THE EVOLUTION OF THE ALLIANCE CONCEPT IN CYBERSPACE: A CONCEPTUAL REVIEW

Onur YILMAZ[*]
ORCID ID: 0000-0001-6846-0968

Declaration[* *]

ÖZET

Bu makale, uluslararası ilişkiler literatüründe uzun süredir tartışılan ittifak kavramını siber güvenlik bağlamında yeniden ele alarak "siber ittifak" olgusunun kavramsal temellerini ve pratik yansımalarını ortaya koymayı amaçlamaktadır. Çalışma, klasik realist yaklaşımın denge ve tehdit temelli analizlerini, siber uzayın çok aktörlü, sınır tanımayan ve hiper-anarşik doğasıyla ilişkilendirerek özgün bir kavramsal açıklama modeli geliştirmektedir. Nitel literatür taramasına dayanan analiz, devletlerin siber tehditleri tek başına caydırma ve bertaraf etme kapasitesinin yetersiz kaldığını; bu nedenle kamu, özel sektör ve uluslararası örgütleri kapsayan esnek iş birliği mekanizmalarının kaçınılmaz hâle geldiğini ortaya koymaktadır. Bu tür bir iş birliğinin mümkün kılınabilmesi için ise, mevcut güvenlik kuramlarının ötesine geçen yeni ve kapsamlı bir ittifak tanımının geliştirilmesi gerekmektedir. Bu bağlamda çalışma, siber ittifak kavramını ve onun klasik güvenlik perspektifleriyle açıklanamayacak niteliklerini analiz ederek literatüre kavramsal düzeyde katkı sunmayı hedeflemektedir.

Anahtar Kelimeler: Siber Uzay, Siber Ittifak, Siber Güvenlik, Uluslararası Ilişkiler

ABSTRACT

The classical realist approach considers the multi-actor, borderless, and hyper-anarchic nature of cyberspace. Supported by a qualitative literature review, the analysis shows that states cannot alone deter and neutralize cyber threats; therefore, flexible cooperation mechanisms

[*] Arş. Gör. Doktora Adayı, Siyaset Bilimi ve Uluslararası İlişkiler (İng), İstanbul Aydın Üniversitesi- İstanbul-Türkiye, yilmaz12onr@gmail.com
[*] Bu çalışma, İstanbul Medeniyet Üniversitesi Sosyal Bilimler Enstitiüsü bünyesinde hazırlanan doktora tezinden üretilmiştir.
[*] Artificial Intelligence (AI) tools were only used to organize the references in this study.

involving the public sector, private companies, and international organizations have become essential. The key to enabling such cooperation is developing a new and broader definition of alliance that goes beyond traditional security theories. In this context, the study aims to contribute to the literature by examining the concept of cyber alliance and its characteristics, which cannot be explained through classical security paradigms.

Keywords: Cyberspace, Cyber alliances, cybersecurity, international Relations

Introduction

It becomes clear that the concept of alliance holds an important place in the security strategies of states when evaluated within the historical context. From a realist perspective, alliances, which are formed by bringing together the military forces of states against common threats, have been analyzed in terms of the balance of power or threat perceptions (Morgenthau, 1948; Waltz, 1979; Walt, 1987). Although these and similar analyses have been intensively studied in the literature for many years, the rapid and unstoppable development of digitalization and information-communication technologies has made it necessary for states to incorporate these developments into their national security paradigms and to combat new threats that push the limits of classical security paradigms.

Cyberspace, which almost eliminates physical borders and extends beyond them, has become a unique security space with a structure that requires states to redefine the concepts of sovereignty and security. This area, where non-state actors are also active, has a complex and anarchic structure; however, international law and norms have not yet been sufficiently developed to address these issues. On the other hand, the anarchic nature of this area and the difficulty of defending it have led states to redefine their basic security requirements, as well as to address cyber-attacks, cyber espionage activities, and threats to critical infrastructures (Deibert & Rohozinski, 2008; Yılmaz, 2020). Considering all these and the fact that states have not yet been able to create a completely cyber-secure environment on their own, it is seen that cooperation and alliance formations in this field have become inevitable.

When considered in this context, the concept of "cyber alliance" may offer a new analytical framework that requires a reinterpretation of classical alliance concepts. With cyber alliances, it will be possible to establish a flexible and dynamic cooperation model that encompasses not only states but also various actors, including the private sector and international organizations.

The increasing diversity and destructiveness of cyber threats and attacks faced by states make such cyber alliances more strategic and essential.

