

**AUGUST 2025**  
**ISSUE 14**



**JOURNAL OF INTERNATIONAL RELATIONS  
AND POLITICAL SCIENCE STUDIES**

ULUSLARARASI ILISKILER VE SIYASET BILIMI CALISMALARI DERGISI



**E-ISSN**  
**2792-0984**







# JOURNAL OF INTERNATIONAL RELATIONS AND POLITICAL SCIENCE STUDIES

ULUSLARARASI İLİSKİLER VE SİYASET BİLİMİ ÇALIŞMALARI DERGİSİ

E-ISSN 2792-0984


## Editors

-  Assoc. Prof. Dr. Pelin Sönmez   
Kocaeli University, Department of International Relations
-  Assoc. Prof. Dr. İtir Aladağ Görentaş   
Kocaeli University, Department of International Relations


## Subject Editors

-  Prof. Dr. Yücel Karadaş  
Migration Studies, Gaziantep University
-  Assoc. Prof. Dr. Zehra Yılmaz  
Islamic Movements and Gender Equality
-  Assoc. Prof. Dr. Hakan Arıdemir  
International Law and Maritime Studies  
Kütahya Dumlupınar University
-  Assoc. Prof. Dr. Güven Gürkan Öztan  
Political Sociology  
Istanbul University
-  Assoc. Prof. Dr. Ayşegül Gökalt Kutlu  
Climate, Gender, Regional Studies  
Kocaeli University
-  Prof. Dr. Ali Çaksu  
Political Theory, Religion and Politics  
Balıkesir University
-  Assoc. Prof. Dr. Remzie Shahini-Hoxhaj  
Media and Journalism  
University of Pristina
-  Dr. Mehmet Sadık Akyar  
European Union and International Organizations  
Girne American University
-  Dr. Hasan Mesut Önder  
Security and Intelligence Studies  
Non-Affiliated

## Managing Editor

-  Burak Yalın  
Phd Cand. Kocaeli University

## Book Review Editor

-  Buket Özdemir Dal  
Phd Cand. Kocaeli University

## Language Editor

-  Büşra Özyüksel  
Phd Cand. University of Szeged

## Publication Board

-  Prof. Dr. Yücel Acer  
Yıldırım Beyazıt Üniversitesi
-  Dr. Leslie Tramontini  
Philipps Universität Marburg
-  Prof. Dr. Mehmet Hasgüler  
Non-Affiliated
-  Prof. Dr. Mesut Idriz  
University of Sharjah
-  Dr. Martina Ponizilova  
University of West Bohemia
-  Dr. Peter Kacziba  
University of Pecs
-  Dr. Pierre Hecker  
Phillips Universität Marburg

## International Advisory Board



Ayhan Kaya  
Bilgi University



Stephanie Schiedermaier  
Leipzig Universität



Ferit Murat Özkaleli  
Azerbaijan Diplomatic Academy



Filip Ejodus  
University of Belgrade



Murat Erdoğan  
Ankara University



İrfan Kaya Ülger  
Kocaeli University



Nihal Eminoğlu  
Çanakkale Onsekiz Mart University



Egeresi Zoltán  
National University of Public Service

## Aim and Scope

The Journal of International Relations and Political Science Studies (JIRPSS) is an open access, peer-reviewed scholarly journal dedicated to advancing the fields of International Relations and Political Science. Published triannually in April, August, and December, JIRPSS serves as a platform for innovative research and critical analysis on contemporary global issues. The journal emphasizes a multidisciplinary approach, welcoming contributions that bridge the gap between political science, law, economics, sociology, and related disciplines.

JIRPSS is committed to fostering **INCLUSIVE NETWORKS** within the academic community, encouraging submissions that contribute to a diverse and dynamic exchange of ideas. The journal seeks to enhance scholarly dialogue by collaborating with national and international institutions, non-governmental organizations, and policy-makers. The scope of the journal encompasses a wide array of topics, including but not limited to:

- International Relations Theory and Practice
- Comparative Politics
- Global Political Economy
- International Law and Human Rights
- Security Studies and Conflict Resolution
- Migration and Refugee Studies
- Global Energy Politics
- Regional Studies

In addition to original research articles, JIRPSS accepts book reviews and critiques of recently published articles. These critiques aim to foster intellectual discussions, encourage the re-examination of existing literature, and contribute to the field's ongoing development.

## Ethical Principles and Publication Policy

JIRPSS upholds the highest standards of publication ethics, in line with international best practices. The journal is committed to ensuring a fair and transparent peer-review process, guided by the principles outlined by the Committee on Publication Ethics (COPE).

## Open Access Statement



JIRPSS operates under an open access model, with all content freely accessible online. Authors retain the copyright to their work, which is licensed under a Creative Commons Attribution-NonCommercial (CC BY-NC) 4.0 International License. This permits others to share and adapt the material for non-commercial purposes, provided proper attribution is given.

## Disclaimer

The opinions expressed in articles published in JIRPSS are those of the authors and do not necessarily reflect the views of the editorial board or the publisher. The editorial board disclaims any responsibility or liability for the content of articles published in the journal. For further details on submission guidelines and ethical standards, authors are encouraged to visit the journal's official webpage at [JIRPSS Website](#).

# Contents

---

## Research Articles

---

Push or Pull Factor: Rationale for the Collapse of the Ottoman Empire 1839-1908

1-27

**Dr. Usman Abass**

**Independent Researcher**

---

The Institutional and Structural Transformation of the European Union Agency for Cybersecurity (ENISA)

28-64

**Hakan İpek & Prof. Dr. Hilmi Yüksel**

**Dokuz Eylul University**

---

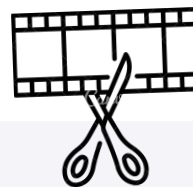
The Balance of Power Theory, Alliances as Both Cause and Shield Of War: NATO and SCO

65-88

**Hacer Kaya**

**Kırıkkale University**

---



Dear Readers,

It is a pleasure to present this new issue of the Journal of International Relations and Political Science Studies (JIRPSS), which brings together three compelling articles on history, institutions, and strategy.

Dr. Usman Abass reframes the late Ottoman trajectory as a push-pull interplay between internal reform and external coercion, moving beyond simple “decline” narratives. The piece is provocative; I encourage future research to pair political history with provincial fiscal records and trade-route data to weigh domestic versus systemic shocks more precisely.

Hakan İpek and Prof. Dr. Hilmi Yüksel trace the institutional evolution of ENISA, showing how a consultative body accrues operational capacity in Europe’s cybersecurity architecture. Their mapping is timely. A comparative lens on Europol/EDA benchmarks, incident-response latency, and NIS2 compliance gaps would further sharpen policy relevance.

Hacer Kaya revisits balance-of-power theory through the NATO–SCO dyad, arguing alliances can be both shield and spark. The argument is persuasive; testing it against post-2022 deterrence dynamics, minilateral hedging, and entrapment indicators would strengthen its explanatory reach.

Taken together, these studies ask how polities learn and adapt through reform, regulatory redesign, and alliance behaviour. We welcome responses integrating archival depth with measurable indicators and extending these debates to under-examined regions.

I sincerely thank our authors and anonymous reviewers for their rigour and generosity and our readers for sustaining JIRPSS’s scholarly community.

Sincerely,

Burak Yalın  
Managing Editor



Dr. Usman Abass  
Independent Researcher

Research Article - Araştırma Makalesi

## PUSH OR PULL FACTOR: RATIONALE FOR THE COLLAPSE OF THE OTTOMAN EMPIRE, 1839-1908

The present paper attempts to chronicle the historical reasons for the collapse of the Ottoman Empire from the mid-nineteenth century to the early twentieth century through a discourse of the “Push” and “Pull” analyses. There may be numerous reasons for the phenomenon from varied perspectives, as the empire was grand and spanned nearly 600 years. However, this paper focuses on the “Push” or “Pull” debate rationale raised by Quataert, as put forward by two scholars: Halil Inalcik and Leften S. Stavrianos, respectively. The “Push” perspective of Inalcik viewed the collapse of the Ottoman state as stemming from its good intentions of bridging the equality gap between the various echelons of the state through the promulgation of various Imperial Rescripts, but it failed to implement the reforms holistically in the nineteenth century. In contrast, the “Pull” standpoint of Stavrianos did not see any good intentions from the Ottoman state but attributed the disintegration of the empire to its political and economic exploitation of the subject peoples, especially the non-Muslim subjects. Thereupon, the paper attempts to connect the dots by exploring these two perspectives from the announcement of the Gülhane Edict in 1839 to the Young Turk Revolution of 1908 that ousted the Ottoman sultanate. The paper concludes that the “Push” factor analysis was instrumental in the collapse of the Empire. The paper uses a qualitative research technique through the lens of comparative-historical analysis to probe the phenomenon.

**Keywords:** Ottoman Empire, Tanzimat, Push and Pull Factors, Muslims, non-Muslims



**Received/Geliş Tarihi**

23 March 2025

**Accepted/Kabul Tarihi**

01 May 2025

**Publication/Yayın Tarihi**

31 August 2025

**Corresponding**

**Author/Sorumlu Yazar**

Usman Abass

usman\_abass@yahoo.com

**DOI:** 10.69494/jirps.1663826

**Cite this article**

Abass, U. (2025). Diaspora, Push or Pull Factor: Rationale for the Collapse of the Ottoman Empire, 1839-1908. Journal of International Relations and Political Science Studies, (14), 1-27.



Content of this journal is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License.

