CHAPTER 29

GEOPOLITICAL IMPLICATIONS OF CYBERSPACE ON INTERNATIONAL RELATIONS: AN INDEPTH ANALYSIS

Nezir AKYEŞİLMEN

GEOPOLITICAL IMPLICATIONS OF CYBERSPACE ON INTERNATIONAL RELATIONS: AN INDEPTH ANALYSIS

Nezir AKYEŞİLMEN
Selçuk University

Abstract

In digitalization age, the intersection of cyberspace and international relations has become a focal point of scholarly inquiry. This research aims to comprehensively analyse the geopolitical impacts of cyberspace on international relations, recognizing the critical importance of understanding the evolving dynamics in the digital realm. The increasing integration of information technologies into global affairs raises pertinent questions about the nature of state interactions, security paradigms, and the potential for cyber capabilities to reshape power dynamics. The primary objective of this research is to explore the multifaceted dimensions of digitalization on international relations, focusing on both state and non-state actors. The research adopts a mixed-methods approach, integrating qualitative analysis of state policies and strategic documents with quantitative assessments of cyber conflicts and their geopolitical impacts. Through case comparative samples and trend analyses, the study aims to unveil patterns, challenges, and opportunities stemming from the utilization of digitalization in international relations. Anticipated outcomes include insights into the emergence and evolution of cybersecurity in international relations, the identification of cyber power and power redistribution, and an evaluation of the effectiveness of existing international norms and regulations. This research holds significance in informing policymakers, scholars, and practitioners about the evolving nature of global politics in the digital age, emphasizing the imperative for adaptive strategies to address the challenges posed by the growing influence of cyberspace on international relations.

Keywords

Cyberspace, Cybersecurity, Power Redistribution, Cyber International Law, Cyber-Attacks, Stakeholders

DOI: 10.53478/TUBA.978-625-6110-04-5.ch36

Introduction

In the era of digitization, the convergence of cyberspace and international relations has emerged as a central topic of academic investigation. The growing incorporation of information technology into global affairs generates important inquiries regarding the nature of state interactions, security paradigms, and the capacity for cyber capabilities to alter power dynamics (Saaida, 2023). The digital transformation accelerated by the Covid-19 pandemic has prompted international relations scholars to increasingly examine the implications of digitalization for global affairs.

As a result of digital transformation, numerous facets of our daily life have undergone significant changes. It brought about profound changes and transformations in all aspects of life, including the economics, politics, entertainment, business, culture, and the environment. Although digitization offers convenience and comfort in our lives, it also introduces numerous risks and challenges. Today, we have a remarkable technology that enables us to save time, space, and money while offering us swiftness, convenience, and comfort in several domains including education, communication, banking transactions, research and so on. Furthermore, it encompasses a multitude of risks, ranging from the exposure of personal data and privacy breaches to cyber bullying and ransomware attacks (Atrews, 2020). Additionally, it poses concerns such as attacks on industrial facilities and the compromise of national critical infrastructures, such as communication, transportation, energy and financial institutions.

The implications of cyber technology, including the emerging technologies has been transforming dramatically the way international relations functions. This transformation encompasses distribution of power, redefining security, influencing diplomatic relations, the emergence of arms races, considerations of national and global security, the actions of non-state actors and state-sponsored cyber operations, the influence of international norms, the interactions between international actors, the concept of deterrence, and the notion of cyber sovereignty (Stevens, 2021). As digitalization continues to grow worldwide, it is crucial to explore the intricacies of the digital age in order to comprehend the geopolitical implications of this transformation on international relations.

This study utilizes a combination of qualitative and quantitative research methods. There will be an emphasis on literature reviews, policy analyses, and case studies as primary tools for qualitative research. The quantitative method, on the other hand, will make use of information gathered via network analyses, comparisons, statistics, tables and graphics produced by companies and international organization, data on cyber attacks and cyber disputes in international relations, and so on.

The objective of this research is to thoroughly examine the geopolitical implications of cyberspace on international relations, acknowledging the crucial significance of comprehending the changing dynamics in the digital domain. The research will basically seek answers to the following questions. How will cyber technology, including emerging technologies transform traditional power structure in international relations? How do these technologies affect national and international security? What kind of norms, strategies and mechanisms will the international community develop to cope with the challenges posed by cyberspace?

This paper is intended to examine the intricacies of cyber international relations by tracing the development of cybersecurity in the context of international relations. It will cover topics such as cyber wars, espionage, and the vulnerabilities of key infrastructure. Furthermore, it will offer valuable perspectives on the evolution of statecraft, the shifting of power dynamics, the erosion of sovereignty, and the empowering of non-state actors in the digital domain. Finally, it will assess the possibilities of diplomatic collaboration and initiatives to build worldwide norms and standards to tackle the challenges arising from the geopolitical effects of cyberspace on international relations.

Cybersecurity in International Relations

The aspect of international relations that is most significantly affected by digitalization is unquestionably security (Saaida, 2023). The inherent transparency, anarchic structure and open-to-offence nature of cyberspace have exposed it to major security challenges (Akyeşilmen, 2018). Just like in physical international relations, security is a highly comprehensive concept in cyber international relations. It covers a wide range of subjects from cyber conflicts to cyber espionage and surveillance, from hybrid wars to cyber terrorism.

Taking the concept of cybersecurity for granted is a serious challenge. Initially, the primary question need to be explored is "whose security?" The notion of security, has undergone a profound transformation evolving from traditional understanding to more critical perspective in the globalization discussions starting from early 1990s (Gobbiscchi, 2004). This evolution has been further strengthened by the emergence of cybersecurity. Cyber security, therefore, deepens security both on the basis of encompassing new actors and enlarges it on the basis of new security sectors (DCAF, 2019). It also strengthened the interconnectedness of security across all actor and all levels, highlighting that the security of one entity cannot be isolated from others.

Cybersecurity encompasses not only only state security but also the safeguarding of individual security which is closely connected to human security (DCAF, 2019). Therefore, it is highly reasonable to assert that cybersecurity can be also considered as a constituent of human security along the political, economic, health, food, environmental, individual, and societal security (Candra & Wardoyo, 2020).

The Evolution of Cybersecurity

Cyberspace is a real space that produces a vast quantity of information and accommodates an exceptionally large population of users. The cyberspace shares resemblances with physical space, as it encompasses an immense amount of data whose limitations remain unknown. Furthermore, it is continuously growing as each piece of information generated in the digital realm is added to it. According to Internetlivestats (2023), the number of Internet users is estimated to be 5.5 billion, and the daily generation of information exceeds 10 billion GB. To provide a more tangible perspective, this vast quantity of knowledge is approximately equivalent to the combined sum of 170 million resources housed in the US Library of Congress (LCM, 2020) or 20 trillion social media messages. Checkpoint's analysis reveals that on a daily basis, the world experiences an average of 100 million cyber attacks (Avast, 2023), resulting in over 300 thousand websites being hacked (Internetlivestats, 2023) . These data provide insight into the impact of cyber technology at the global stage.