Although the importance of cyberspace as a new security domain is now widely recognized, the concept of “cyber alliance” has not yet been sufficiently conceptualized in the literature of international relations. Most existing studies focus either on national cyber security strategies or bilateral cooperation practices. However, there is a need for an analytical framework that can comprehensively address the structural and functional dimensions of cyber alliances. This study aims to highlight the conceptual uniqueness of cyber alliances by examining the aspects that distinguish them from traditional military alliances and to explain their similarities and differences concerning the conventional understanding of alliances in the international relations literature. In this regard, the research is structured around the following questions: "How do cyber alliances differ conceptually from traditional alliances and under what conditions do they emerge? How does the unique structure of cyberspace transform the way the concept of alliance is approached?" In seeking answers to these questions, the study compares the relational aspects of classical alliance approaches with the phenomenon of cyber alliances and attempts to establish a theoretical framework for this new concept.

The Concept of Alliance in International Relations Literature

The concept of alliance is a frequently referenced feature in the field of International Relations. Beyond the classical realist narrative that views International Relations as a history of conflict and war, it is an undeniable reality that this field also encompasses aspects of diplomacy and cooperation. As such, alliances emerge as a natural and undeniable component of International Relations.

When faced with threats and risks of war, states seek to form alliances, either formally or informally, motivated by the promise of fighting the common threat together and neutralizing it together. Although the forms of alliances can be symmetrical and asymmetrical, or defensive and offensive, the three underlying elements of alliances are unity in the sense of "actors (parties), common threat, and joint elimination of the threat". Since realist studies largely influence alliance studies, it becomes clear that what is meant by 'actor' is typically nation-states. On the other hand, a consensus among studies on the concept of alliance is that the actors who form alliances are nation-states. It is also undeniable to say that the history of international relations is shaped as a cross-section of who has maintained alliances with whom, against whom, for what motives, and for how long. Although it is foreseen that strong states and weak states act with different motives when forming alliances, the desire to form alliances and avoid facing the threat alone is similar. While strong states seek to consolidate their dominance, the weak state may pursue a strategy of 'balancing the hegemon'. However, the main intention of both types of states, whether weak or strong, is to utilize the capabilities of the other for their benefit, and they have similar incentives in this regard. On the other hand, the alliance relationship between states is not always formalized through agreements, pacts, or written texts; it can sometimes be unofficial and secretly established. In terms of duration, while some alliances are long-lasting, others may end when the desired goal is realized or terminated and may be short-term (Yalçın, 2014; pp. 399-401).

To say that states form alliances only to counter common threats may be an incomplete observation on its own. The motivations of states can be as diverse as having similar beliefs, economic concerns, and maintaining stability in their favour. Behind this diversity, however, lies one constant: reciprocity. This reciprocity relationship can be established at the beginning of alliances as well as at the end (Saka & Abdullahi, 2021, pp. 1-3).

There are different views on why alliances are formed in international relations. While Stephen Walt argues that alliances are formed to protect against threats, John Mearsheimer contends that strong states form alliances to gain power, while weak states do so to create a balance of power. Despite these different approaches, there is more consensus on the consequences of alliances. While alliances can sometimes lead states to war, they can also contribute to peace by increasing security. In general, alliances can make the international system more predictable and stable, but not always in a positive way. For example, in the First World War, secret alliances led to a security dilemma and fueled conflicts. In this context, Kenneth Waltz, in contrast to the classical balance of power approach, argued that states form alliances to balance threats rather than power (Arshid, Irfan, & Tanveer, 2017, pp. 44-51).

The tendency of states to form alliances in the face of a common threat offers a fundamental explanation for the formation of these structures. According to this approach, alliances aim to ensure security, share military resources and increase deterrence against external threats. Hans Morgenthau argues that in multipolar systems, states can pursue three main strategies to increase their power: building internal capacity, consolidating power through alliances, and preventing rivals from cooperating. The second and third of these strategies lead directly to the formation of alliances. Stephen Walt, however, adopts an approach based on threat rather than power. According to him, alliances are shaped not only by material capacities, but also by geographical proximity, intent to attack and how these elements are perceived. Therefore, a state's power may not always be perceived as a threat by other states, and alliance decisions are based on these relative perceptions of threat.

In the IR literature, not only have the conditions under which states form alliances been extensively discussed, but also how they choose sides in alliances. In this context, the most basic dichotomy is shaped by balancing and bandwagoning strategies. Balancing is based on the concept of balance of power, one of the fundamental tenets of realism. It implies that states seek to offset potential threats by either increasing their capabilities or forming alliances to maintain stability.