## **Introduction**

The period from 1300 to about the latter half of the seventeenth century witnessed the burgeoning of a tiny khanate into an empire with vast territories. This was the Ottoman Empire. It encompassed the Black, Aegean, Mediterranean, Caspian, and Red Seas (Quataert, 2005). Internally, several forces were at play, especially during the reign of Sultan Abdülhamid II, when the concept of modernism interacted with Ottoman-Islamic-Turkish historical factors to produce new syntheses (Karpas, 2001, p. 157). Thus, the 19th century in Ottoman lands was different from previous centuries, as it included competitive consumption of goods; the vizier and pasha households at the centre; the tax farm as the political-financial instrument for revenues linking the two; and the role of the religious scholars, the ulema. With an expanded bureaucracy, activities previously considered outside the purview of the state were embraced. Furthermore, Western knowledge became the kernel of service and mobility in the burgeoning bureaucracy. Western knowledge was infused into Ottoman practices, and this became especially evident during the expansion of the educational system under Abdülhamid II (Quataert, 2005, pp. 62–63).

Before the accession of Abdülhamid II in 1876, Mahmud II (in about 1826) had tried to establish the central government's authority in the provinces by suppressing all powers and privileges. Mahmud II's action was colligated with his cognizance that unless all the authority derived from other intermediaries had been curtailed in the Ottoman state, and the Sultan's will made the only point of authority, no genuine advancement in the direction of reform would be possible. Thus, he abolished the Corps of Janissaries and set up in their stead a new army, the Asakir-i Mansure-i Muhammediye, and dissolved the dervish brotherhood of the Bektaşî (Lewis, 1961, pp. 75, 77-79). Furthermore, Mahmud II modernized existing schools and sent a batch of military and naval cadets to diverse European capitals. They were instrumental in the country's transformation when they returned. He expressed interest in training young diplomats and civil servants in the use of foreign languages. This turned civil servants into an important new element in Ottoman society (Lewis, 1961, pp. 83-84, 89-90). Under Sultan Abdülmecid, Reşid Pasha drafted and promulgated the first of the great reforming edicts in Turkish history, the Tanzimat. One of the most important new institutions created by the Tanzimat for the proper administration of the Empire was the Meclis-i Ahkam-i Adliye, commonly referred to as the Council of Justice (Lewis, 1961, pp. 107-108).

Reşid Pasha's reforms were later reorganized by Ali and Fuad Pashas from 1856 onwards into the Hatt-ı Hümayun. Subsequently, Sultan Abdülaziz continued with the reforms on his accession in 1861.



Ottoman success against Russia over the period 1853-56 led to wider European socio-cultural influences in the empire. The denouements of such influence, according to Karpat, produced two incompatible outcomes: first, “they undermined the traditional social order and mobilized the masses in populist religious movements” that espoused a return to the old order; second, they precipitated “the rise of a new and increasingly individualistic middle class with its own” values and modernist Islamic identity (2001, p. 181). Thus, Lewis was apt when he postulated that by 1871, reforms were so advanced from the old order that the Ottoman land was left with only one path: modernization and Westernization (1961, p. 128). But there were territorial challenges along the way, and from the 1870s to the “Young Turk” revolution in 1908, Ottoman provinces fell away.

What did then account for the rise of nationalism and the eventual collapse of the Ottoman Empire from the nineteenth century to the early twentieth century? There are two schools of thought. These are the “Push” and “Pull” thoughts that Inalcik and Stavrianos espoused, respectively. These two analyses were first put forward by Quataert (2005). He argues that the “push” analysis viewed the collapse of the Ottoman state from its good intentions of bridging the equality gap between the various echelons of the state but failed to effectively implement the intended reforms completely in the nineteenth century. Here, he stressed that the state sought to bring about equality between Muslim and non-Muslim subjects and more equitable relations between elites and the lower strata. However, because it was slow to do so, “frustrations mounted and revolts ensued” (Quataert, 2005, p. 70), thereby leading to the emergence of separatist movements.

Conversely, the nub of the “Pull” analysis centred on Ottoman political and economic exploitation. Quataert noted that nationalist sentiments developed among local leaders who spearheaded the drive for independence due to the deprivation of political rights and mounting economic impoverishment under Ottoman maladministration (2005, p. 70). Thus, it is from this juncture that the study attempted to probe into the views of these scholars to deduce the fundamental causes of the collapse of the Ottoman state. Hence, the paper’s central position is that, while the Pull analysis presents some historical facts, as was the case with old imperium, to back its position as the rationale for the collapse of the Empire, it finds the Push analysis standpoint as the instrumental factor that led to the collapse of the empire by allowing the conquered people to maintain their own identity in tandem with its failed attempt to extend the privileges of the Muslim majority subjects to the non-Muslim minority subjects.

## **Methodology**

A descriptive and explanatory research design was used in this paper. The study utilized qualitative research methods in the form of secondary sources to analyse the causes of the eventual collapse of the Ottoman Empire from the Push and Pull analyses perspective between 1839 and 1908, through the lens of comparative-historical analysis (CHA). CHA is an important methodological approach that is used in social sciences. The aim of CHA, according to Mahoney and Rueschemeyer, is to offer “historically grounded explanations of large-scale and substantively important outcomes” (2003, p. 4). The analysis “assumes that there are large social structures in the real world” that could be grouped into cases of similar nature or cases of different nature (Streeck, 2015, p. 264).

Some of these cases for which CHA concerns itself include, inter alia, nation-states, institutionalized structures, supra and subnational economies, democracies, civilizations, religions, and histories. In its attempt to reach conclusions, CHA regards differences in social structures “to have been caused by identifiable events or conditions in a historical past,” such that those events or conditions are not “to be contemporary with the effects to be causally explained by them” (Streeck, 2015, p. 265). In other words, the comparative-historical analysts parse these past causes as “responsible for present differences”, which were deemed “powerful enough to produce an impact of historical significance, one that is durable, robust, and identity-defining” (Streeck, 2015, p. 265).

Based on this, Mahoney and Rueschemeyer have identified three features for CHA and put forward that it is concerned with “causal analysis, an emphasis on processes over time, and the use of systematic and contextualized comparison” (2003, pp. 6, 10), although not synthesized by one method to arrive at outcomes. These historical analysts ask big questions “about the basic contours and evolution of the modern world” by focusing on “comprehensive structures and large-scale processes that provided powerful clues to the patterning of social life” at individual, group, and state levels across boundaries (Mahoney and Rueschemeyer, 2003, p. 7). Further, these analysts do not generally “seek universal knowledge about all instances of a historically constituted population of cases” in their big-question inquiries (Mahoney and Rueschemeyer, 2003, p. 7), but they rather look for similarities and differences in policies and phenomena within specified historical eras to address present concerns and provide choices for the future. Since CHA is fundamentally aligned with explanation and the identification of causal configurations that produce major outcomes of interest, Mahoney and Rueschemeyer regard the causal argument as central to the

analysis because “causal prepositions are carefully selected and tested” by analysts rather than “introduced ad hoc as incidental parts of an overall narrative” (2003, p. 11). Furthermore, CHA analysts holistically analyse historical events by considering changes over time and considering “the effects of the timing of events relative to one another,” including possibilities of events intersecting with each other and the relative importance of the “timing of that intersection” (Mahoney and Rueschemeyer, 2003, p. 13). By focusing on systematic and contextualized cases of similarities and differences, CHA focuses “on a small number of cases” within defined historical milieus, thus it can achieve “a higher level of conceptual and measurement validity” (Mahoney and Rueschemeyer, 2003, p. 13), because its analysts are well-versed with their cases as opposed to a larger number of cases. Hence, it is in this context that this paper makes use of comparative-historical analysis to establish the Push analysis as the instrumental factor that led to the collapse of the Ottoman Empire.

### **I.The Pull Analysis**

This analysis was espoused by Leften Stavros Stavrianos, a Greek Canadian historian. In his book, *The Balkans since 1453*, which is a synthetic compendium of Balkan[1] historiography, he thoroughly investigated the creation of the Balkan states from about the last years of the First World War and colligated Balkan interrelationships with the Great Powers, including the Ottoman state. The Ottoman state was composed of heterogeneous and polyglot nations, which included Turks, Jews, Arabs, Egyptians, Greeks, Slavs, etc., with ‘unrestrained’ autonomy.

In the Ottoman state, for instance, although the non-Muslim elements paid a special capitation tax, they were free to worship as they wished, and they were allowed to organise into communities with their own ecclesiastical leaders (Stavrianos, 1958, pp. 89-90). In the sixteenth century, Sultan Mehmet II gave the patriarch greater ecclesiastical and secular jurisdiction than he had under the Byzantine emperors. Thus, Stavrianos believed that Mehmet II acted in that capacity to perpetuate the rift between the Catholic and Orthodox worlds (1958, p. 103). The extended jurisdiction of the patriarch came in the form of an ordinance. Among other things, the patriarch was declared “untaxable and irremovable” with “the authority to settle all matters of doctrine”, etc., and could pass judgment

[1] For further readings on how the Ottoman Empire expanded its influence in the Balkans from whence it cemented its presence in Europe, see for example, Standford, J. Shaw, *History of the Ottoman Empire and Modern Turkey: Empire of the Gazis: The Rise and Decline of the Ottoman Empire, 1280-1808*, Vol. 1, New York: Press Syndicate of the University of Cambridge, 1976.

on issues pertaining to “marriage, divorce, and inheritance” (Stavrianos, 1958, p. 104).

In effect, the patriarch served as a liaison between the Ottoman administration and his community. Despite the religious freedom enjoyed by the non-Muslims, Stavrianos held the view that this did not translate into religious equality. Some of what Stavrianos considered unequal, inter alia, were that:

Non-Muslims were forbidden to ride horses or to bear arms; they were required to wear a particular costume to distinguish them from the true believers; their dwellings could not be loftier than those of the Muslims; they could not repair their churches or ring their bells except by special permission which was rarely granted; they were required to pay a special capitation tax levied on all non-Muslim adult males in place of military service (1958, p. 105).