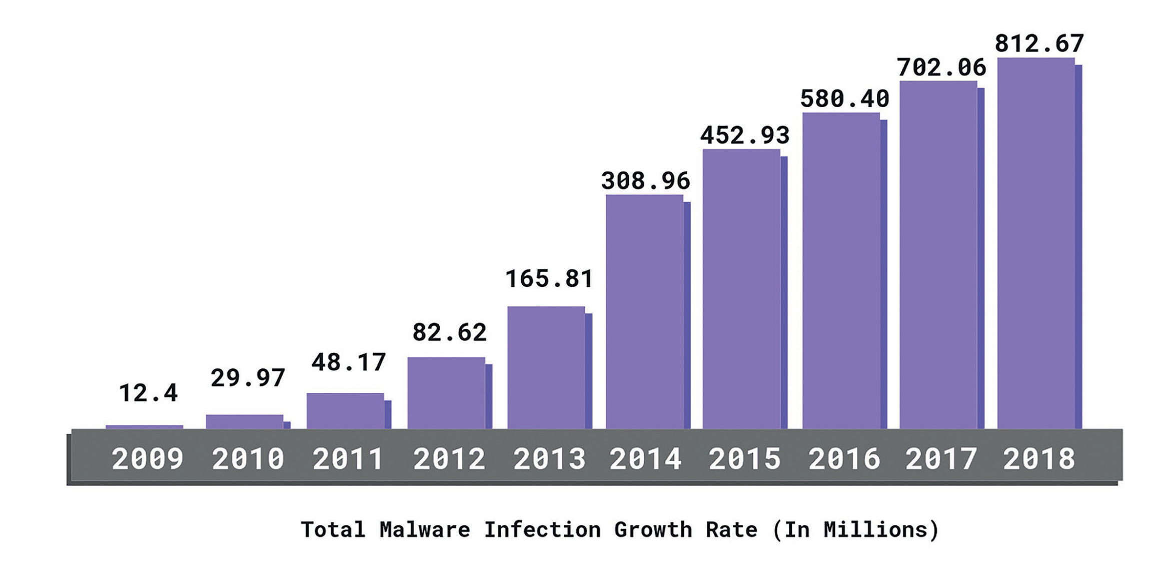
The first internet connection was set up in 1979 and the initial two decades of cyberspace has been peaceful without serious or harmful cyber attacks. Although the first malware, Elk Cloner, released in 1982, it was not a harmful attack (Levy et al., 2020). Due to its transparency and information sharing nature the cyberspace has remained a peaceful domain for the first 20 years.

The first damaging cyber attack known as the Morris worm, was launched in 1989. Approximately 10 percent of all computers roughly around 6.000 computers connected to the internet at that time were impacted (Du, 2021; Kraken, 2019). Following that incident the notion of cybersecurity emerged, mostly at the personal level. Thus, people have become increasingly concerned about the information they produced on their computers and share online. Yet the numbers and types of cyber attacks have significantly increased since then.

In the year 2000, a cyberattack carried on by a 15-year old boy- known as mafia boy- targeted the webpages of major global big-tech companies. " In 2000, a high school student named Michael Calce, who went by the online handle Mafiaboy, brought down the websites of Amazon, CNN, Dell, E-Trade, eBay, and Yahoo!. At the time, Yahoo! was the biggest search engine in the world" (Hersher, 2015). This incident brought about the emergence of the notion of cybersecurity at the network or institutional levels.

The frequency of cyber attacks has significantly risen alongside the advancement of digitalization. According to Figure-1, the daily number of attacks surpassed 2.5 million. However, Avast reports that it experiences over 100 million attacks per day (Avast, 2023). The significant variations can be attributed to disparities in the methods of measurement, sources of data, geographical scope, and organizational policies and thresholds. The field of cybersecurity, as well as cyber attacks, will continue to progress in parallel with the rapid advancement of technology. Consequently, the domain of Cybersecurity will persistently progress and get more complex. To ensure continued success, governments and the international community must be ready to adapt to forthcoming innovations.

Figure 1
Total Malware Infection Growth Rate (in million)

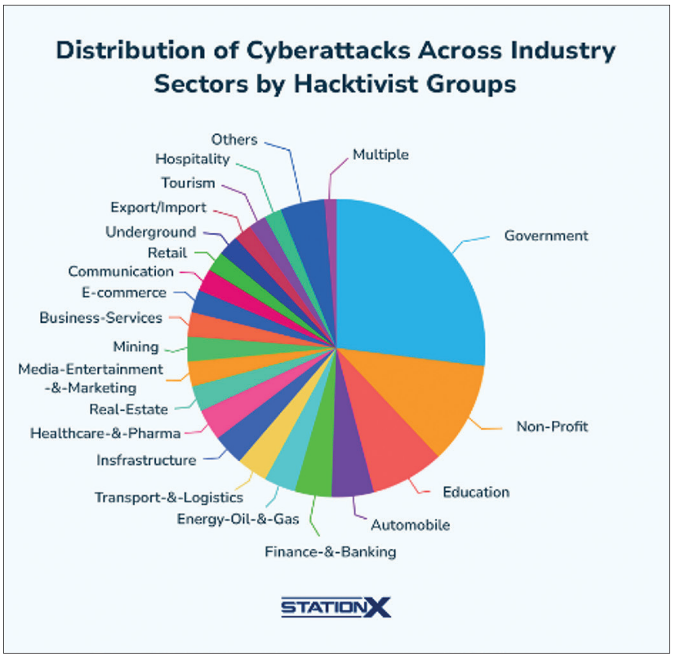


Cyberspace has been considered a long time by the states an issue of low politics or secondary issues in IR such as entertainment, economics, environment and human rights that is not directly related to security, military and strategy (Choucri, 2013). However, following significant cyber attacks on industrial facilities and critical national infrastructures in the late 2000s such as the attacks on Estonia and Stuxnet targeting Iranian nucleer facilities has changed this perception. The DDoS attacks from late March to late April of 2007, "resulting in temporary degradation or loss of service on many commercial and government servers. While most of the attacks targeted non-critical services like public websites and e-mail, others concentrated on more vital targets, such as online banking and DNS" (Ottis, 2018) and Stuxnet worm, another major attacks in IR, targeting Iranian nuclear facilities in 2010 is known as the first cyber weapons due to causing physical damage. Falco (2012) also puts forward that "Stuxnet is a cyber weapon built to sabotage the uranium enrichment centrifuges". After these sophisticated cyber attacks, states have come to recognize cyberspace as an issue of high politics. That means it is now seen directly connected to military, strategy and security concerns.

Consequently, the DDoS attacks on Estonia (2007) has led the development of understanding of national cybersecurity in the Western world. Additionally, the global awareness of national and international cybersecurity has expanded following the Stuxnet attack in 2010. Since then cybersecurity has evolved as a significant, and arguably, the most vital element of both national and international security. Although states traditionally have developed strategy documents that address risks to national security, they have recently began developing a specific national cybersecurity strategy document (ITU, 2024) that address only to cyber risks and threats. In other words, only the field of cybersecurity possesses an exclusive strategy document. This demonstrates the significance and primacy of cybersecurity in the national security landscape.