While classical realists, such as Morgenthau, attributed these choices to the political calculations of state elites, neo-realist Waltz argues that this behaviour stems from the survival instinct inherent in the anarchic nature of the system. According to Waltz, if the ultimate goal of states were an absolute increase in power, bandwagoning —a less costly strategy —would be preferred. However, states often choose to join weak coalitions to maintain the balance of power and prevent the emergence of a possible hegemonic structure. Therefore, the dominant tendency at the systemic level is toward balancing (Morgenthau, 1948; Waltz, 1979). In this framework, Waltz's view of balancing as a structural consequence of the international system has led to criticism that he positions states as implementing actors who fulfill the requirements of the system, rather than being subjects in their own foreign policy. This approach is at the center of the ongoing theoretical debates on structuralism in the IR literature.

Bandwagoning, as discussed by Kenneth Waltz in his Theory of International Politics (1979), refers to the tendency to ally with the stronger side against a rising threat. In this context, it stands opposite to the balancing strategy. While balancing aims to achieve stability by supporting the weaker side against a stronger actor, bandwagoning is based on the desire to ensure security by joining forces with the source of the threat. In this approach, the state perceives a threat and prefers to act in concert with it rather than oppose it. The primary motivation for this choice comes from the need for survival and security in the anarchic nature of the international system (Waltz, 1979, pp. 126-127). Especially when a dominant hegemon exists in the global system, aligning with it is viewed as the least costly way for states to secure their interests. In this context, bandwagoning is not solely about security;

sometimes, states seek alliances with powerful actors to maximize their national interests, material gains, or territorial expansion. As a result, alliances can form not only as a means of defense but also to create opportunities and reward mechanisms (Siddiqi, 2016, p. 77). Compared to the balancing strategy, the lower cost of bandwagoning—aligning with stronger actors—makes this approach a rational choice for many states. This strategy is not limited to small states; major powers may also pursue it. The foreign policy of British Prime Minister Neville Chamberlain in the 1930s exemplifies this. Additionally, the expectation of gaining greater benefits at a lower cost has led some states to adopt bandwagoning. For instance, Hungary and Bulgaria's accession to the Axis Powers was primarily driven by their desire for territorial gains (Eckstein, 2023, pp. 1–11). While Waltz's system-centered model emphasizes threat-based balancing, many theorists argue that opportunistic motives can also influence alliance behavior. Schweller (1994), for example, introduces the idea of "bandwagoning for profit," suggesting that states may align with stronger powers not just for protection but to achieve strategic or material advantages. This view broadens the traditional understanding of alliances beyond the security dilemma, allowing for interest-driven behavior within the limits of the international system (Schweller, 1994, pp. 72–107).

In the anarchic structure of the international system, not only the preferences of states for strategies such as bandwagoning or balancing, but also the motivations, with whom, and on what grounds they cooperate when forming alliances, constitute a more in-depth discussion area in the literature. Historically, alliances have been as decisive as wars in determining the survival of states. States have developed alliance relations for various purposes, such as enhancing power, promoting economic and ideological harmony, fostering strategic partnerships, mitigating security threats, and contributing to global governance and development. In this framework, the question of whether similar alliances can be established in cyberspace, which stands out as a new security dimension, is becoming increasingly important. With its multi-actor and anarchic structure, cyberspace is turning into a plane that reflects the power struggles of the classical international system. In this context, the positioning of states in cyberspace has become a central aspect of the contemporary global security architecture

The Concept and Characteristics of Alliance in Cyberspace

Before discussing the possibilities of alliance in cyberspace, it is essential to clearly define the meaning and boundaries of the concept of "alliance" in this field. Since conceptual ambiguity can undermine analytical coherence, a clear framework of what is meant by 'alliance' in the cyberspace context is essential for the healthy progress of the discussion. Relying on a common terminology when analyzing a particular domain provides conceptual clarity and a solid ground for theoretical and empirical evaluations (Cains, Liberty, Taber, King, & Henshel, 2022). However, cyberspace and its specific concepts—especially relatively new terms such as "cyber alliance"—have not yet reached a common terminological consensus in the literature. This makes it challenging to achieve conceptual clarity and requires additional attention in establishing the analytical framework. Therefore, for the theoretical coherence of the study, it is necessary to develop a specific approach to the concept of "cyber alliance". This approach seeks to make sense of cyberspace within the context of the discipline of International Relations, particularly within the framework of state-centred political readings. However, before proceeding to this framework, it would be more appropriate to present a general assessment of the structural characteristics of cyberspace