One of the consequences of allowing the conquered people to retain their languages and religions was that it made it easier for them to develop national consciousness. Thus, Stavrianos argued that the Ottomans were able to rule the Balkans for five centuries because they had allowed the Balkan people to live in compact groups with their languages and religions intact. Consequently, when the Ottoman administrative institutions deteriorated in later centuries, it did not threaten their national identity or cohesiveness. Additionally, the Ottomans strengthened the group solidarity of their subjects by granting a large degree of communal autonomy, imposing regulations that separated Muslims from non-Muslims, and exterminating the native aristocracies (Stavrianos, 1958, pp. 112, 114). Hence, Stavrianos opined that, although the latter policy had deprived the Balkan people of their leaders, it freed them from social differentiation and strife, and this was the reason why the Balkan people were able to retain their unity and identity to win their independence (1958, p. 114).

## **II.Reasons for the Decline of the Empire between 16-18<sup>th</sup> Centuries**

The empire started crumbling by the late 18th century. So, what events did lead to that? It began after the demise of Sultan Süleyman the Magnificent with a shift in the succession system. Towards the end of the sixteenth century, the efficacy of the succession system began to decline. This change manifested in how the royal princes were groomed for their respective undertakings. More importantly, in the seventeenth century, Mehmet II's fratricide decree, according to Stavrianos, was modified to the extent that the royal princes, except the sons of the reigning sultan, were confined to special quarters in the palace and denied all communication with the outside world, and they spent their lives in the company of a few eunuchs, pages, and sterilized harem inmates (1958, p. 118).

Thus, the seclusion and the sort of people the princes found themselves with had negative consequences on their thoughts and personalities.

From 1617 onwards, there was an edict which stipulated that the throne should pass to the oldest member of the imperial household. The ramification of that was that future sultans were to be drawn from the brothers, uncles, and cousins who had lived their lives in seclusion. Thus, when they became rulers, they “selected ill-equipped advisers” (Stavrianos, 1958, p. 119). Hence, the internal upshots of the change, inter alia, on the empire included the corruption of the administration as the financial statuses of candidates for office were regarded over their competencies, the ineffectiveness of the fighting force, and the deterioration of the timar system (Stavrianos, 1958, pp. 119-123).

Externally, the empire capitulated to the demands of the European powers. The capitulations exempted the Europeans from Ottoman taxation and courts. It led them to establish direct trade with the provinces of the Ottoman Empire. Among other things, the effect of the capitulations on the empire was marked inflation, debasement of the currency, and the heavy burden of unprofitable and unsuccessful wars (Stavrianos, 1958, pp. 126-127).

Furthermore, as the West made momentous economic gains within the empire, a new political dynamic, nationalism and the notion of nation-states, which emerged in the West, were transmitted into the Ottoman lands. Factors such as “the appearance of a middle-class desiring unity and order, the spread of literacy, and the development of new techniques for mass propaganda and indoctrination” were infused into the idea of nationalism to form new and inclusive nations (Stavrianos, 1958, p. 130). Since the empire’s subjects continued to live as coteries with shared interests, they were linked to their autonomous coteries “in a more religious than a political character” (Stavrianos, 1958, p. 130), which made the empire susceptible to foreign aggression.

But how did the Ottoman regime handle this foreign intrusion? It was poorly challenged because the regime did not have any nationalistic ideologies at that time. Thereupon, the provinces which had been allowed to remain intact with their ways of life and were the beneficiaries of the new political ideologies from the West, started to detach themselves from the Ottoman capital. In the wake of that emerged a nationalist ideology and identity for the Balkan, African, and Arab subjects of the empire. This was followed later by a Turkish nationalism of itself.

What eroded the Ottoman military, intellectual, and economic progress was the empire's approach to the emerging scientific knowledge. For instance, while schools and universities across the rest of Europe were engulfed in empiricism, the Ottoman madrassas "emphasised theology, jurisprudence, and rhetoric at the expense of astronomy, mathematics, and medicine" (Stavrianos, 1958, p. 131). The territorial losses to the Great Powers and the emergence of multifarious ideological demands towards nation-states lasted from the late seventeenth century to the years of the First World War, which catalysed and expedited the crumbling of the empire.

Thus, from Stavrianos' purview, the main rationales for the emergence of newly independent states within the Ottoman empire and its eventual collapse were the military and administrative deterioration of the empire; theocracy replaced nationalism; the rise of chifliks which revolutionised the hungry peasantry in some regions; the growth of commerce and industry, which introduced new social elements and ideas to the Balkan; the contacts with the rest of Europe, which produced an analogous upsurge in the influence of foreign ideologies; the intervention of the great powers, which ended Ottoman relations with the rest of Europe (1958, pp. 222, 226).

### **III. The Push Analysis**

This analysis was favoured by Halil Inalcik, a Turkish historian who specialised in social and economic policies and approaches of the Ottoman Empire and wrote extensively in that regard. In *Application of the Tanzimat and its Social Effects*, Inalcik looked at how the Ottoman state sought to quash inequalities that existed among the various polyglot communities towards establishing equitable relations between them through the passage of the *Gülhane Imperial Rescript*. The imperial document, which was developed by Reşid Pasha and passed by Sultan Abdülmecid in 1839, contained reforms about making non-Muslim subjects of the empire equal to their Muslim counterparts and reorganising the empire.

From the outset, directives were issued for the various articles of the document to be made public to the masses, and to be "thoroughly explained to all the people, great and small" (Inalcik, 1973, p. 3). Thus, the ultimate objective of the decree was to ensure "the well-being of the people", whose happiness was deemed "a necessary pre-condition for the reinvigoration of religion and state and the prosperity of the country" (Inalcik, 1973, p. 4). However, the reformers failed to effectively implement the outlined reforms in the nineteenth century. It must be pointed up that while the Muslims and their leaders objected to the Sultan's decree to extend those privileges to the non-Muslims, the non-Muslim subjects and their leaders on the other hand, were overwrought by the euphoria of "high hopes and created unrest and upheavals" (Inalcik, 1973, p. 4).



To evince its commitment to ensuring the well-being of the people, as early as 1831 and as a presage to the announcement of the Imperial Rescript, the government had launched the first official Ottoman newspaper, *Takvim-i Vekayi*, to improve the communication of imperial policy throughout the empire, and by 1838 the state had started to issue passports to Ottoman subjects, initiated postal service reforms, and established ministries and councils similar to those in Europe (Hanioglu, 2008, p. 62). That is, the Ottoman state was well on course to improving the affairs of its people. One of the vital reforms of the *Gülhane* decree was an attempt at administrative reform towards decreasing the administrative authority of the provinces' governors. According to Inalcik, while the security matters of the provinces were left in their hands, officials with wide-ranging power (*muhassil-emvals*) were appointed directly by the central government and charged with handling financial matters.

Furthermore, new local administrative councils were to be established everywhere to get subjects to participate in administration at diverse levels (Inalcik, 1973, p. 5). This could be viewed as a sort of organic change embedded with a precept of democratisation since it focused on citizen participation in governance. On top of that, the changes also affected the office of the *Şeyhülislam*. For instance, the deputies of the *qadis* were to become salaried employees of the state with monthly salaries like all other Ottoman employees paid directly by the *muhassil* and they were stopped from collecting remunerations, such as “dues on inheritance taxes or fees for judicial deeds and licenses, and for services forming part of their duties”—such remunerations were to be treated as court revenue (Inalcik, 1973, p. 6). This further evinced “the good intentions” of the Empire as it aspired to purge the Ottoman bureaucratic institutions of competing power interests towards creating a homogeneous and equitable state.

Moreover, per the directive of the decree to get people to participate in the administration of the state, upper and lower councils were formed in the provinces, counties, and townships. The upper councils were formed in the capital cities of the counties and in the sub-counties to which *muhassils* were appointed, while lower councils were formed in counties and townships to which *muhassils* were not appointed by the Sultan. A typical upper council had 13 members—6 officials, including the *muhassil* himself and his two clerks, the local *qadi*, the *mufti*, and the security chief; the rest were made up of local Muslim notables, or the metropolitan and two village elders would be included if the population was a non-Muslim one.

Inalcik expressed that “the non-officeholding members of the council had to be elected representatives of the community” (1973, p. 6). With regards to the lower councils, they consisted of five members—the qadi of the place, the security chief, the deputy muhassil, and two local notables—and if there were Christians in the community, one of the notables had to be a Christian village elder (Inalcik, 1973, pp. 6-7). Thus, the reforms made prepense attempts to include non-Muslim subjects in the governance and administrative apparatus of the various provinces and townships.

Nonetheless, one thorny issue that the reformers faced throughout the reform period was that of taxation. There was a systematic endeavour to reorganize the revenue system of the state into a modern revenue budget system where all state revenues were to be collected into a centralized treasury from which state expenses were to be paid. Thence, to achieve this objective, the Tanzimat programme set out to abolish the system of farming out-state-revenue collection and the system of state leases, with the passage of a new law to ensure tax-payers were taxed according to their means and to create a census system and survey of properties to ascertain payments per head (Inalcik, 1973, pp. 8-9).