During the 2010s, there were numerous prominent instances of hacking and attacks that began to impact the national security of countries and resulted in significant financial losses for organizations. Due to the emergence of novel cyber warfare techniques, increasing worries regarding the privacy of personal data, and the substantial dangers associated with corporate data breaches. Therefore, 2010s witnessed numerous notable transformations (Roberts, 2023). Figure 2 illustrates the occurrence of cyber attacks across several industries. Government institutions are at the top of the list, with non-profit associations following closely after. These sectors include education, finance and banking, energy (specifically oil and gas), health infrastructure, media and entertainment, market, mining, e-commerce, and communication.

Figure 2
Distribution of Cyber Attacks Across Industry Sectors by Hacktivist Groups



Undoubtedly, cybersecurity has a significant impact on international security and has emerged as the foremost priority on the global security agenda in the last decade. Cobb argues that cyber conflicts pose the most significant threats to humans, second only to nuclear weapons in the 1940s (Kshetri, 2014, p. 2). Table 1 illustrates the actors involved, methods employed, and the socio-political consequences of each attck. Table 1 encompasses 11 significant international cyber conflicts that occurred between 1986 and 2016.

Table 1
Major Cyber Conflicts Affecting International Relations

Major International Cyber Conflicts					
No.	**Conflict**	**Actors**	**Effects**	**Techniques Features**	**History**
1	*Cuckoo's Egg*	*Markus Hess Clifford Stoll*	*Alarm bells are ringing regarding cyber intelligence and cyber security*	*Unauthorized access with malware*	*1986*
2	*Morris Worm*	*Robert Morris - Cornell University, Barley University, MIT, NASA and Pentagon*	*The first harmful attack created cybersecurity awareness. It brought the issue of internet security to the agenda and caused studies to be initiated in the field of cyber security.*	*DDoS attack*	*1989*
3	*Moonlight Maze*	*Russian Cyber Agents - USA, UK, Brazil, Canada and Germany*	*Provides information about the extent and danger of cyber intelligence*	*APT attack with backdoors*	*1989-2003*
4	*Attack on Multinational Companies*	*Mafia Boy Michael Calce – Amazon, Yahoo, eBay and CNN*	*It has spread out the issue of internet security while creating a concern for corporate and institutional security.*	*DoS attack*	*2000*

5	*China's Cyber Intelligence Activities*	*China's official and private cyber actors - USA, European countries, developed Asian countries*	*Dimensions of global cyber intelligence and China's active stance*	*APT, Backdoors, Trojan*	*2005-2013*
6	*DDoS Attacks on Estonia*	*Estonian Official Institutions, Estonian Private Sector, NATO and EU - Russian Official Institutions, Russia-Supported Hacker groups, Russian Minority in Estonia, Russians in Diaspora*	*Global cyber security awareness has emerged; Cybersecurity has become an element of national and international security; Considered the first cyber war (at least known); NATO invoked Article 5 in cyberspace for the first time; Estonia became the cyber security and defense center of the EU and NATO.*	*Botnet, DDoS*	*2007*
7	*Georgia Hybrid War*	*Russia, Russian-backed cyber actors - Georgia, Georgian civilian actors and Western countries supporting Georgia*	*The first conventional-cyber hybrid war; Awareness of cyber security has increased; Contributed to countries' development of cyber strategies*	*Botnets and DDoS attacks*	*2008*
8	*Stuxnet*	*USA and Israel - Iran*	*It's considered to be the first cyber weapon; It has been revealed that systems that are air gapped or not connected to the internet can also be exposed to cyber attacks. It is one of the first examples of the use of cyber as an offensive tool in foreign policy.*	*Trojan horses, Man in the Middle, Phishing, Social Engineering.*	*2010*
9	*Wikileaks*	*Wikileaks, Julian Assange - USA, England, and many other countries*	*The security of secret-diplomatic correspondence was questioned; Countries searched for more secure means of correspondence and storage, and the power of cyber was realized in diplomacy.*	*Key loggers, Trojans, Social engineering, phishing attacks*	*2011*
10	*Snowden Case*	*Edward Snowden- NASA, GCHQ, USA and England*	*The effects of cyber technology on domestic politics and its reflections on foreign policy*	*Insider attack, decryption of generated digital keys.*	*2013*
11	*Russia's Interference in US Elections*	*Russia- USA*	*Interference in the internal affairs of other countries through cyber means; Concern about interference in elections globally bu authoritarian states*	*Backdoor, Trojans, Social Engineering, and Fishing*	*2016*

Notable cybersecurity incidents depicted by Table 1 are Cuckoo's Egg (1985), Morris Worm (1989), Moonlight Maze (1999), DoS Attack on Multinational Companies (2000), Chinese Cyber Intelligence Activities (2005-2013), DDoS Attacks on Estonia (2007), Georgia' Hybrid Attacks Against a (2008), Stuxnet (2010), Wikileaks (2011), Edwards Snowden Affair (2013), and Russia's Interference in US Elections (2016).

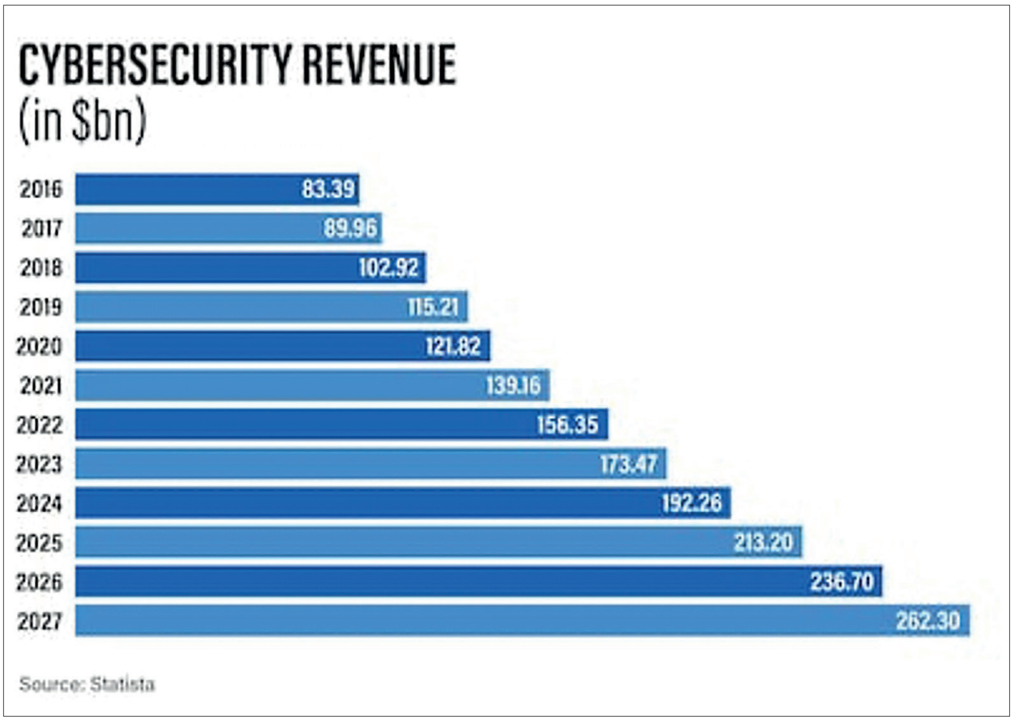
Coursera reports that while malware, phishing, spoofing, backdoor Trojan attacks, ransomware, password attacks, Internet of Things attacks, crypto jacking, drive-by downloads, and denial-of-service attacks are the most prevalent cyber attacks in 2024 (Coursera, 2024), there are tens of thousands of different types of cyber attacks, both large and small.

