability. (Waltz 2010, p. 161) Instead, the number of highly capable and powerful states is increasing by the day in the digital world and in a multi-polar world with a large number of relatively close powers, the boundaries between friend and foe start to blur, and dealing with threats and problems becomes increasingly uncertain (Waltz 2010, p. 170).

Traditionally, great powers within the international system enjoyed relative security provided, especially by their rank in superiority in military advancements. The uncertainty, the so-called "fog of

war," was always present, but only a handful of states with the potential to cause considerable harm required their close attention. All states had to carefully consider the implications of aggression toward one another before taking action, especially against a higher power. Although some tools offered a modicum of anonymity and protection from the wrath of great powers, such as proxy wars and state-backed terrorists, the anonymity provided by these methods was relatively limited. While all states yearned for more power or influence, they had to calculate the risks carefully. Meanwhile, the digital world became increasingly pervasive and provided the perfect arena for states seeking more power or space to wield it since it provided the prime conditions for anonymous aggression and comparatively low risks. Considering that the required development time and investment for advanced attacks or security systems are infinitesimal relative to the physical world, states are taking advantage of the digital realm intensively. As a result, we conclude that these changes affect the structure of the international system by increasing the number of greatly capable powers while diminishing the effectiveness of deterrence with the high level of anonymity offered. We must analyze the structure of the international system and the interactions of states in the digital world, bearing these shifts in mind, independently from their conventional rankings in the physical world.

References

Acosta, J. and Liptak, K., 2015. U.S. slaps new sanctions on North Korea after Sony hack [online]. *CNN*. Available from: https://www.cnn.com/2015/01/02/politics/new-sanctions-for-north-korea-after-sony-hack/index.html [Accessed 3 Apr 2021].

Armstrong, M., 2019. All of the data created in 2018 is equal to… [online]. *Statista Infographics*. Available from: https://www.statista.com/chart/17723/the-data-created-last-year-is-equal-to/ [Accessed 4 Apr 2021].

Ashmore, W.C., 2009. Impact of Alleged Russian Cyber Attacks.

Berthold, O., Federrath, H., and Köhntopp, M., 2000. Project "anonymity and unobservability in the Internet". *In*: *Proceedings of the tenth conference on Computers, freedom and privacy challenging the assumptions - CFP '00*. Presented at the the tenth conference, Toronto, Ontario, Canada: ACM Press, 57–65.

Castells, M., 2010. *The rise of the network society*. 2nd ed. Chichester, West Sussex ; Malden, MA: Wiley-Blackwell.

Christopherson, K.M., 2007. The positive and negative implications of anonymity in Internet social interactions: "On the Internet, Nobody Knows You're a Dog". *Computers in Human Behavior*, 23 (6), 3038–3056.

Collier, M., 2007. Estonia: Cyber Superpower. *Bloomberg.com*, 17 Dec.

Cyber Security Intelligence Index, 2014. IBM Security Services.

Davenport, D., 2002. Anonymity on the Internet: why the price may be too high. *Communications of the ACM*, 45 (4), 33–35.

Deutsch, K.W. and Singer, J.D., 1964. Multipolar Power Systems and International Stability. *World Politics*, 16 (3), 390–406.

DOD Releases Fiscal Year 2021 Budget Proposal [online], 2020. *U.S. Department of Defense*. Available from: https://www.defense.gov/Newsroom/Releases/Release/Article/2079489/dod-releases-fiscal-year-2021-budget-proposal/ [Accessed 31 Mar 2021].

Eichensehr, K.E., 2016. Public-Private Cybersecurity. *Texas Law Review*, 95 (467), 72.

FY 2021 Budget in Brief, 2020. Department of Homeland Security.

Geers, K., Kindlund, D., Moran, N., and Rachwald, R., 2014. *WORLD WAR C : Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks*. FireEye.