To that effect, the maktu system (fixed rate system) was introduced across the Empire for tax collection. Thus, from 1840:

A register showing the total of the poll tax paid by a sancak (province) or a kaza (sub-province) was to be presented to the government-appointed muhassil. Based on these registers, the muhassil had to establish on the spot the portion of the total amount collected that a given village had been paying in the past. He then had to call in the village elders and notify them of the sum he had arrived at. To collect the prescribed amount of the poll tax established for their area, the village elders had to portion it out among the inhabitants according to their standing in three categories—they had to set different rates for the wealthy, for the poor, and for those of medium means (Inalcik, 1973, p. 12).

The law seemed fair as it sought to obtain the tax based on the possession and social standing of the subjects. However, the non-Muslim subjects who doubled as the poll-tax payers described the maktu system as a “measure contradictory to the principle of equal taxation proclaimed by the Tanzimat”, while the European press criticised it and “maintained that the proclamation of equal rights was nothing but an empty promise” (Inalcik, 1973, p. 12). They were justified in their criticism of the reforms, which on paper promised equality for both Muslim and non-Muslim subjects in the eyes of the law, but in turn exacted the poll taxes from only the non-Muslims.



However, Inalcik believed that there was no way the Ottoman government could have scrapped the poll tax in one go, thereby it decided to “lift the poll tax by 1851” and convert the same “into a kind of capitation levied equally on every subject,” which came to fruition with the Hatt-ı Hümayun of 1856 whereby the poll-tax was “converted to the military service exemption tax” (Inalcik, 1973, p. 12). However, Zürcher believed the sultan’s decision to grant equality before the law to non-Muslims and to replace the cizye with a military exemption tax in 1856 was achieved under pressure from Britain and France (Zürcher, 2010, p. 62), and promises from the Ottomans themselves to amend the conditions of their subjects (Richard, 1877, p. 4).

Thus, the concomitant effects of the tax-reform tempests were pockets of uprisings in the provinces of Nish and Vidin (see Inalcik, 1973, pp. 21-33). Such uprisings lit the fire of the emergence of independent states and the disintegration of the Ottoman Empire. Thus, although the expansion of the new military service exemption tax to include the Muslim-majority subjects from 1856 onwards should have conciliated the non-Muslim subjects that the Ottoman regime meant to keep all the promises it made in the intended reforms, it did not. Why? This was because “the realization of these promises was slow in coming and the rights granted to them (non-Muslim subjects) were not immediately recognized” (Inalcik, 1973, p. 29).

In the empire from the onset, social and political order, as delineated by Quataert, was based on differences among ethnicities, religions, etc. Forming part of the distinction of the era were the clothing laws of the eighteenth century. This law stipulated the dress code for different classes of people, and “some colours and certain fabrics worn by Muslims” were disallowed to non-Muslims, who also “were ordered to wear other colours and materials” (Quataert, 2005, pp. 44, 65). However, the Ottoman centralization and reform efforts of the nineteenth century tried to eradicate all those distinctions and to bring all its subjects directly under the Sublime Porte.

Thus, between 1829 and 1856, three enactments—the 1829 clothing law, the 1839 Gülhane Decree, and the 1856 Hatt-ı Hümayun—were passed by the Sublime Porte to remove all distinctions among the empire’s subjects and to “bring its Christian subjects who had become proteges of foreign states under direct Ottoman jurisdiction” (Quataert, 2005, pp. 65-66). Thereupon, if the Ottoman state intended to institute its own “civilizing” reforms by granting equal rights to all persons found within its territory, towards creating a homogeneous modern state, why did the Ottoman state fail to achieve that or implement its reforms successfully?

#### **IV.Impediments to the Successful Implementation of the Reforms**

There were sound impulses behind the various edicts, albeit not all of the proclamation was locally developed. Hanioglu expressed that the Tanzimat reformers incorporated foreign ideas into the Gülhane Decree to “serve as an insurance to the Great Powers that the empire was bent on domestic reforms in return for future recognition as a member of the concert of Europe” (2008, p. 73).

The Ottoman state’s shift in socio-political policy from the eighteenth century to emphasize equality and change in social basis was shaped by three factors. These were (1) the French Revolutionary principles of the rights and obligations of man; (2) European economic strength which had surpassed that of any other region and had promoted the economic power of the Ottoman Christians more than the Muslims; (3) the systematic attempt to retain the loyalty of the Ottoman Christian subjects in the Balkans who were courted by Russia and the Habsburgs and the separatist movements (Quataert, 2005, pp. 67-68).

Hence, the implementation of the reform was flawed from the outset, as its architect, Reşid Pasha, failed to effectuate the reforms successfully. Inalcik (1973) said it failed because the new system lacked personnel to see to the actualization of the proposed reforms. The maktu system was challenged by many of the notables in the provinces who earned their money as provincial tax farmers. These groups realized that the new form of taxation required them “to pay considerably higher taxes” and “deprived them of the benefits they had obtained previously from the inhabitants through forced labour” (Inalcik, 1973, p. 13). Hence the repercussions of this protestation were the emergence of uprising in 1841 in Nish and 1850 in Vidin, among the Christian notables and the peasant population themselves, while the Muslim inhabitants also turned against the reforms and “adjudged it a great injustice to be subjected to the taxation” which hitherto they were exempted (Inalcik, 1973, pp. 22-23, 30-32). In other words, the collective consequence of this was the eruption of an uprising against the government and Muslim subjects on one hand, and the peasants and their wealthy Christian notables on the other hand.

Russia used the uprising as a pretext to get involved to be seen as protecting the Christians in the Balkans (Inalcik, 1973, pp. 25-26), and other powers joined Russia in the defence of the Christians. The Sublime Porte despatched Ahmet Tevfik Bey, in its efforts to end the uprising and to prevent the involvement of foreign powers, with investigating and reporting on the event to the government. Per Ahmet Tevfik’s findings, the turmoil was not caused by “the unjust treatment the population had suffered in tax and other matters”, but it was caused by “an

upheaval of a political nature” towards a demand for “the annexation of the region to Serbia”, which the Christian peasants had hoped that the Muslim inhabitants would realise and eventually leave the area (Inalcik, 1973, p. 27). Thus, to keep the territory as part of the empire and to prevent Christians from taking refuge in Serbia, it was decided that “the non-Muslim subjects be pacified to bring the unrest to rest” and “the Sultan ordered the distribution of 150.000 piastres to the non-Muslim subjects as his imperial gift” for their losses in the uprising (Inalcik, 1973, p. 28). The hands behind the turmoil were said to be those of the Christian notables who took leading roles with the hopes that, if the Ottoman authority proved unsuccessful and the Muslim residents were to leave the area, they would take charge as landowners (Inalcik, 1973, p. 29).

Furthermore, the proclamation about getting people to participate in local administration was slow to be implemented. Not only that, but it was also largely skewed towards the Muslim subjects and was nobility-centred. According to Inalcik, the new councils were composed of members of “government employees responsible to the governors” picked from the leading men of the place, and even though the councils were “to represent the people of their respective areas, the Muslim members in them were in the overwhelming majority even in places where the population consisted mainly of Christians” (1973, p. 14). Hanioglu, on the other hand, expressed that the representative system created by the Tanzimat was practically undemocratic “but was a policy designed to co-opt different ethno-religious groups into the administration by soliciting advice and intelligence from their loyal and respected leaders without actually allowing them to participate in political decision-making” (2008, p. 76). Nonetheless, the point must be made that organic change requires time to materialize, and thus the reforms could not have been effectuated instantaneously because there were matters of pressing judicial reforms and structurally social, economic, and political changes that must be enacted for it to succeed.

Thus, two years into the Gülhane reforms, Reşid Pasha was dismissed due to these shortcomings and replaced by Riza Pasha. The latter took a stance and sought to “appease the conservative Muslim elements” by abolishing the office of the muhassil, restoring the governors’ authority of their provinces, terminating the established salaried status of the deputy qadis, and permitting qadis to once again take their legal fees directly in the courts (Inalcik, 1973, pp. 19, 21). In effect, he rolled back all the changes initiated by Reşid Pasha.

Thus, the reform edict that commenced on the prescripts of ensuring a fair and equal system ended up pitching the peasants against the landowners, and Muslim subjects against non-Muslim subjects.

The outcome was that individuals or groups with political interests capitalised on the loopholes in the reform to turn the social reforms into political demands. Zurcher was apt in expressing that “the Ottoman reformers were late in recognizing the power of nationalism and the danger it brought to the empire” (2010, p. 60), and their policies might have contributed greatly to the disintegration of the empire. Thus, two parallel groups emerged. While the Christian leaders were bent on extending the meaning of the reforms to give their endeavour a nationalistic character in close working with the peasantry, the Muslim landowners and notables were anxious to preserve the traditional social structure sanctioned by the Sharia (Inalcik, 1973, p. 33). Thereupon, the desire of communities to detach themselves permanently to form independent nations came to characterize the empire in the nineteenth century.

To explore the causes of the failures of the Tanzimat statesmen, Carter V. Findley came up with four factors he termed “the structural weaknesses” that weakened their position in implementing their reforms. The first was “the mimetic quality of the reforms,” i.e., the postulation that some of the reforms in the Tanzimat, like the Council of State and some legal codes of the period, imitated knowledge of Western prototypes (Findley, 1989, pp. 156-158), as such they were not original to the Ottoman statesmen and were not implemented well. The second was “the problems of human and economic resources” i.e., the Tanzimat reformers “lacked subordinates prepared to understand and support their efforts” (Findley, 1989, p. 158), as the available schools failed to churn out the needed personnel. This failure manifested immensely on the economic front and stalled progress in the state because of their inability to create a truly centralised treasury system, which led to the burgeon salaried officials overburdening the state and the emergence of tax resistance in the face of expanding government structures due to the bureaucratization of the provincial administration (Findley, 1989).