Cyber attacks have unquestionably a concern for individuals, small businesses, major organization and governments. The projected cost of cybercrime is estimated to reach 14.57 trillion dollars in 2024, with an anticipated increase to 23.82 trillion dollars by 2027 (Sharlton, 2024). Cybercrime, cyber espionage, and other criminal cyber operations, which some refer to as "the most significant transfer of wealth in human history" (McAfee, 2013).

To mitigate substantial expenses and maintain a safe online environment, numerous highly efficient cybersecurity solutions have been developed in recent years. Implementing cybersecurity measures can be quite expensive as depicted in Figure 3. Furthermore, there is no guarantee that these items will provide security. Since, cybersecurity encompasses not only technical aspects but also social elements, such as social engineering, and political factors, including legal and administrative regulations. The risk is significantly elevated, particularly if the user lacks awareness and knowledge, regardless of the number of technical measures employed. There is an often used phrase that "The user is the weakest link in cybersecurity."(Akyeşilmen, 2018). Hence, user training, particularly about social engineering such as deceit, manipulation, and exploiting susceptibilities, unequivocally exemplify this reality.

According to Statistics illustrated in Figure 3, the revenue of the worldwide cybersecurity industry is projected to increase to $262.3 billion by 2027, which represents a growth of over 32% compared to the 2024 year's revenue of $236.30 billion (Sharma, 2023).

Figure 3
Cybersecurity Revenue



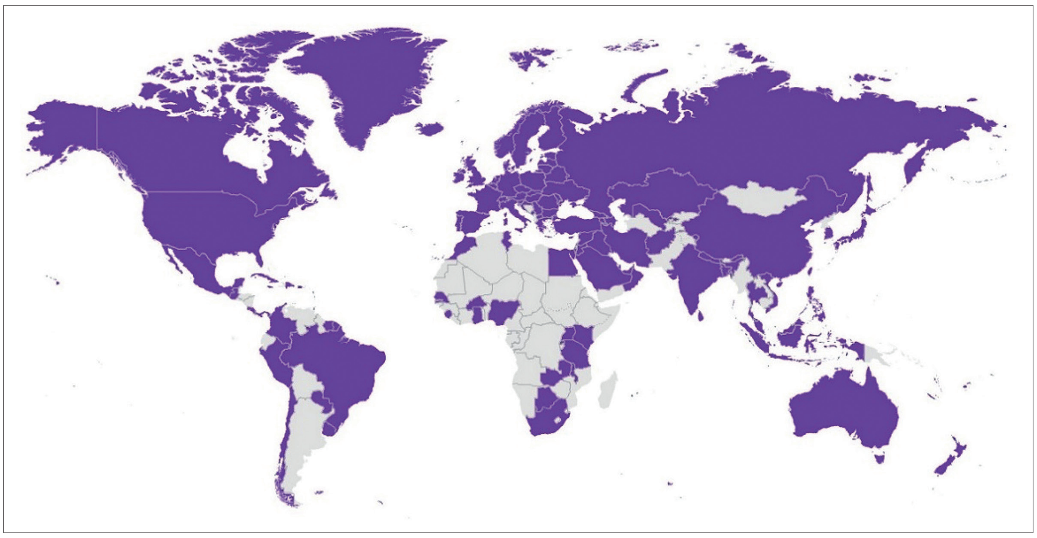
Cybersecurity Measures

Although cyber security measures require different applications at different levels and for different actors, they generally form a whole. The most efficient means of safeguarding against interconnected security issues at personal, organizational, societal, national, and global scales lie in the collaboration and collective actions undertaken by all these stakeholders. However, if a general framework is to be drawn, since the individual is the weakest link in cybersecurity, awareness and training activities at the individual level are vital. A useful approach in this matter is providing education that instructs individuals on the ethical, safe, and responsible use of cyberspace. This type of education is referred to as global citizenship education by the OECD (2019) and as digital citizenship education by the Council of Europe (2019).

Nationally, the most efficient approach is the implementation of national cyber security strategies (ITU, 2024) that have become widespread globally in the last decade. National cyber security strategy documents are measures taken for cybersecurity that encompass the legislative and administrative regulations, technical measures, institutional structures and mechanisms, capacity building (including technical and awareness training), and cooperation amongst all stakeholders including governmental agencies, NGOs, expert associations, and international actors. The ITU national cybersecurity guide identifies these as the five fundamental principles of cybersecurity measures (ITU, 2011).

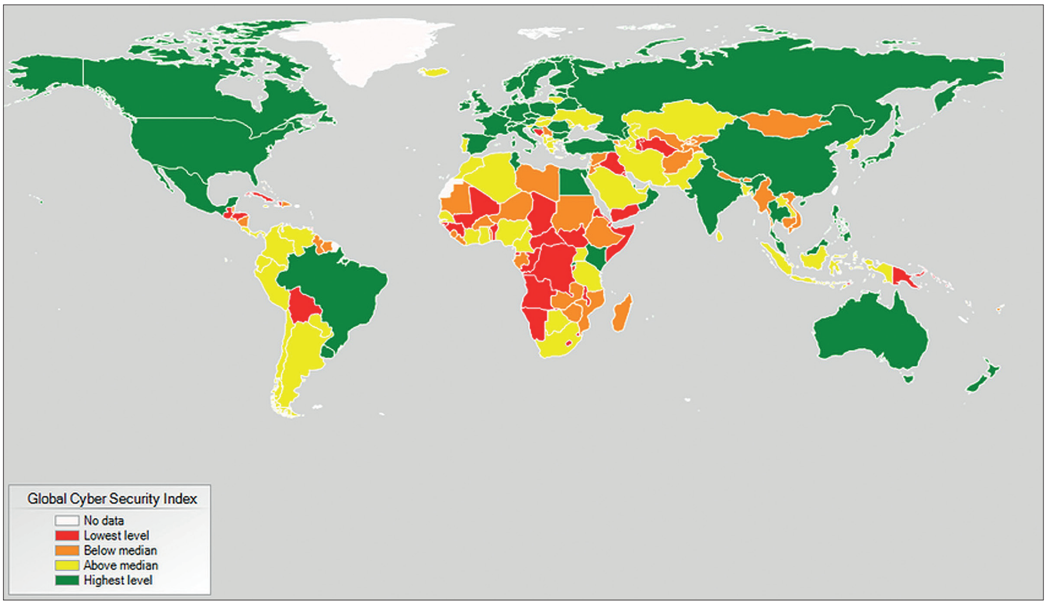
The number of states with national cybersecurity strategies has tremendously increased since 2010 as depiceted in Figure 4.

Figure 4
Map shows the states with National Cybersecurity Strategies



The ultimate approach to addressing cybersecurity, a global problem, is through international collaboration and comprehensive global strategies. Global cyber good governance is essential in this context. Within this framework, it is necessary to establish international agreements, institutions, methods, practices, and the exchange of good practices in order to ensure cybersecurity. This cooperation should involve all stakeholders in the cyber domain.