By its very nature, cyberspace has a complex and multi-layered structure. Although there is no single agreed-upon definition, it is possible to develop a general understanding based on various institutional frameworks. Sources such as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the Pentagon's Dictionary of Military and Associated Terms offer efforts to define different dimensions of cyberspace. However, these definitions differ in content and scope, and may be incomplete or limited in some aspects. The Pentagon dictionary has attempted to adapt to the changing dynamics in the field by updating its definition of cyberspace with revisions in 2007, 2009, and 2017. This diversity makes the need for clarity on the scope of cyberspace even more visible (Mayer, 2015, pp. 6-9). Although different institutional definitions of cyberspace vary in their details, certain common elements emerge. First of all, cyberspace is not a physical but a virtual medium, and as such, it is beyond the legal and technical limitations applied to traditional physical spaces. Structured as a global network system, cyberspace consists of networks interconnected through computers, software, and digital communication devices. It encompasses not only data and software, but also a social dimension involving its users and stakeholders. Its decentralized, ever-evolving and dynamic structure makes it difficult to control, which is why cyberspace is increasingly seen as a strategic area of power by states and other powerful actors.

The importance of cyberspace as an area of power lies in its anarchic nature, similar to that found in International Relations. In the international system, anarchy refers to the absence of a binding and regulatory authority over states, which renders the system uncertain, unpredictable, and competitive due to the lack of a centralized structure to constrain the behavior of states. Similarly, cyberspace, with its lack of a central authority, represents an anarchic plane where rules are not clearly defined, power struggles intensify, and actors prioritize their interests (Morgenthau, 1954, pp. 131-133). This anarchic structure has historically paved the way for conflicts and wars in the international system, and this situation has become a continuous reality in the ordinary course of international relations. Today, this dynamic persists in various forms.

In this framework, the fact that cyberspace, like the international system, has a structure with multiple actors, inadequate legal regulations, and a weak binding structure, strengthens the view that it has an anarchic nature. To further define these structural features, the concept of "hyper-anarchy" has emerged in the literature. This concept was first introduced by Rafal Rohozinski and Ronald Deibert in 2008, referring to the fact that cyberspace lacks a central authority or governance structure. Hyper-anarchy is used to describe an order in cyberspace where there is no binding law-making or enforcement power for actors at different levels, such as individuals, hackers, criminal networks, private companies, and states (Deibert & Rohozinski, 2008, pp. 432-435). The structure of cyberspace, which physical borders cannot enclose, its rapidly changing technological infrastructure, and the difficulties of rule-making in the digital space make the concept of hyper-anarchy a meaningful and appropriate one. In this framework, a hyper-anarchic cyberspace refers to a structure that is ungovernable, where the probability of crime and conflict is high, state sovereignty is weakened, and the risks of cyber warfare increase. This structure is not only a technical domain, but also a new plane of power that profoundly affects international security and relations of sovereignty.

On the other hand, the approach that cyberspace has an entirely hyper-anarchic structure has faced various criticisms in the literature. This is because the capacity of actors with considerable power and influence in cyberspace—primarily states, multinational corporations, and various non-state structures—to create norms and order in cyberspace cannot be ignored. These actors have the potential to achieve their strategic goals and limit the inherent anarchy of cyberspace.

In this context, the hyper-anarchy narrative that cyberspace is completely ungovernable is not only a conceptual exaggeration but also highlights a practical risk for cybersecurity policies. Such a narrative weakens trust in governability, reducing motivation to build order and possibly hindering the progress of cyber governance and security efforts (Akyeşilmen, 2017, pp. 1-18). Even the definitions of cyberspace imply it is becoming a new security domain, often mentioning the variety of threats and the unpredictability of involved actors. This domain, noted for its anarchic nature and governance challenges, gained attention on the global security agenda especially after the 2007 cyberattacks against Estonia—described by many as the "first cyber war." The rapid destruction of Estonia's digital infrastructure, the disruption of government functions, and the subsequent political fallout highlighted the serious cyber threats to nations. This event pushed for faster securitization in cyberspace and encouraged regional cooperation among Baltic states, leading to initiatives for joint cyber defense and shared deterrence strategies. The incident exposed the fragility of digital infrastructure and the difficulties of protecting it, prompting strategic cooperation among Baltic countries and allies. One key result was the development of a shared cyber defense framework, focusing on regional readiness and collective deterrence (Libicki, 2019). Afterwards, not only small and medium-sized countries but also major powers—such as the United States, the United Kingdom, and Turkey—faced cyberattacks and started creating national strategies in response (Yilmaz, 2020). NATO's security focus has increasingly included cyberspace, and bilateral cyber alliances have become more prominent. A prime example is the formal cyber cooperation between the United States and Japan, as reported by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE, 2023). This partnership shows how geopolitical interests and technological vulnerabilities influence the formation of cyber alliances.