The third was “the inconsonance of reformist principle and political behaviour,” which Findley said had emanated from “the imperfect extent to which they accommodated their political behaviour to certain implications of their own reforms” (1989, p. 163). They failed to develop a clear political principle but held on to the tradition of patrimonial factionalism and used the reform measures to vilify their political enemies (See Findley, 1989, pp. 164-165). Furthermore, the fourth identified structural weakness was “the problems that the westernizing reformers experienced in the legitimation of their power and their policies”. The reformers did not have a smooth run in their attempts to implement their reforms. In their search for a political balance to legitimate their policies they had to contend with three traditional sources of legal authority,

which Findley identified as “the Islamic religious-legal tradition, custom, and the will of the sovereign” and they depended on the latter since their policies did not conform to the first two (1989, p. 166). Thus, the reformers, it seemed were content with the superficial application of their reforms which would justify Findley’s expression that they “feared to go further and were, in any case, in no position to attempt a thoroughgoing restructuring of the polity as traditionally conceived” (1989, pp. 166-167).

## **V.The Hamidian Era and the Struggle to Maintain the Empire**

According to Yasamee (2011), the decline of the Ottoman Empire was relatively swift between 1768 and 1839, with the decisive loss of power occurring in the 1820s and 1830s. As part of the nineteenth-century reforms, edicts were promulgated towards establishing a single legal framework for all the subjects and transforming the clusters of communities into one single Ottoman identity. The Muslim ulema were not the only religious figures to oppose or feel threatened by the new reforms, the non-Muslim clerics also “viewed the policies as a threat to their positions in the established order” to the extent that “the Ottoman religious communities insisted that any new privileges must be conferred upon them as a distinct community, not as Ottomans” (Hanioglu, 2008, p. 75). Thus, from the outset, the Imperial Decrees were fraught with insurmountable challenges.

Although the Ottoman state went ahead in the nineteenth century to even abrogate old laws to accommodate the changes of the Tanzimat by applying the same measures to Muslims and non-Muslims, extended “testimony in courts to Christians” (Karpat, 2002, p. 546), and allowed huge numbers of non-Muslims in official government services (Findley, 1989, p. 23), the changes could not be fully implemented and controlled and eventually resulted in the breakaway of the empire. The reforms further stratified the social fabric of the Ottoman state by creating new cultural cleavages such as “the new Westernist elite, Ottomanism, and egalitarianism” (Findley, 1989, pp. 201-202).

Thus, from Yasamee’s (2011) purview, the empire declined because of its vastness and large subject populations, as its Christian subjects became a potential weapon in the hands of foreign powers, and it pursued a cheap tradition of a flexible provincial government that rendered the empire vulnerable to the imperial powers’ technique of “peaceful penetration”. Additionally, the privileges of capitulations were used by the powers to weaken the empire’s economic actions, and more importantly, the Muslim front had become divided from 1878 as the “centralising effects of the Tanzimat reforms had not been fully felt in outlying regions,

including Albania and the bulk of the Arab provinces” in tandem with the failure of the centralization attempts as local power remained in the hands of landowners, tribal chiefs, religious leaders and other influential men (Yasamee, 2011, pp. 2-3, 46).

In effect, the reforms failed to achieve their intended objective of creating one Ottoman state, and the millets continued to exist. The Tanzimat reforms rather appeared to have instigated the non-Muslim subjects towards nationalism and eventually demanded permanent political separation from the empire. Thus, Zurcher has postulated that the empire failed because it lacked the manpower, money and industrial base to compete with European powers, and the division of labour between Muslims who dominated the state apparatus and a modern industrial and commercial sector dominated by Christians under foreign protection (2010, p. 72), meant that the Christians possessed the wealth, social and cultural identities, and political leverage to demand or force separation from the empire.

For instance, the Greeks and the Armenians were well-educated millets of the empire. The Greeks from an early date had viewed the Ottoman Empire as the Tourkokratia. According to Issawi, they held this view because the Turks and other Muslims apart from being in total control of the government in terms of commanding the armies, governing the provinces and dispensing justice in the qadi courts, raising taxes and controlling the bureaucracy and serving as advisers and ministers to the sultan, had “delegated many economic, social, and cultural activities to their millets” (1999, pp. 1-2). What occurred was that they utilised those avenues to maintain their cultural roots, develop national consciousness, and control commercial activities in the empire.

Thereupon, when Sultan Abdülhamid II came to power, he attempted to alter the failed Ottoman citizenship reform around Islamism to save the empire. Karpas believed Ottomanism was successful, but not how the Ottoman government had envisioned it, as it came to represent a sort of Islamic (political) ideology among the Muslims (2002, p. 546). Nonetheless, the question is, why did Sultan Abdülhamid II agree with the Great Power’s Berlin Treaty of 1878? The deterioration of the empire did not start with him, as was highlighted above. He only assumed control of an empire on the verge of disintegration. Sultan Abdülhamid II came to power in August 1876 (Sancak, 2019), in the latter stages of the war with Russia.[2]

[2] For further reading on the Russo-Turkish war of 1877-8, see, for example, R. Grant Barnwell, *The Russo-Turkish War*, San Francisco: A. Roman & Company, 1877.



Karpat believed that the Ottoman-Russian War of 1877-8 and its consequences caused the ruination of the Ottoman reforms. Karpat expressed that the changes the war brought:

...distorted and diverted the general course of the socio-cultural evolution in the Ottoman domains by making ethnic and religious affiliations the ideological basis of the newly independent national states, and by accelerating the emergence of a socio-economic system which intensified the political, social and ethnic conflicts in the area (2002, p. 352).

Thus, Karpat affirmed that the main casualty of the war was “the constitution of 1876 and the two-chamber parliament which aimed at giving political representation to all the chief ethnic and religious groups living in the state” towards “achieving the modernization of Ottoman bureaucracy and the fiscal system” (2002, p. 352).

Before Sultan Abdülhamid II came to the throne, Mithat Pasha and his liberal constitutionalists in 1876 had attempted to restrict the throne’s power and sought a new source of legitimacy for it in a consensus of the people with the aim of “generalizing Ottomanism and to give the non-Muslims representation in the government” (Karpat, 2001, p. 164). This was something the European powers detested. Thus, when Mithat Pasha presented his constitutional ideas to the European powers at the Istanbul Conference in 1876, they rejected them and instead presented their own list of reforms, which Mithat Pasha also rejected. Afterwards, Russia employed war as the only alternative left to solve the Eastern Question. This war in effect, according to Karpat, “was a religious war which aimed at destroying the Muslim Ottoman society and at replacing it with national states whose national ideology was inspired by the Russian Pan-Slavic and Orthodox Christian concept of nationality” necessitated by the “fear that the reforms contemplated by Mithat Pasha” and his group “might strike roots and succeed in solving the country’s problems” (2002, pp. 352-353).

Sultan Abdülhamid II was a reluctant politician who combined four political outlooks: autocracy, conservatism, reformism and Islam (Yasamee, 2011, pp. 20-23, 41-44). European literature had depicted him as an anti-Western civilization, which he was not. Karpat stated that Sultan Abdülhamid II was the most Europeanized sultan in terms of his daily living habits, promotion of modern reforms in education, and government, and transformed the inner fabric of the Ottoman society more profoundly than the Tanzimat reforms, kept many close confidants who were non-Muslims, and extended government services and high positions to many Christians over Muslim subordinates (2001, p. 155).

He blended the traditional and new, Islamic and Western traditions. His religiosity was not cast aside but featured prominently in his reign. Deringil postulated that the sultan came to be represented by symbols (those about his sacrality, personal and imperial munificence, and religious symbols) in the society (1998, pp. 18-19, 21, 25).

When he started his reign, he knew the weaknesses of the empire—economically and militarily—and as such sought to shake up the existing societal structure towards the survival of the state. Thus, when presented with the dilemmas of the Treaty of Berlin of 1878, he juxtaposed his foreign policies with the ongoing internal challenges and opted to focus on the latter. Thus, as Yasamee put it, his principal objective “was to secure the external peace and security essential for the accomplishment of the internal reorganization and regeneration upon which the empire’s survival ultimately depended” (2011, p. 41).

Unlike his predecessors, Abdülhamid II did not trust the European Powers because of the outcome of the Eastern Question. Yasamee expressed that his predecessors had assumed that all the powers, but Russia, were in favour of the Empire’s preservation and that they could rely on Britain to defend the empire against a Russian attack (2011, pp. 43-44). Conversely, the sultan believed that the British, in particular, were bent on the destruction of the empire when during the Eastern Crisis the British, the French and the Austrians combined with Russia at the Istanbul Conference of 1876 to put forth a programme intended to destroy the empire from within, and in 1878 they again combined with Russia to produce the Treaty of Berlin “despoiling the Empire of substantial European and Asiatic territories in what amounted to a form of preliminary partition” (Yasamee, 2011, p. 44). Thus, the Berlin Treaty declared formal independence for most of the Balkan states. Not only that, but the sultan’s reluctance also to confront the powers and his reliance on “peaceful” diplomacy easily gave away other nominal territories of the empire like Tunisia to the French in 1881, Egypt to the British in 1882, the annexation of Eastern Rumelia by Bulgaria in 1885, with Sudan and Eritrea to follow subsequently (Hanioglu, 2008, pp. 129-130).

As the most Europeanized Sultan, Abdülhamid II pursued laissez-faire economic policies towards businesses and built infrastructure to expand the economy. Thus, his economic policies led to over-reliance on the West and produced an Ottoman commercial bourgeoisie who were mostly Christian and an Ottoman-Muslim agrarian elite, and the acceptance of material welfare and pleasure (Karpas, 2001, p. 162). Thus, he felt betrayed, during the partition of the empire, by especially the Christian elements whose economic and social influences he had helped to create.