Figure 5
ITU Global Cybersecurity Index – 2018



The Figure 5 depicted that countries colored green are considered to be secure, while those colored yellow are relatively less secure. On the other hand, those colored orange and red are deemed to be risky. The table is based on 25 indicators and organized into 5 pillars. These pillars are legal measures, technical measures, institutional measures, capacity building, and cooperation of stakeholders. The 2020 index ranks the top 10 countries based on these indicators: USA, United Kingdom, Saudi Arabia, Estonia, South Korea, Singapore, Spain, Russia, United Arab Emirates, and Malaysia. The majority of the countries at the bottom of the list are located in Africa (ITU, 2020).

Cyber Technology and Power Redistribution in International Relations

Cyber technology has profoundly impacted the power dynamics in international relations, leading to a redistribution of power among states, non-state actors, and other cyber international actors. One of the crucial geopolitical implications of digitalization on International Relations is asymmetric power distribution, the rise of cyber powers, and the empowering of non-state actors including individuals. Some other related impacts are espionage and information warfare, attacks on national critical infrastructures, and the erosion of sovereignty.

To fully grasp the magnitude of change and the redistribution of power among international actors or stakeholders, it is helpful to examine a scenario that exemplifies the empowerment of non-state actors, specifically individuals. It is now normal for a person, or even a kid, to inflict as much damage on a state as they would on another state. This was exemplified in the case of Kane Gamble, who successfully hacked into the personal accounts of CIA Director John Brennan in 2015 and released information of thousands of agents and ten thousands of confidential documents on Iraq and Afghanistan wars (Paganini, 2018).

Cyberspace, unlike physical space, is a man-made space. The US Department of Defense has developed internet for defensive purposes in 1969, but it was later opened to private companies and commerce in the 1990s. Today, the driving force of cyberspace is private sector consisting of so called big-tech companies (Paganini, 2022). Thus, the most powerful actors in cyberspace are Microsoft, Amazon, Google, Apple, IBM, Cisco Systems, Palantir Technologies, NortonLifeLock, CheckPoint and Fortinet (IRSEM, 2024). States have neglected this area for a long period of time because they considered it as a domain of low politics (Choucri, 2013).

Currently, private companies are the ones that develope new products, leading innovation, and making significant investments in cyberspace, including emerging technologies. For instance, the metaverse, which is the most recent version of the internet with 3D, was exclusively produced by private enterprises. States appear to be very weak in this sector compared to companies. Once again, at the onset of the global covid-19 pandemic in 2020, schooling worldwide has to transition to online platforms. However, no nation possessed the adequate infrastructure to fully conduct education through online means. Global education, including major nations like the USA, China, and Russia, had to rely on private sector platforms such as Zoom, MS Teams, and Google Meet to conduct education (Vorina et al., 2022).

Thus, cyberspace or cyber international relations differ from physical international relations in terms of borders, effectiveness of traditional regulations, weakening of sovereignty and the impact of nation states. In other words, the cyber international relations, unlike physical IR, is not a state centric domain (Akyeşilmen, 2018). States do not hold the highest level of power in this realm. Although states possess regulatory, order-making, and control powers in physical international relations, they have challenges in establishing order in cyberspace due to the absence of borders and the limitations of traditional legal and administrative rugalations. They, indeed, rely on companies for various matters such as software, hardware, data flow, communication platforms etc. Due to this rationale, there are private big-tech companies that rival and surpass states in this domain (Paganini, 2022). By operating in this manner, these corporations impose restrictions, confine, and pose a challenge to the sovereignty of nation states.

Cyber as a Power Input in International Relations

Undoubtedly, one of the geopolitical consequences of cyberspace on international relations is the generation of power. Traditionally, the elements of power were limited to military capabilities (Jablonsky, 2008), economic resources, population size, geographical advantages, and cultural factors. However, with digitalization, cyber technology has become an additional element of power (Albakjaji & Almarzoqi, 2023). Cyber power, in this context, refers to the capability of international actors in the digital domain to effectively utilize cyber technology, possess significant capabilities in both offensive and defensive cyber operations, and demonstrate expertise and competences in cyber-related skills. The literature now explores the notions of cyber power and even cyber superpower, which pertain to the capabilities and deterrent abilities of actors in the cyber domain.

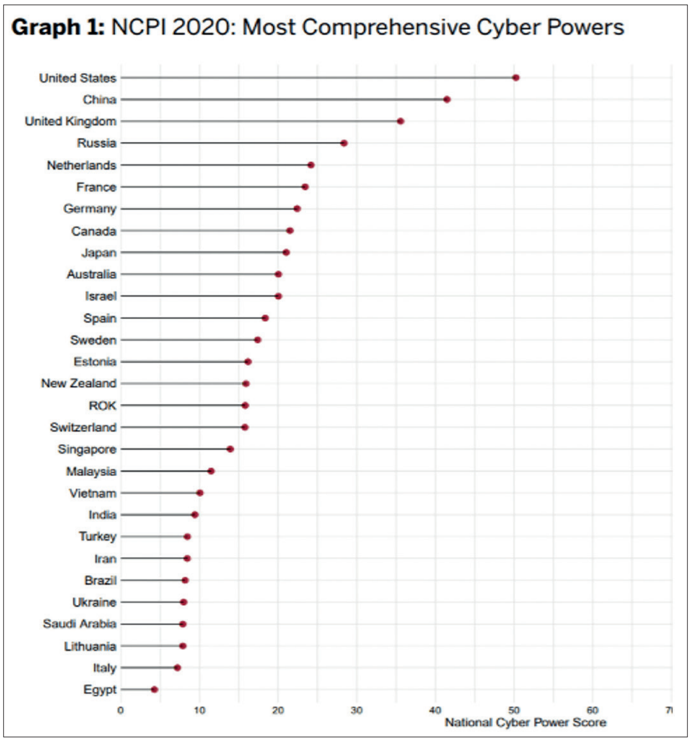
Referring to Voo, Akyeşilmen defines cyber power as:
capabilities to achieve their intended objectives. Cyber capabilities relate to the creation, control and communication of electronic and computer-based information infrastructure, networks, software, and human skills. Therefore, countries invest in a wide range of resources including areas such as military cyber capabilities, cyber defense, and surveillance, but also in human capacity, institutional strengthening, and domestic policy. (Akyeşilmen, 2022)

The National Cyber Power Index (NCPI), created by the Cambridge Belfer Center, assesses the cyber capabilities of 30 countries by evaluating their pursuit of seven national objectives through cyber methods. The following items are:

- *Surveilling and Monitoring Domestic Groups*;
- *Strengthening and Enhancing National Cyber Defenses*;
- *Controlling and Manipulating the Information Environment*;
- *Foreign Intelligence Collection for National Security*;
- *Commercial Gain or Enhancing Domestic Industry Growth*;
- *Destroying or Disabling an Adversary's Infrastructure and Capabilities*; *and,*
- *Defining International Cyber Norms and Technical Standards* (*Voo*, 2020; *Akyeşilmen*, 2022).

NCPI analyzes countries' intent and capability in various areas, including surveillance, defense, control, intelligence, trade, offense, and norms.