The dominant trend in the cybersecurity literature generally focuses on the anarchic nature of cyberspace, the unpredictability of threats, and the isolation of states in this domain. However, this perspective also reveals the impossibility for states and other actors to deal with these threats alone. This highlights the need for establishing an effective governance mechanism in cyberspace. To protect against the risks posed by the anarchic structure and to capitalize on the opportunities in cyberspace, actors need to develop not only national but also collective policies and action alliances. In this context, the concept of cyber alliance gains strategic significance in terms of both security and governance; however, a clear definition of its scope and boundaries becomes essential for developing a sound analytical framework.

Before addressing the concept of alliance in cyberspace, it is necessary to understand the extent to which contemporary societies and state structures are affected by cyberspace. In the 1990s, while the US had serious initiatives on cybersecurity, the report by the US National

Academy of Sciences, with the words "...we are at risk," attracted attention in this regard. The report highlighted that the US was becoming increasingly dependent on computer systems every day (Tarhan, 2022, pp. 393-424). Today, almost all digitalized structures, from banking to air traffic control, from communication infrastructures to market chains, from individual privacy data to national security systems, have become potential targets in cyberspace. This situation shows that states and societies have become structurally vulnerable to cyberattacks. Indeed, past cyberattacks have provided important indicators of the extent of the damage that can occur in the absence of adequate protection and cooperation mechanisms. It is now clear that cyber threats and attacks also have physical consequences (Afsar, 2022, pp. 77-96).

In this context, cybersecurity should be seen not only as a technical issue, but also as a political, social, and international one. However, even today, there is no international consensus on fundamental questions such as "what is a cyber attack", "who poses a threat", and "who needs to be protected". As long as this conceptual and institutional gap persists, cyberattacks can have far-reaching consequences, including the overthrow of governments, undermining national security, political and economic instability, and erosion of public health and social trust. Therefore, seeking cooperation and alliances in cyberspace should be considered not only a choice but also a necessity (Li & Liu, 2021, pp. 8176-8186). The most effective and cost-efficient way to mitigate all these risks is to develop comprehensive cooperation and alliances among cyberspace actors. Clarifying the boundaries of attack-defense, crime-punishment, and friend or foe will reduce uncertainties in this area. In this context, cyber alliances are no longer a choice but a strategic necessity

Before discussing cyber alliances, it is necessary to clarify what the concept of "alliance" means in the context of International Relations. Alliances are cooperative structures, sometimes formal and sometimes informal, that states develop based on common interests or shared threat perceptions. These cooperations may arise even in cases of partial overlap of interests, rather than complete overlap. Moreover, alliances are formed in different ways, depending on the power distribution of the period, and are often established with a defensive reflex against a common or potential enemy (Mearsheimer, 2001). By joining forces against a common enemy, which can often be a counter-alliance system, states aim to provide deterrence and eliminate threats at a lower cost. Alliances are also formed to protect strategic regions, secure trade routes, or achieve common goals more efficiently. Historically, such collaborations have been frequently used as a means of both defense and interest maximization (Morgenthau, 1948, pp. 203-204).

Similar motivations in cyberspace shape Alliance relations. States cooperate to collaborate in line with shared interests and against common threats. One of the first examples of this is the Southeast Asia Enhanced Engagement Program (SEEP), a cyber alliance between the Philippines and the United States signed in 2022. This cooperation against cyber threats emanating from China is based on three pillars: information sharing, capacity building, and response mechanisms. However, it is debatable whether such structures can provide complete protection against all cyber threats. There are also significant shortcomings in terms of international law and binding regulations (Winger, 2022, pp. 1-6).

With its anarchic, multi-actor and complex structure, cyberspace has turned into a security space where conflict and cooperation are possible not only between states but also with non-state actors. The fact that attacks do not only originate from states, but also that hacker groups, companies, and individuals can pose a threat, shows that no actor can provide absolute security in this area. Therefore, states, companies and other actors are turning to formal or informal cooperation to share risks and costs, build capacity or counter common threats. Just as in classical international alliances, the aim is to ensure security in cyberspace collectively; such organizations can be evaluated under the concept of a cyber alliance.