Yasamee has put forward two possible explanations for the Sultan's feeling of betrayal: religious and diplomatic reasons. Religious because "as Christian states, the Powers felt a common antipathy to the Muslim Ottoman Empire, and this had overridden their mutual conflicts of interest", and diplomatic in the sense that "the unification of Germany had destroyed the Crimean balance of power, weakening France and Austria-Hungary, isolating Britain, and forcing the Powers which had hitherto protected the empire to safeguard their own interests by attacking it" (2011, p. 44).

What followed the Berlin Treaty was an attempt by the Sultan to establish his legitimacy and to find a political ideology that would appeal to the Muslim subjects, just like the Christians did to prolong the empire. Thereupon, in domestic affairs, he strove to safeguard his absolutist rule against the disruptive forces of nationalism and constitutionalism to the extent that he utilised spying and censorship to gag his critics (Tunaya, 1985), and he discouraged travel and study abroad (Stavrianos, 1958, p. 525). He perceived the liberal constitutional elements "as a great danger to his regime" because for 30 years (Heyd, 1950, p. 20), this clique of intelligentsia had become his ardent critics, insisting that he restore the constitution of 1876 and reopen the parliament. Thus, he came to rely on the ulema.

To concatenate the dots, the 1876 constitution which was shown to him by Midhat Pasha, and he accented to, was the one that granted and affirmed representation and equality before the law to non-Muslim subjects. The Christian millets backed by the European powers objected to that and so capitalised on the Berlin Treaty to separate their Christian fellows from the empire. Thereupon, Sultan Abdülhamid II turned on Midhat Pasha and his liberal compeers. For instance, in 1877, the sultan forced Midhat Pasha to resign as the Grand Vizier and in 1881, charged him with the murder of Sultan Abdülaziz. Midhat was sentenced to life imprisonment in the same year and exiled to Taif, where he died (see Tunaya, 1985, p. 33). Subsequently, Sultan Abdülhamid II suspended the 1877 parliament, which had eighty Muslim members and fifty non-Muslim members, for a period of thirty years, 1878-1908 (Tunaya, 1985, p. 33).

Thus, his critics and opponents, in the face of mounting persecution, were compelled to flee the empire for refuge abroad. The opponents of Abdülhamid II's regime included some "ulema, bureaucrats, and nationalists" (Hanioglu, 2008, p. 144). Some ulema criticized his endorsement of materialism and worldly pleasure, which they deemed did not conform to Islam. Collectively, the opposition strands became known as the Young Turks. What political ideology did the sultan settle on as the potential unifier of the Muslim subjects?

According to Karpas, since Arabs constituted the largest Muslim group, Abdülhamid II “engaged in a policy seeking to integrate fully the Arabs into the Ottoman state” through Islam as an ideology to cement the bonds between the centre and the periphery (2002, p. 549).

It was unconventional in Ottoman history that the state “used ideology advisedly and consciously” through Islamism, “not as a means to promote Islam but rather to promote political goals, namely internal unity” (Karpas, 2002, p. 549). As part of his thoroughgoing reforms, the sultan’s role came to be conceptualized in the state as its main source of “unity and legislative authority apart from Islamic law and established custom,” kanunnames or codes were promulgated to circumvent the Islamic laws, the sultan’s power was vigorously used to issue decrees, and integrated “religious-legal scholarship through the Hanafi methods” (Findley, 1989, pp. 7-9). According to Deringil, the Hanafi mezheb was adopted as the official ideology of Abdülhamid II’s empire to conciliate “the resentment of the 1839 Tanzimat era, where the Muslim elements felt the equality status extended to the non-Muslims was a threat to their position” (1998, p. 48).

His use of Islam to integrate the Arabs into Ottoman society later presented a new challenge, especially to the Ottoman elites: that of an identity crisis. Would the new society be able to maintain its Ottoman and Turkish identity, or would it be replaced by an Arab identity? According to Karpas, this dilemma came to the fore from 1908 onwards, when some political leaders began to think in terms of “an ethnic Turkish nationalism, based on religion and ethnicity” and the adoption of “Turkish as their main language of communication” to unite the state (2002, pp. 552-553), which in turn led to the rise of a series of Arab nationalism and demands for separation from the empire. Furthermore, Abdülhamid II found himself in quandaries about three situations: (i) the Armenian nationalist awakening; (ii) the island of Crete that wanted a union with Greece; (iii) Macedonia (Stavrianos, 1958, p. 525). The latter, for instance, was instrumental in the internal uprising that led to his overthrow by the Young Turk Revolutionaries in April 1909.

## **VI. Push and Pull Factors through the lens of Comparative Historical Analysis (CHA)**

Comparative-historical analysis aims to explain the outcome of large-scale historical changes, which occurred in the past but whose effects are felt in the present or the future, by asking big questions. From such a standpoint, this paper asked whether it was the Push or Pull perspective that caused and expedited the collapse of the Ottoman Empire. By this, the paper has delineated the causal argument element of CHA, which is central to it and denotes identifying the contours that produced the outcome of interest.

The Pull analyst had argued that the Ottomans were able to rule the Balkans, for instance, for five hundred years because they had allowed the conquered people to live in their compact groups, though with vestiges of differential treatment such as non-Muslims made to pay poll tax and to wear particular costume to distinguish them from the Muslims. This was the praxis for empires of the past. For instance, on the African continent, the British Empire imposed the poll tax and hut tax on their colonies, and the Spanish introduced the quinto real in South America towards generating income for social, economic, administrative, and defence purposes. Unlike in Africa and South America, where the imperial powers forced their religious beliefs and languages on the local people, the Ottomans did not do so in the Balkans but allowed the people to maintain their religious communities and even granted the patriarch the authority to adjudicate religious and social life issues of their members. However, the big question is, why did the Balkan states not secede from the Empire when those differences were visible, but only did that when the Empire attempted to bridge the inequality gaps among its subjects?

Furthermore, the Pull analyst argued that from 1617 onwards, Ottoman economic and administrative structures had become corrupt and paved the way for its ruination and the emergence of independent nation-states in the Balkans. Yet, it was only from the middle of the nineteenth century onward that the independent movements gained momentum. Hence, what could have been the catalyst to push through such demands? The answer, inter alia, is the passage of the Gülhane Imperial Rescript of 1839, to promote the well-being of the Empire's subjects, including the non-Muslims. It gave them glimpses of what being equal with the Muslim-majority subjects meant. Thus, as the non-Muslim subjects clung to the ropes of liberation, the Muslim front remained disunited as the subjects objected to the attempts to extend their privileges to the non-Muslim subjects.

Although the imperial document had instituted new local administrative councils everywhere for the subjects to be involved in the administration of the provinces of the empire to the extent that Christian notables and village elders were made part of them, and Islamic religious figures were made salaried employees of the state like all other state employees to create a homogenous and equitable society, the non-Muslim subjects protested the implementations of the irade. Such demurrals did not occur in nihility but coincided with other historical events of equal weight. This thus leads to the consideration of the second feature of CHA, which is the consideration of historical changes over time, including the timing of events and their intersection with other events of relative importance.

The period coincided with the increasing economic strength of Christian European states. Hence, both analysts agreed that the European states promoted the economic power of Ottoman Christians by establishing direct trade with them and made efforts to win their loyalty through the introduction of the notion of nation-states. The Ottoman statesmen were late in recognizing the subtle effects of the foreign ideologies that originated from mainland Europe on their provinces in the Balkan region. On top of that, they did not have any national ideology for the empire. Thus, as the Tanzimat statesmen clambered over the residues of their reforms to salvage the empire from the increasingly interventionist approach of the Great Powers, they faltered because they lacked the personnel, among other things, to see to the realization of the reforms they had set in motion. This failure thus catalysed the emergence of politically inclined groups within the empire towards secession. Thus, according to the Push analyst, it was this slowness in implementing their reforms and their failure to pre-empt the dangers of the multitude of foreign political ideologies into their provinces that intersected with their reform agenda to cause the eventual disintegration of the empire.

## **Conclusion**

For centuries, the successes of the Ottoman Empire hinged on its military might and on allowing ethnic and religious distinctions among its subjects. The subjects were allowed to organize into clusters of communities with their religious leaders and languages, and they were free to worship and conduct their economic activities upon paying the *cizye*, which guaranteed their security under the dominant Muslim subjects. From 1829, attempts were made by the Ottoman government to scrap some of the restrictions. That attempt ushered the empire into a period of reforms. While some viewed the reforms as an influence from the 'civilizing' principles of the West, others juxtaposed the necessity of the reforms to the deterioration of Ottoman military might, its intellectual and economic retrogression due to its focus on theology, jurisprudence and rhetoric in an era where Europe and the Christian world was engulfed in empiricism.

These structural changes in the social, economic, and political fabric of the Ottoman society meant that the Ottoman Empire was no longer equipollent to the might of the Christian West, whose economic and military strengths were on the horizon. Thus, the Ottoman policy of allowing the confessional communities to retain their languages and religion was exploited by the West at a time when the Ottoman state was declining to influence the Christian elements of the state with political ideologies of national consciousness from mainland Europe.

The response of the Ottoman statesmen was to introduce the Gülhane Rescript in 1839, which was later reorganized into the Hatt-ı Hümayun of 1856. The quiddities of the reforms were to promise equality for all Ottoman subjects, including the non-Muslims before the law, to reform the tax regime, to scrap forced labour, to abrogate certain traditional laws including the one on poll-tax, and to allow citizenry participation in the administration of the provinces, inter alia, as means of retaining their non-Muslim subjects.