Figure 6
NCPI 2020: *Cyber Powers*



The countries with the highest level of intent and capabilities across all seven objectives, ranked in order of comprehensiveness, as depicted by the Figure 6 (Voo, 2020), are as follows: United States (50), China (47), United Kingdom (41), Russia (29), Netherlands (25), France (24), Germany (23), Canada (22), Japan (21), and Australia (20). Turkey is positioned 22nd out of 30 countries, with a score of 9. Turkey's rankings in each sub-section are as follows: surveillance (19th), defense (21st), information control (28th), intelligence (27th), commerce (29th), offense (19th), and norms (21st).

Cyber International Norms as a Global Cyber Governance Issue

In today's digitally-enriched world, developing international norms and rules that will relatively ensure order and stability in cyberspace stands out as a critical and global issue for cyber governance. It is essential to develop global codes of conducts so that stakeholders can engage responsibly and safely in cyberspace (BGF, 2015). Traditional state-centric structures and norms are far from regulating cyberspace. Because there are no borders in cyberspace, there is no sovereignty in the traditional sense, the level of anarchy is much higher, the nature of cyberspace is open to offence, and non-state actors are much powerful. Therefore, it is challenging to establish new regulations and standards that accommodate each of these distinctive characteristics.

Cyberspace is distinct from air, land, sea, and physical space, as it exists in a separate realm with a unique dimension. It is a worldwide physical and social network that is built on a man-made technology, and largely exists in a virtual domain (Fourkas, 2004). As technology rapidly advances, it also creates new challenges in various aspects of social life, which is governed by a system of laws, institutions, principles, and norms. Due to the disparity in speed, cyber technology undergoes rapid development and transformation, whereas social and legal change and transformation occur at a far slower pace. Thus, formulating regulations that align with technology is a significant challenge. Furthermore, the perception of societies and states in cyberspace, as well as their respective interests in this domain, exhibit significant variations. Undoubtedly, the anarchic nature of cyberspace that is open to offence is an additional challenge (Akyeşilmen, 2018). Moreover, traditional legal systems and societal standards may prove to be less efficient or entirely ineffective in some aspects of this domain. Consequently, it becomes increasingly challenging to set the necessary legal and administrative standards required to protect and promote a more harmonious online world.

Although cyber technology, which has been around for 55 years and has been widely used globally for 25 years, there is currently no universally applicable legal framework regulating it in place. While some legal regulations have been implemented at national and regional levels, the most efficient approach to establishing order in the global network, which is a worldwide issue, can only be achieved through a global cooperation and legislation. In today's world, it is common to find several cyber laws and administrative rules in every country, that regulate different aspects to varying degrees (Jayan, 2011). Every country has formed these regulations, although only to a certain extent, based on its particular capabilities and requirements. In the absence of a global agreement, nations attempt to regulate cyberspace and, in some instances, regional levels can only be partially effective (Akyeşilmen, 2018).

International cyber law can be analyzed from two distinct perspectives: regional and global mechanisms. Although regional mechanisms are undergoing development, a global cyber law regime is far from being realized (Akyeşilmen, 2018). Various regional regulations have been enacted to address cyber crimes, such as the Council of Europe's Convention on Combating Cyber Crimes (also known as the Budapest Convention), legally binding directives from the European Union, the Personal Data and Cyber Security Convention of the African Union, and a legal regulation on cyber security by the Arab League. While these achievements hold significance, they are inadequate and fall short of making a worldwide influence.

Since the early 2000s, when cyberspace began to be debated and cybersecurity posed serious threats, significant regulations have been enacted at the regional level, albeit not effectively (Jayan, 2011). The main regulations implemented within this framework include (Schjolberg, 2017; Akyeşilmen, 2018):

- *The Council of Europe Convention on Cybercrime* (2001);
- *The Shanghai Cooperation Organization (SCO) -The Shanghai Convention on Combatting Terrorism, Separatism and Extremism* (2001);
- *The OECD Policy Guidance on Online Identity Theft* (2008);
- *The Shanghai Cooperation Organization (SCO) - Cooperation in the Field of Information Security* (2008);
- *The League of Arab States Convention on Combating Information Technology Offences* (2010);
- *HIPCAR – Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean* (2012);
- *The European Union Directive on attacks against information systems* (2013);
- *UNODC Expert Group comprehensive study on cybercrime* (2013);
- *African Union African Union Convention on Cyber Security and Personal Data Protection* (2014);
- *The Commonwealth - Report of the Working Group of Experts on Cybercrime* (2014)

The number of countries that have signed, ratified, or become parties to at least one of these regional regulations has exceeded 125 (Schjolberg, 2017). Despite being fragmented and scattered, these regional regulations will contribute to the development of global cyber law. Despite all these constructive efforts, there seems to be a reluctance at the international level to negotiate or establish an international agreement or regime in cyberspace (Akyeşilmen, 2018).

The United Nations, on the other hand, lacks a substantial organizational framework, with only a limited number of non-binding resolutions made in the General Assembly pertaining to cyber security. Other steps taken by the UN include, a) a comprehensive study on cybercrime by the UN Office on Drugs and Crime - UNODC Expert Group (2013), and b) The Global Cybersecurity Agenda among Member States on Cybersecurity issues was adopted by the ITU in 2007 (Rossini and Green, 2015).

At the UN level there are not only some soft law regulations, but also a few week institutional initiatives. There are administrative and consultative bodies such as the Internet Governance Forum (IGF) operating under the ITU's jurisdiction. "The United Nations Internet Governance Forum (IGF) serves to bring people together from various stakeholder groups in discussions on digital public policy. While it does not produce negotiated outcomes, the IGF informs and inspires those with policy-making power in both the public and private sectors" (IGF, 2024). Nevertheless, it is imperative that a succession of legally enforceable treaties be established within the United Nations, an organization with worldwide representation. The primary issue in the United Nations arises from the divergence in perception and approach to cyberspace among power blocs within the UN. China and Russia's efforts to monitor and regulate cyberspace, as well as their attempts to participate in US-based NGOs like ICANN and Internet Task Force (Akyeşilmen, 2018), which have a limited role in Internet governance, have not been successful so far.

In addition to the limited legal regulations mentioned above, it is also possible to mention some non-governmental and business initiatives developing some conduct and ethical norms in cyber domain. The Tallinn Guide is a very crucial initiative in this context. Today, "The Tallinn Manual has become an influential resource for legal advisers and policy experts dealing with cyber issues" (CCDCOE, 2024). Again, some common ethical regulation initiatives of international organizations and big-tec companies, and some codes of conduct developed by professional organizations and business circles operating in the field of cyberspace are crucial regulations as soft law. For instance, The Ethics Code of Conduct for Cyber Peace and Security developed by Boston Global Forum (BGF, 2015), NCSC Code of Conduct by National cyber Security Center (NCSC, 2018) and code of Conduct and Ethics Policy by MSC are a few of time. Perhaps they can also be a source of binding law in international relations in the coming decades.

States need to promptly recognize the significance of regulating cyberspace. Cyberspace should be regarded by states as an extra-legal domain (Holder, 2022). This is primarily due to the fact that they have lagged significantly behind the private sector in this domain. They lagged behind private companies in numerous areas as a result of their protracted ignore of this realm, perceiving it as a domain of low politics (Choucri, 2013). They are currently making concerted efforts to overtake competitors in cyberspace. They are not inclined to be constrained by legal regulations, which would impede their progress. As a result, they refrain from establishing legally enforceable standards.