The Concept of Alliance in International Relations and Cyberspace: Similarities and Differences

When the concept of alliance is analyzed in the International Relations literature and the context of cyberspace, it becomes apparent that there are both similarities and significant differences in terms of structure, functioning, actors, and scope of the alliance. While these differences stem from the unique dynamics of both fields, similarities emerge from their intertwined structures over time. Therefore, for the sake of conceptual clarity, it would be useful to first address the differences in the alliance phenomenon between the two fields, in order to better interpret the similarities.

In international relations, alliances are typically formed between states that share common interests and ideologies, allowing them to coordinate their physical actions and policies. These alliances are often formed based on geopolitical proximity and are influenced by the actions of great powers. For example, US allies typically must consider US strategic priorities in their dealings with China. Rui Mao's analysis of the agricultural sector reveals that alliances can even influence trade decisions and limit the room for independent action of their allies (Mao, 2023, pp. 433-437).

In International Relations, alliances are often formed to enhance military capacity, deter rivals, and establish standard defense systems. These alliances are typically formalised through strategic and security-based agreements, in which nation-states are the primary actors (Holsti, 1995, pp. 112-118). NATO and the Warsaw Pact are the two prominent examples of classical alliance structures in the history of International Relations. Geopolitical concerns, the search for a balance of Power, and defense against common threats have shaped the motivation of states to form alliances throughout history. In traditional alliances, respect for the sovereignty and territorial integrity of member states is essential; protecting national interests within the framework of international law is one of the primary objectives (Morgenthau, 2006, pp. 45-48).

On the other hand, although it is emphasized that NATO operates based on the classical alliance understanding, it is worth noting that this organization continually renews and reorganizes itself in response to new threats, thereby maintaining its relevance and continued existence. It is evident that NATO, which can continually create new security agendas for itself, continues its expansion. One of the main threats included in the security agenda in this new construction process is the one related to cyberspace and its security (Erendor, 2016, pp. 114-133)

Alliances in cyberspace are often created to enhance cybersecurity, share intelligence, and coordinate responses to attacks. Because this domain involves multiple actors, alliances can be formed between states, national institutions, and private companies. The rise of transnational threats has transformed cyberspace into a new security domain for nations, making alliances vital in this context (Eichensehr, 2017, pp. 52-57). Unlike traditional IR alliances, cyber alliances tend to be more flexible and less formal. Since cyberspace evolves rapidly, these agreements frequently take the form of memoranda of understanding or informal pacts, enabling quick adaptation to new technologies and threats (Li et al., 2020, pp. 31–33). Additionally, the involvement of non-state actors—such as private firms, international organizations, and civil society groups—emphasizes the borderless and decentralized nature of cyberspace (Khraisat & Alazab, 2021, pp. 18–22). Building on these distinctive features, recent theoretical efforts have aimed to understand the dynamics of cyber alliances through formal modeling approaches. One example is Benkő and Biczók's (2024) cyber alliance game, which illustrates how actors evaluate the costs and benefits of cooperation versus unilateral action when confronting emerging threats. Their findings highlight that cyber alliances are driven by strategic logics that differ significantly from those underlying traditional, state-centric security agreements (Benkő & Biczók, 2024).

When evaluated in terms of differences:

- Although both types of alliances aim for security and stability, traditional alliances focus on geopolitical and physical security, whereas cyber alliances emphasize the protection of digital infrastructure and information systems.
- While traditional alliances are formed between sovereign states, cyber alliances are more multi-actor structures that include private sector and civil society actors.
- In contrast to classical alliances defined by physical boundaries, cyber alliances require flexible strategies against a decentralized and borderless threat environment.

In conclusion, although the two types of alliances have different structural and operational characteristics, this does not mean that there are no similarities between them. Therefore, it is essential to identify the commonalities between alliances in both domains.

Although alliances in IR and cyberspace have their differences, they are both shaped by the goal of achieving security and strategic advantage. Traditional alliances, such as NATO, are structured based on military capacity and collective defense. Similarly, cyber alliances aim to establish a collective cybersecurity environment among their members by creating an effective line of defense against common threats (Council of Europe, 2001). Another similarity is that both types of alliances are based on the principle of mutual benefit. While traditional partnerships are formed to balance power or address threats, cyber alliances similarly pursue common goals to mitigate cyber risks and enhance security capacity.