However, the soi-disant reforms later initiated the rapid ruination of the empire. According to Mardin, what Reşid Pasha failed to anticipate when drafting those reforms and making promises was the fact that “specific demands to establish equality between Moslems and Christians would come soon” in tandem with his failure to “foresee that they (the demands) would be as strong and explosive as they turned out to be” (2000, p. 14). The demands became strong and explosive and raised diverse problems for the Ottoman state for several reasons—because commercial and industrial control was in the hands of the Christian subjects backed by the Western powers, there was growth in missionary activities to maintain the distinctions, the influence of Enlightenment principles on the Christian population of the empire and the subsequent eruption of national consciousness amongst them, the incessant interest of the European powers as the protectors of the Christian, and the fact the some of the Muslim subjects were against the Imperial documents and what they offered to the non-Muslims because they stripped them of their privileges. The Ottoman statesmen believed that surrendering the privileges of the Muslim subjects, according to Mardin, “should be the price paid for the establishment of an Ottoman nationality under which everyone would fully enjoy the benefits of state services as well as the equal protection of the laws” (2000, p. 15).

The implementation of the reforms was replete with turmoil and demurrer, especially the tax reforms. Thus, from 1841 it led to the rise of peasant revolts first in Nish and in 1850 in Vidin and later became widespread across the empire. The theme of the uprising was the fulfilment of the promises made by the Tanzimat statesmen and for the principles to be applied equally to all subjects, which the statesmen failed to do. They were in no position to actualize their reforms because they had failed to train staff for the tasks ahead, the reforms incorporated foreign ideas alien to the empire, which the statesmen themselves were unable to implement fully, and they also failed to develop a clear political path to legitimate their authority and policies. This outcome stratified the Ottoman state into two parallel groups: Christians and their leaders who came to interpret the reforms politically and gave it a nationalistic character, and the Muslims and their landowners and notables who were bent on preserving the status quo sanctioned by Sharia.

The latter manifested vividly during the reign of Sultan Abdülhamid II, who came to rely on Islam and the ulema as a unifying political ideology to retain the empire post-Berlin Treaty of 1878. The Treaty marked the end of the Eastern Question, where the powers rejected the constitutional reforms submitted by Midhat Pasha towards solving the Ottoman internal crisis to rigorously demanding the establishment of independent Christian states for nearly all the Balkan subjects of the Ottoman Empire. Abdülhamid accepted the Treaty as a way of surviving as he could not match the army and resolve of the Great Powers and was slow to take decisive military actions against the powers, both in the Balkan and in the North African provinces, which led to the loss of Ottoman territories to the powers (Russia, France, and Britain in particular). Hence, post-haste of the Berlin Treaty, Abdülhamid II took steps and tools such as spying, censorship, and exiles to rid himself of the liberal constitutionalists whom he saw as a nuisance to establish his absolute rule. Had the Treaty of Berlin failed, and the populist reforms of the liberal statesmen succeeded in uniting the state, the sultan would have accepted the role of a constitutional sultan, and he would not have tried to eradicate the constitutionalists from his administration.

In conclusion, while the “Pull” standpoint may have some merits as was the case with well-nigh empires of the past, the “Push” standpoint resonates well with the good intentions of an empire which hitherto had allowed the non-Muslim subjects to maintain their own identity and was willing to strip away and extend the privileges of the Muslim subjects to the non-Muslim subjects. Such attempts should not be taken superficially, for had it succeeded, it would have become a model for other imperial powers to emulate. Thereupon, it is prudent to view the actions of Sultan Abdülhamid II in the form of suspending the parliament and distancing himself from the liberalists as a desperate attempt at a desperate time by a desperate ruler who was willing to go the extra mile to protect his empire at all costs. Nonetheless, the upshots of his actions were baleful and led to the emergence of the Young Turk group as an opposition to his regime. This group eventually toppled his administration in 1908 and paved the way for the establishment of the modern Turkish Republic by Gazi Mustafa Kemal Atatürk in 1923.

## **Bibliography**

- Barnwell, G. R. (1877). *The Russo-Turkish war*. San Francisco: A. Roman & Company.
- Bein, A. (2011). *Ottoman Ulema, Turkish Republic: Agents of Change and Guardians of Tradition*. Stanford: Stanford University Press.
- Deringil, S. (1998). *The Well-protected Domains: Ideology and the Legitimation of Power in the Ottoman Empire 1876-1909*. I.B. Tauris Publishers.
- Findley, C. V. (1989). *Bureaucratic Reform in the Ottoman Empire: The Sublime Porte, 1789-1922*. New Jersey: Princeton University Press.
- Hanioglu, M.S. (2008). *A Brief History of the Late Ottoman Empire*. Princeton: Princeton University Press.
- Hanioglu, S. M. (2001). *Preparation for a Revolution: The Young Turks, 1902-1908*. Oxford: Oxford University Press.
- Heyd, U. (1950). *Foundations of Turkish Nationalism: The Life and Teachings of Ziya Gokalp*. London and Beccles: Luzac & Company and The Harvill Press Ltd.
- Inalcik, H. (1973). *Application of the Tanzimat and Its Social Effects*. Belgium: The Peter de Ridder Press, (5): 1-36.
- Issawi, C. (1999). Introduction. In Gondicas, D., and Issawi, C. (eds.), *Ottoman Greeks in the Age of Nationalism: Politics, Economy, and Society in the Nineteenth Century*. New Jersey: The Darwin Press, Inc., 1-16.
- Karpat, K. H. (2002). *Studies on Ottoman Social and Political History: Selected Articles and Essays*. Ed. Reinhard Schulze, Vol. 81. Leiden: Brill.
- Karpat, K. H. (2001). *The Politicization of Islam: Reconstructing Identity, State, Faith, and Community in the Late Ottoman State*. New York: Oxford University Press.
- Lewis, B. (1961). *The Emergence of Modern Turkey*. Second Edition, London: Oxford University Press.
- Mardin, S. (2000). *The Genesis of Young Ottoman Thought: A Study in the Modernization of Turkish Political Ideas*. New Jersey: Syracuse University Press.



- Barnwell, G. R. (1877). *The Russo-Turkish war*. San Francisco: A. Roman & Company.
- Bein, A. (2011). *Ottoman Ulema, Turkish Republic: Agents of Change and Guardians of Tradition*. Stanford: Stanford University Press.
- Deringil, S. (1998). *The Well-protected Domains: Ideology and the Legitimation of Power in the Ottoman Empire 1876-1909*. I.B. Tauris Publishers.
- Findley, C. V. (1989). *Bureaucratic Reform in the Ottoman Empire: The Sublime Porte, 1789-1922*. New Jersey: Princeton University Press.
- Hanioglu, M.S. (2008). *A Brief History of the Late Ottoman Empire*. Princeton: Princeton University Press.
- Hanioglu, S. M. (2001). *Preparation for a Revolution: The Young Turks, 1902-1908*. Oxford: Oxford University Press.
- Heyd, U. (1950). *Foundations of Turkish Nationalism: The Life and Teachings of Ziya Gokalp*. London and Beccles: Luzac & Company and The Harvill Press Ltd.
- Inalcik, H. (1973). *Application of the Tanzimat and Its Social Effects*. Belgium: The Peter de Ridder Press, (5): 1-36.
- Issawi, C. (1999). Introduction. In Gondicas, D., and Issawi, C. (eds.), *Ottoman Greeks in the Age of Nationalism: Politics, Economy, and Society in the Nineteenth Century*. New Jersey: The Darwin Press, Inc., 1-16.
- Karpat, K. H. (2002). *Studies on Ottoman Social and Political History: Selected Articles and Essays*. Ed. Reinhard Schulze, Vol. 81. Leiden: Brill.
- Karpat, K. H. (2001). *The Politicization of Islam: Reconstructing Identity, State, Faith, and Community in the Late Ottoman State*. New York: Oxford University Press.
- Lewis, B. (1961). *The Emergence of Modern Turkey*. Second Edition, London: Oxford University Press.
- Mardin, S. (2000). *The Genesis of Young Ottoman Thought: A Study in the Modernization of Turkish Political Ideas*. New Jersey: Syracuse University Press.



Mahoney, J. and Rueschemeyer, D. (2003). Comparative Historical Analysis: Achievements and Agendas. In Mahoney, J., & Rueschemeyer, D. (Eds.), *Comparative Historical Analysis in the Social Sciences*. Cambridge: Cambridge University Press, 3-38.

Quataert, D. (2005). *The Ottoman Empire, 1700-1922*. 2<sup>nd</sup> Ed. Cambridge: Cambridge University Press.

Richard, H. M.P. (1877). *Evidence of Turkish Misrule: Papers on the Eastern Question*. No. 1. London: The Eastern Question Association.

Sancak, L. (2019). *The Islamism of Abdulhamid and its Opposition in the Last Period of the Ottoman Empire*. Unpublished MSc. Thesis. METU, Ankara.

Shaw, J. S. (1976). *History of the Ottoman Empire and Modern Turkey: Empire of the Gazis: The Rise and Decline of the Ottoman Empire, 1280-1808*. Vol. 1. New York: Press Syndicate of the University of Cambridge.

Stavrianos, L. S. (1958). *The Balkans since 1453*. New York: Rinehart & Company, Inc.


Tunaya, T. Z. (1985). 1876 Kanun-i Esasisi ve Türkiye’de Anayasa Geleneği. In M. Belge, and F. Aral (eds.). *Tanzimat’tan Cumhuriyet’e Türkiye Ansiklopedisi*, 1. Cilt. Istanbul: İletişim Yayınları, 27-39.