Metaverse technology, however, has demonstrated that this endeavor is in vain. Notwithstanding these endeavors, every metaverse platform was created by private companies. Big-tech companies serve as the primary catalysts and pioneers of advancements and innovations within this domain. It is in the best interest of the entire world that nation states realize this.

It has also been emphasized before that cyberspace is a multi-stakeholder realm and that is not a state-centric structure and that the strong actors in this field are companies. Therefore, the cyber international law making process must also adopt this change. In other words, the traditional legal understanding that only considers the state as the subject of international law should be abandoned, and international organizations, especially big-tech companies, expert associations, and NGOs operating in this field should be included in this process. It is difficult for legal and administrative regulations to be effective by ignoring other stakeholders (we do not call it non-state actor because cyberspace is not state-centric domain. The state is just one of the stakeholders there).

Legal and administrative regulations and mechanisms made with cooperation of all stakeholders at the global level can establish a more successful cyber order (Buchan, 2016). However, states still refuse to be equal with other stakeholders because they do not want to give up their traditional understanding of sovereignty. They do not want to come together as equal actors on international platforms. They do not want to transfer the international regulatory authority they have, even to a limited extent. They also want to maintain their patronage position in cyber international relations. However, states are no longer the bosses in this field. So to speak, they are now in the position of poor masters in this domain. But they haven't realized this yet. Once they realize it, perhaps they will become willing to cooperate.

Only through the establishment of a global cooperation, integrated, and holistic mechanism comprised of all stakeholders—including experts, NGOs, international organizations, and behemoths—is an effective and functional cyber law feasible (Buchan, 2016). Both a national cyber law system and a global mechanism face significant challenges in establishing and maintaining secure cyberspace. It is virtually unfeasible for a national cyber law system to ensure cyberspace security in the absence of a global system. By incorporating regional mechanisms into these two tiers, the three-tiered mechanisms ought to function synergistically and in conjunction. Nevertheless, although it is presently feasible to discuss moderately developed regional mechanisms and national systems, the existence of such a regime on a global scale is difficult to ascertain (Akyeşilmen, 2018).

Conclusion and Evaluation

The process of digitalization has significantly transformed the way international entities interact with one another, leading to extensive geopolitical implications of cyberspace on international relations. Primarily, the rise of cybersecurity as a significant concern for both states and non-state actors, the shifting balance of power that empowers non-state actors to challenge state influence in cyber international relations, and the absence of a comprehensive framework of cyber international law governing interactions in cyberspace are prominent issues that require attention.

The subject of cybersecurity as a critical concern in international relations dates back to the 1990s. However, it became a worldwide issue in the 2010s when Estonia experienced DDoS attacks and Stuxnet targeted Iranian nuclear facilities. Cyberspace, being vulnerable to offense, experiences a wide range of cyber attacks, including those sponsored by governments, cyber surveillance, attacks on key infrastructure, and attacks on industrial facilities. The rise of non-state actors has led to asymmetric attacks, posing challenges to the order and stability of cyber international relations. The necessary actions span from educating individuals about digital citizenship to implementing national cybersecurity strategies and establishing global cyber governance based on international cyber law through global cooperation among all stakeholders.

One additional geopolitical obstacle we have in cyber international relations is the problem of power redistribution. Cyber technology has introduced a new aspect called cyber power to the conventional aspects of power, encompassing military, economy, geography, and population. Cyber technology grants power to all stakeholders in cyberspace, including states. However, it seems to disproportionately benefit non-state actors such as private companies, international organizations, hacker groups, and even individuals. The redistribution of power presents a significant challenge to the field of International Relations, as it fundamentally alters the global balance of power.

The emergence of cyber international law is a significant geopolitical consequence of the use of cyberspace in the field of international relations. The field of traditional international law faces challenges in effectively addressing cyber threats and attacks, making it difficult to establish order and governance in cyber international relations. The necessity for a new global cyber law is evident. However, due to the absence of agreement among actors in the digital realm, the international community has been unable to establish universally binding treaties within the framework of the United Nations. While there are certain legally enforceable norms at the regional level and national legislation in place, they are inadequate in ensuring order in cyber incident response and establishing effective global cyber governance. Given that cyberspace is a worldwide network, it necessitates global cooperation among all stakeholders involved, including not only states but also private big-tech companies, international organizations, expert associations, NGOs and other relevant actors.

References

Akyeşilmen, N. (2018). *Siber politika ve siber güvenlik*. Orion.

Akyeşilmen, N. (2022). Türkiye in the global cybersecurity arena: Strategies in theory and practice. *Insight Turkey, 24*(3), 109-134. https://www.insightturkey.com/file/1483/turkiye-in-the-global-cybersecurity-arena-strategies-in-theory-and-practice

Albakjaji, M., & Almarzoi, R. (2023). The impact of digital technology on international relations: The case of the war between Russia and Ukraine. *Access to Justice in Eastern Europe*, 2(19), 1–17. file:///C:/Users/User/Downloads/The_Impact_of_Digital_Technology_on_International_.pdf

Atrews, R. (2020). Cyberwarfare: Threats, securıty, attacks, and impact. *Journal of Informatıon Warfare*, 19(4). https://www.jinfowar.com/journal-issue/volume-19-issue-4

Boston Global Forum (2015). *The ethics code of conduct for cyber peace and security* (*ECCC*). https://bostonglobalforum.org/mdi/wp-content/uploads/sites/15/ECCC-Sep-2015.pdf

Buchan, R. J. (2016) Cyberspace, non-state actors and the obligation to prevent transboundary harm. *Journal of Conflict & Security Law, 21*(3), 429-453. https://eprints.whiterose.ac.uk/103386/11/Buchan%20FINAL%20Cyberspace.pdf

Candra, D. S., & Wardoyo, B. (2020). Implementing human security measures in the cyberspace: Navigating through the institutional and regulatory disarray. *IR-IU Commentaries, 1*(9), 1-5. https://ir.fisip.ui.ac.id/wp-content/uploads/2020/10/ToPublish_vol1.no9_Human-inSecurity-in-Cyberspace_Oct20_02.pdf.