Geller, E., 2020. How U.S. agencies' trust in untested software opened the door to hackers. *POLITICO*, 19 Dec.
Gusovsky, D., 2016. How investigators decide that a country is behind a cyberattack [online]. *CNBC*. Available from: https://www.cnbc.com/2016/09/19/how-investigators-decide-that-a-country-is-behind-a-cyberattack.html [Accessed 3 Apr 2021].
Guttentag, D., 2010. Virtual reality: Applications and implications for tourism. *Tourism Management*, 31, 637–651.
How Estonia became a global heavyweight in cyber security [online], 2017. *e-Estonia*. Available from: https://e-estonia.com/how-estonia-became-a-global-heavyweight-in-cyber-security/ [Accessed 1 Apr 2021].
Kaplan, M.A., 1957. *System and Process in International Politics*. New York: Wiley.
Lieberman, M., 2013. Language Log: Zettascale Linguistics [online]. Available from: http://itre.cis.upenn.edu/~myl/languagelog/archives/000087.html [Accessed 4 Apr 2021].
Marchionini, G., Samet, H., and Brandt, L., 2003. Digital Government. *Communications of the ACM*, 46.
Mearsheimer, J.J., 1994. The False Promise of International Institutions. *International Security*, 19 (3), 5.
Mearsheimer, J.J., 2001. *The tragedy of Great Power politics*. New York: Norton.
Mikalauskas, E., 2020. Critical US infrastructure can be hacked by anyone [online]. *CyberNews*. Available from: https://cybernews.com/security/critical-us-infrastructure-can-be-hacked-by-anyone/ [Accessed 3 Apr 2021].
Mikalauskas, E., 2021. The Oldsmar water treatment facility hack was entirely avoidable – and it can happen again [online]. *CyberNews*. Available from: https://cybernews.com/editorial/oldsmar-water-treatment-facility-hack-was-avoidable-can-happen-again/ [Accessed 3 Apr 2021].
Musil, S., 2014. Sony hack leaked 47,000 Social Security numbers, celebrity data [online]. *CNET*. Available from: https://www.cnet.com/news/sony-hack-said-to-leak-47000-social-security-numbers-celebrity-data/ [Accessed 1 Apr 2021].
Nye Jr., J.S., 2010. *Cyber Power*. Belfer Center for Science and International Affairs.
Park, M. and Ford, D., 2015. North Korea denies being behind Sony hack [online]. *CNN*. Available from: https://www.cnn.com/2015/01/13/asia/north-korea-sony-hack/index.html [Accessed 1 Apr 2021].
Parrish, M.E., 2001. Soviet Espionage and the Cold War. *Diplomatic History*, 25 (1), 105–120.
Perlroth, N., 2012. In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back. *The New York Times*, 24 Oct.
Perlroth, N. and Krauss, C., 2018. A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. *The New York Times*, 15 Mar.
Romerstein, H. and Breindel, E., 2014. *The Venona secrets: the definitive expose of Soviet espionage in America*.
Rue, F.L., 2011. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development.
Sanger, D.E., 2020. Russian Hackers Broke Into Federal Agencies, U.S. Officials Suspect. *The New York Times*, 13 Dec.
Schneier, B., 2004. *Secrets and lies: digital security in a networked world*. Paperback ed. Indianapolis, Ind: Wiley.
Schofield, J., 2008. The Russian defence against global cybercrime [online]. *the Guardian*. Available from: http://www.theguardian.com/technology/2008/jan/31/eugene.kaspersky [Accessed 29 Mar 2021].
Severed cables disrupt internet, 2008, 31 Jan.
Shackelford, S.J., Sulmeyer, M., Deckard, A.N.C., Buchanan, B., and Micic, B., 2017. From Russia with Love: Understanding the Russian Cyber Threat to U.S. Critical Infrastructure and What to Do about It. *Nebraska Law Review*, 96 (2), 20.
Tidy, J., 2019. 'I kept my multimillion dollar business secret'. *BBC News*, 21 Jul.
Waltz, K., 1964. The Stability of a Bipolar World. *Daedalus*, 93 (3,), 881–909.
Waltz, K., 2010. *Theory of international politics*. Long Grove, Ill: Waveland Press.