Another similarity between traditional and cyber alliances is the principle of flexibility. While international alliances have the ability to adapt to changing geopolitical conditions, cyber alliances must similarly develop flexible strategies against a dynamic and rapidly changing threat environment (Li, Zhao, & Zhang, 2020, pp. 31-33). Another similarity between cyber and traditional alliances is the principle of cooperation and coordination. Just as joint operations and military strategies are coordinated in traditional alliances, information sharing, response planning, and capacity building in cyber alliances are based on a similar coordination logic (Russett, 1971, pp. 263-281). In cyber alliances, intelligence sharing, joint strategy development, and defense exercises are the main elements of cooperation. Just like traditional alliances, risk sharing is a common feature of cyber alliances. In both structures, the aim is to minimize threats by sharing the burden. The success of this process relies heavily on open and transparent information sharing, which becomes one of the main parameters determining the effectiveness of the alliance (Eichensehr, 2017, pp. 467-505). Traditional alliances have historically played a crucial role in shaping international norms and security standards. Similarly, cyber alliances, although not yet fully institutionalized, may become important platforms for determining cybersecurity norms in the future through inter-actor interaction (Hare, 2021, pp. 123-145). Another common aspect of traditional and cyber alliances is the efficient and collective use of resources. Both structures are based on sharing military, economic, technological, or human resources to strengthen defense against common threats. Whereas in traditional alliances, this takes the form of weapons systems or financial support, in cyber alliances it takes the form of exchanges of specialized personnel, technology sharing, and infrastructure support.

To summarize, the similarities between traditional and cyber alliances can be summarized as follows:

- Both types of alliances are formed in pursuit of shared interests and objectives.
- Mutual defense responsibility is essential (e.g. NATO's Article 5).
- Information and risk sharing are key elements of alliances.
- Joint use of resources (military, economic, technological, manpower) is emphasized.
- Strategic coordination is ensured through joint exercises, simulations and strategies.

Table 1: Common Characteristics of Traditional and Cyber Alliances

Similarity Field	Traditional Alliances	Cyber Alliances
Purpose of Establishment	Established to defend against common interests and threats.	It is created to ensure coordination and security against common cyber threats.
Defense Responsibility	As in the case of NATO, the principle of collective defense is essential.	A collective security approach is often adopted in common cyberattack scenarios.
Information and Risk Sharing	Sharing military intelligence and security information is essential.	Cyber intelligence, attack data and risk sharing play a critical role.
Resource Sharing	Joint use of military, economic and technological resources is common.	Resources such as technological infrastructure, specialized personnel and financial support are shared.
Strategic Coordination	Through joint military exercises, planning and operational coordination.	Joint cyber exercises, simulations, and strategic planning are conducted.

Note: Table created by the author.

Conclusion

Analyzing the concept of alliances in cyberspace requires going beyond the traditional discipline of International Relations. At this point, the parameters that need to be included in the analysis include security and power dynamics, and only an analysis in this direction can provide a competent perspective.

Both the complexity and diversity of cyber threats and the fact that states are becoming more and more equipped with digital infrastructures and that the seriousness of this has reached the level of addiction, combined with the unique structure of cyberspace, brings the possibility of states' alliances in the hyper-anarchy environment that emerges, and brings the concept of cyber alliance to a strategic position. While cyber alliances, like traditional alliances, act with the logic of uniting forces in the face of common threats, they also differ from it in structural and functional aspects.

The analysis conducted in this study reveals that alliances in cyberspace envision a multi-actor and more comprehensive cooperation model that encompasses actors beyond states, including the private sector and international organizations. Cyber alliances are critical for security in today's rapidly changing and diversifying threat-attack environment, as they are more flexible and capable of adapting to rapidly changing situations, unlike traditional alliances. In this framework, cybersecurity cooperation between states and other actors in the coming period will become one of the key factors determining the stability of the international system.

As a result, the role and strategic importance of cyber alliances in the international security system will continue to increase significantly over time. The difficulties that states face in combating cyber threats on their own make broader-based cooperation, involving various actors, inevitable. Therefore, steps to be taken in the field of international law and the development of common standards are of great importance. Academic research and applied studies on this issue, to be conducted in the coming period, will play a crucial role in strengthening cybersecurity policies and reshaping the understanding of international security.

References

Akyeşilmen, N. (2017). Cyberspace as hyper-anarchy: A critical analysis. *Journal of Cyber Policy*, 2(1), 1-18.

Afsar, Ö. A. (2022). The Evolution of NATO's Cybersecurity Policy. *Cyberpolitik Journal*, *7*(13), 77-96.

Arshid, I., Irfan, H., & Tanveer, A. (2017). Alliances in international politics: A comparative study of Kenneth Waltz's and Stephen Walt's theories of alliances. *Kaav International Journal of Arts, Humanities and Social Science*, 4(3/A9), 44-51.