CCDCOE (2024). *The tallinn manual*. https://ccdcoe.org/research/tallinn-manual/

Choucri, N. (2013). *Cyberpolitics in international relations*. précis, MIT Center for International Studies, Spring 2013, 6–10, & 28. https://dspace.mit.edu/bitstream/handle/1721.1/141672/Choucri%20%282013%29%20Cyberpolitics%20in%20international%20relations.pdf?sequence=1

Council of Europe (2019). *The reccommendation of developing and promoting digital citizenship education*. https://search.coe.int/cm#{%22CoEIdentifier%22:[%2209000016809 8de08%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}

Coursera (2024). 10 *common types of cyberattacks and how to prevent them*. https://www.coursera.org/articles/types-of-cyber-attacks

DCAF (2019). *Guide to good governance in cybersecurity*. Geneva Centre for Security Sector Governance. https://www.dcaf.ch/sites/default/files/publications/documents/CyberSecurity_Governance_ENG_Jan2021_0.pdf

Du, W. (2021). *Morris worm attack lab*. https://seedsecuritylabs.org/Labs_20.04/Files/Morris_Worm/Morris_Worm.pdf

Falco, M. (2012). *Stuxnet fact report*: *A technical and strategic anaysis*. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf

Fourkas, D. (2004).*What is Cyberspace*? WACC. https://www.researchgate.net/publication/328928631_What_is_'cyberspace'

Gobbicchi, A. (2004). *Globalizatin, armed conflict and security*. Rubbettino. https://www.files.ethz.ch/isn/137879/ricerche.04-Globalization.pdf

Hersher, R. (2015, February 7). *Meet mafiaboy, the 'Bratty kid' who took down the internet*. Npr. https://www.npr.org/sections/alltechconsidered/2015/02/07/384567322/meet-mafiaboy-the-bratty-kid-who-took-down-the-internet

Holder, M. (2022). Cyberspace in a state of flux: Regulating cyberspace through international law. *Groningen Journal of International Law, 9*(2), 266-280. https://ugp.rug.nl/GROJIL/article/view/38689

Internet Governance Forum (2024). *About IGF*: *Internet governance forum*. https://www.intgovforum.org/en/about#about-us

IRSEM (2024). *Big Tech as an actor of global security and geopolitical conflicts*. https://www.irsem.fr/media/appel-contributions.pdf

ITU (2011). *ITU National Cybersecurity Guide*. Generva: International Telecommunication Union. https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-national-cybersecurity-guide.pdf

ITU (2020). *Global cybersecurity index*. ITU. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Jablonsky, D. (2008). National power. *Strategic Studies Institute*, Volume-I. US Army War College. https://

www.jstor.org/stable/pdf/resrep12115.13.pdf

Jayan, S. D. (2011). *Cyber Law – an Introduction for Non Law Professionals*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1873248

Kraken, J. (2019). *Analysis of malware - the Morris Worm* [Doctoral thesis, Metropolia University of Applied Sciences]. https://www.theseus.fi/bitstream/handle/10024/171871/bachlorThesis-Worm.pdf;jsessionid=039C4937721F280B60700D9F5A254C04?sequence=2

LCM (2020). An unparalleled collecton. *Library Congress Magaazien*. March / April 2020, *9*(2). https://www.loc.gov/lcm/pdf/LCM_2020_0304.pdf

Levy, S., & Crandall, J. R. (2020). The Program with a Personality: Analysis of Elk Cloner, the First Personal Computer Virus. *arXiv*:2007.15759v1. https://arxiv.org/pdf/2007.15759.pdf

McAfee (2013). *The economic impact of cybercrime and cyber espionage*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf

NCSC (2018). NCSC code of conduct. (Date Accessed: 16.04.2024) https://www.ncsc.gov.uk/information/ncsc-code-conduct

OECD (2019). *Future of Education and Skills*. https://www.oecd.org/en/about/projects/future-of-education-and-skills-2030.html

Ottis, R. (2018). *Analysis of the* 2007 *cyber attacks against Estonia from the information warfare perspective*. Cooperative Cyber Defence Centre of Excellence. https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Paganini, P. (2022). *Non state actors in cyberspace: An attempt to a taxonomic classification, role, impact and relations with a state's socioeconomic structure*. Center For Cyber Security and International Relations Studies. https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf

Robert, S. (2023). *History of Cybersecurity: A Brief Explanation*. https://www.theknowledgeacademy.com/blog/history-of-cyber-security/

Rossini, C., & Green, N. (2015). *Cybersecurity and Human Rights*. GCCS 2015 - Webinar Series Training Summaries. https://www.gp-digital.org/wp-content/uploads/2015/06/GCCS2015-Webinar-Series-Introductory-Text.pdf

Saaida, M. B. E. (2023). The use of cyber warfare and its impact on international security. *Science For All Publications*. July 2023, *1*(1), 1-5. https://dapp.orvium.io/deposits/64d32b1b5fb1f4fefdc25c9c/view

Schjolberg, S. (2017).*The history of cybercrime* (1976-2016). Cybercrime Research Institute.

Stevens, T. (2021). Cyber Power in International Relations. Cornish, P. (Ed.) *The Oxford Handbook of Cyber Security* .pp.66-81. Oxford University Press. https://academic.oup.com/edited-volume/41360.

URL 1. ITU (2024, n.d.). *National cybersecurity strategies repository*. (Date Accessed: 16.04.2024) https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

URL 2. MSC (2024). Code of conduct & Ethics policy. (Date Accessed: 16.04.2024) https://www.micromindercs.com/codeofconductethicspolicy

URL 3. Paganini, P. (2018, April 21). UK teenager kane gamble who hacked cia chief and other us intel officials gets 2-year jail sentence. (Date Accessed: 16.04.2024) https://securityaffairs.com/71593/cyber-crime/kane-gamble-cia-hack.html

URL 4. Sharma, A. (2023, January 6). Why remote and hybrid work could fuel cyber attacks in 2023. *The National News*. https://www.thenationalnews.com/business/technology/2022/12/30/why-remote-and-hybrid-work-could-fuel-cyberattacks-in-2023/

URL 5. Sharlton, E. (2024, January, 10). 2023 was a big year for cybercrime – here's how we can make our systems safe. *World Economic Forum*. https://www.weforum.org/agenda/2024/01/cybersecurity-cybercrime-system-safety/

Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, Dan., & Schwarzenbach, A. (2020). *National Cyber Power Index* 2020. Belfer Centre. https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

Vorina, A., Vrcelı, N., & Bevanda, V. (2022). Usage of E-platforms Google Meet, Microsoft Teams and Zoom in education. *Conference: Sixth International Scientific Conference ITEMA Recent Advances in Information Technology, Tourism, Economics, Management and Agriculture*. ITEMA 2022 – Conference Proceedings, Hybrid (University of Maribor, Slovenia), October 27, 2022. https://www.researchgate.net/publication/372034130_Usage_of_E-platforms_Google_Meet_Microsoft_Teams_and_Zoom_in_Education

About Author

**Prof. Dr. Nezir Akyeşilmen | Selçuk University | nezmen[at]yahoo.com |
ORCID: 0000-0001-8184-5280**

Dr. Nezir Akyeşilmen is a Professor of International Relations at Selcuk University. He earned his undergraduate and Ph.D. degrees from Middle East Technical University (METU) in Ankara, and his Master's degree from the University of Essex. His extensive research portfolio spans critical areas such as cybersecurity, digital politics, human rights, and international conflict analysis. Having previously chaired the Centre for Peace Research at Selçuk University, he currently Chairs the Association for Human Rights Education. Notably, he has been a member of the Expert Group on Digital Citizenship Education (DCE) at the Council of Europe since September 2021, contributing his expertise to this influential international body. Dr. Akyeşilmen is the author of the book *Cyberpolitics and Cybersecurity with an Interdisciplinary Approach*: Ankara: Orion- 2018. In addition to his scholarly contributions, he serves as the Editor-in-Chief of the esteemed *Cyberpolitik Journal*. follow him on Twitter @nezmen.