Benkő, G., Biczók, G. (2024). The cyber alliance game: How alliances influence cyber-warfare. *arXiv, 2410*(05953), 1–18.

Cains, M. G., Liberty, F., Taber, D., King, Z., & Henshel, D. S. (2022). Defining cybersecurity and cybersecurity risk within a multidisciplinary context using expert elicitation. *Risk Analysis*, 42(8), 1643–1669.

Council of Europe. (2001). Convention on Cybercrime. Strasbourg, France: Council of Europe. https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Deibert, R. J., & Rohozinski, R. (2008). Cyberspace as hyper-anarchy: Towards a new research agenda. In R. J. Deibert & R. Rohozinski (Eds.), Access controls and digital governance in the global information age (pp. 431–454). Toronto: University of Toronto Press.

Eckstein, A. M. (2023). 'Jackal bandwagoning'? The Achaean League shifts alliances from Macedon to Rome, autumn 198 B.C. *The International History Review*, 45(1), 1–11.

Eichensehr, K. (2017). Public-private cybersecurity. *SSRN Electronic Journal,* 467-505.

Erendor, M. E. (2016). Cyberterrorism within the framework of risk society and reflexive modernization: The problem of definition and typology. *Cyberpolitik Journal*, 1(1), 114–133.

Hare, F. (2021). Cybersecurity and cyber warfare: What everyone needs to know. *Journal of Cyber Policy*, 6(2), 123–145.

Khraisat, A., & Alazab, A. (2021). A critical review of intrusion detection systems in the Internet of Things: Techniques, deployment strategy, validation strategy, attacks, public datasets and challenges. *Cybersecurity*, 4(1), 1–27.

Li, J., Zhao, B., & Zhang, C. (2020). Fuzzing: A survey. *Cybersecurity,* 3(1), 1–41.

Libicki, M. C. (2019). Baltic-area cyberspace alliance. In T. Minárik, R. Jakschis, & L. Lindström (Eds.), 11th International Conference on Cyber Conflict: Silent Battle (pp. 201–212). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Mao, R. (2023). Coalitions in international relations and coordination of agricultural trade policies. *China Agricultural Economic Review,* 15(2), 433–437.

Mayer, M. (2015). Cyberspace and international politics (pp. 6–9). https://doi.org/10.13140/RG.2.1.4470.0886.

Mearsheimer, J. J. (2001). The tragedy of great power politics. New York, NY: W. W. Norton & Company.

Morgenthau, H. J. (1948). Politics among nations: The struggle for power and peace (4th ed., pp. 203-204). New York, NY: Alfred A. Knopf.

Morgenthau, H. J. (1954). Politics among nations: The struggle for power and peace (2nd ed., rev. & enl., pp. 131-133). Knopf.

Morgenthau, H. J. (1960). Politics among nations: The struggle for power and peace (3rd ed., pp. 137–138). New York, NY: Alfred A. Knopf.

NATO Cooperative Cyber Defence Centre of Excellence. (2023). The NATO CCDCOE welcomes new members: Iceland, Ireland, Japan and Ukraine. *NATO CCDCOE News Bulletin*, *2023*(March), 1–2.

Russett, B. M. (1971). An empirical typology of international military alliances. American Journal of Political Science, 15(2), 263–281.

Saka, B., & Abdullahi, M. (2021). Alliance and coalition in contemporary international relations: The case of US-South Korea. *Zamfara Journal of Politics and Development*, 2(2), 1–3.

Schweller, R. L. (1994). Bandwagoning for profit: Bringing the revisionist state back in. *International Security, 19*(1), 72–107.

Siddiqi, F. (2016). Security Estimations in South Asia: Alliance Formation or Balance of Power. *Strategic Studies*, 36(2), 77–83.

Tarhan, K. (2022). Historical development of cybersecurity studies: A literature review and its place in security studies. *Przeglad Strategiczny*, 12(15), 393-414.

Waltz, K. N. (1979). Theory of international politics (pp. 126–127). Reading, MA: Addison-Wesley.

Winger, G. H. (2022). Cybersecurity in the U.S.-Philippine alliance: Mission seep. The Pacific Review. Advance online publication.

Yalçın, H. B. (2014). İttifaklar. In Ş. Kardaş & A. Balcı (Eds.), Uluslararası ilişkilere giriş: Tarih, teori, kavram ve konular (pp. 399–401). İstanbul: Küre Yayınları.

Yilmaz, O. (2020). Change of security paradigm; manifestation of the US and Russia competition in the cyber domain (Master's thesis, Kocaeli University, Institute of Social Sciences, Department of International Relations).