Streeck, W. (2015). Epilogue: Comparative-historical Analysis: Past, Present, Future. In Mahoney, J., & Thelen, K., (Eds.), *Advances in Comparative-Historical Analysis* (pp. 264-288). Cambridge: Cambridge University Press.

Yasamee, F. (2011). *Ottoman Diplomacy: Abdülhamid II and the Great Powers, 1878-1888*. Piscataway, New Jersey: Gorgias Press.

Zurcher, E. J. (2010). *The Young Turk Legacy and Nation Building: From the Ottoman Empire to Atatürk’s Turkey*. London: I.B. Tauris.



 Hakan İPEK  
Dokuz Eylül University

 Prof. Dr. Hilmi YÜKSEL  
Dokuz Eylül University



**Received/Geliş Tarihi**  
21 January 2025

**Accepted/Kabul Tarihi**  
24 August 2025

**Publication/Yayın Tarihi**  
31 August 2025

**Corresponding  
Author/Sorumlu Yazar**  
Hakan İPEK  
[ipek.hakan@ogr.deu.edu.tr](mailto:ipek.hakan@ogr.deu.edu.tr)

**DOI:** 10.69494/jirps.1623800

**Cite this article**

İpek, H. and Yüksel, H. (2025).  
The Institutional and Structural  
Transformation of the European  
Union Agency for Cybersecurity  
(ENISA). Journal of International  
Relations and Political Science  
Studies, (14), 28-64.



Content of this journal is  
licensed under a Creative  
Commons Attribution-  
Noncommercial 4.0  
International License.

**Research Article - Araştırma Makalesi**

## THE INSTITUTIONAL AND STRUCTURAL TRANSFORMATION OF THE EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA)

In the European Union (EU) context, the necessity for security within the information society has been a recurring theme for the last two decades, and the European Cybersecurity Agency (ENISA) has become a critical part of the EU's institutional structure. The agency has been assigned specific and important tasks and responsibilities within this framework, positioning it as a crucial element in the EU's cybersecurity ecosystem. As a pan-European network and information security expertise centre, ENISA collaborates with its stakeholders (namely, EU institutions, Member States, the Information and Communication Technology (ICT) sector and businesses) to develop advice, recommendations and standards on good practices in information security. The Agency's tasks include enhancing coordination with EU bodies and Member States in cybersecurity, as well as cooperation with third countries and international organisations to ensure the most secure cyber environment. The present study aims to introduce ENISA as an EU institution that has proven its institutionalisation in cybersecurity worldwide.

**Keywords:** European Union, Cybersecurity, ENISA, ICT, Certification

## **Introduction**

The increase in ICT and the digitalisation that affected the world in the 1990s and 2000s have brought about a remarkable change in all segments of society regarding lifestyles and habits. Our daily lives, fundamental rights, social interactions and economies have become dependent on the sustainable and trouble-free operation of the infrastructures created by these technologies in an integrated manner. An open and free cyberspace (Duic & Petrusevic, 2023, p. 99) fostered worldwide economic and social inclusion, eliminating the obstacles between states, people, and individuals, enabling the influence of each other, and sharing knowledge and thoughts.

With the proliferation of communication networks and information systems as indispensable tools for everyone, the level of concern about the security of these tools and the processes that run on them has also increased. The economic and legal damage caused by Internet-based security breaches worldwide raises the prospect of a gradual decline in confidence in the Internet unless necessary measures are taken, raising concerns that both e-commerce and socio-economic progress will suffer. There is also a perception that any damage caused by an attack on critical infrastructures can hinder the supply of services important for the well-being of the citizens. This study examines ENISA's evolving overall role in harmonising Member States' cybersecurity capabilities and standardising practices and the updates to its organisational structure, tasks, and responsibilities since its establishment in line with emerging needs and circumstances. The study also examines the increasing level of its competencies under the EU Cybersecurity Act, which, in its latest update, aims to certify practices and tools across the EU. It is based on a comprehensive review of the extant academic literature on ENISA's efforts to enhance and improve cybersecurity across the EU, and it demonstrates the need for transformation to increase the impact and capacity of a cybersecurity institution that functions as a coordination and support body in the international arena. This is particularly important given the challenges arising from its limited financial resources and mandate.

This study examines the transformation of a network and information security agency established as a centre of excellence with a crucial advisory role into a cybersecurity agency with a wide range of cybersecurity activities, from cybersecurity policies and standards to operational implications, with updates based on the achievements of the last two decades and emerging needs. It also assesses the identified shortcomings and the effectiveness of the agency's coordination in eliminating existing cyber threats.

## **I. Background on ENISA's Mandate**

Since the beginning of the 2000s, cybersecurity has been at the top of the management of security measures at the global level (Ruohonen et al., 2016, p. 746), and there has been a significant response by individuals, public administrations and businesses to take security measures against increasing insecurity in parallel with ICT developments. The expansion of ICT and the Internet has brought many benefits to individuals and many public and private institutions and actors. Still, it has also brought serious threats to the cyberspace we live in today. While these threats have highlighted important information security policy issues consistent with the vulnerability of ICT, they have also underlined the multidimensional nature of the information-related security problem in all developed countries and the need to involve many actors in the struggle. In this context, the EU has also made specific recommendations through various policy papers prepared by the European Commission. However, Carrapico & Farrand emphasised the need for a broader view of cybersecurity that is more holistic and part of the EU's defence strategy rather than a narrow approach to cybercrime-specific classifications due to the lack of well-functioning intergovernmental cooperation between EU member states for specific security-related bureaucratic tasks and the limited ability of member states to counter multilateral attacks (2024, p. 2).

On 26<sup>th</sup> January 2001, the Commission of the European Communities published a Communication outlining the necessary initiatives for information infrastructures and cybercrime to create a secure information society (Commission of the European Communities, 2000). In this Communication, the EU recognised cyberspace as a necessity for everyday life, upholding fundamental values and human rights and economic development (Dewar, 2017, p. 113) and emphasised the need for effective action to address threats to information systems and networks concerning the problem of cybercrime (Gercke, 2009, p. 411). The document stated that the level of network and information security (NIS) played an important role in a wide range of critical infrastructure activities, including public utilities such as water and electricity supply, and supported the services provided as part of these activities in the form of the ability to counter accidental events or malicious acts that could jeopardise the services provided and the data stored or transmitted on the infrastructures where such activities were carried out (Irion, 2014, p. 94). However, cybercrime was assessed in the same framework as NIS (Didier Bigo et al., 2009, p. 21), and it was warned that information and communication infrastructures offer new opportunities for criminal behaviour due to security vulnerabilities (Cornish, 2009, pp. 24-25).

About five months later, on the 6<sup>th</sup> of June 2001, the Commission of European Communities presented a communication that published a European policy approach through the network and information security (Commission of European Communities, 2001). This emphasised the vital and central importance of cooperation with the private enterprise due to its ownership of information infrastructures and perceived expertise (Carrapico & Farrand, 2020, p. 115), and that security had become a key priority as information and communication had become an essential factor for economic and social development. This provided a statement of intent for a comprehensive framework for institutionalising NIS. It listed the main types of cybercrime and suggested improving security in various aspects (Renda, 2022, p. 475).

Addressing both immediate and long-term challenges in cybersecurity, these strategic initiatives reflect the EU's deep-rooted commitment to fostering a secure, resilient, and reliable digital environment and demonstrate the EU's proactive approach to protecting its digital infrastructure. The following sections of the paper will analyse the impact of these developments on EU cybersecurity policy and provide a comprehensive overview of the steps taken towards a more secure digital Europe.

## **II. Short-term Establishment of ENISA: Responsibility for Network and Information Security**

Following these, the vulnerability of critical infrastructures, where services for fundamental social and individual needs were conducted and provided, had become very apparent for the European continent, as for all developed societies, due to the Twin Towers attacks in the USA. Member States and EU institutions agreed to establish an EU-wide agency to provide guidance and leadership to Member States on network and information security issues (Brun, 2018, 48). On 11<sup>th</sup> of February 2003, the Commission of European Communities presented a draft regulation on the establishment of a body with the important task of developing a common network and information security culture for any individual or legal entity using the ICT component throughout the EU and thus conducting business and transactions related to the common market (Commission of European Communities, 2003). As a result of the studies and evaluations carried out within this framework, Regulation (EC) No 460/2004 of 10<sup>th</sup> of March 2004 (Official Journal of the European Union, 2004, L 077) established the European Network and Information Security Agency (ENISA) with the mission of ensuring a comprehensive and dynamic level of network and information security in the Member States. The Regulation was an indicator of the priority given to the creation of a network and information security culture in the EU, in terms of meeting the network and information security requirements of the European

Commission and the Member States, ensuring working in partnership with the private sector for this purpose, and being the first piece of legislation to show that the business community could not be ignored in technological developments (Mitrakas, 2016, p. 36).

The Regulation's legal basis was Article 95 of the European Community Treaty as an appropriate instrument to prevent the emergence of inequalities that might impede the harmonious working of the single market (Chamon, 2014, p. 389; Voss, 2021, p. 266), and ENISA was recognised as a body established solely to remove certain obstacles to the adoption of cybersecurity measures of a supranational nature in EU Member States (Pauri, 2017, p. 104)[1].

The Agency's Management Board was its decision-making body, comprised of state and Commission of European Communities appointed delegates. The Board included industry, consumer, and academic representatives without voting rights. Other elements included an Executive Director and a Permanent Stakeholders' Group. The Group was to assist the Director in performing his/her duties. The Group also prepared a proposal for the Agency's work programme and liaised with relevant stakeholders (Vercher-Moll, 2014, pp. 205-206; Voss, 2021, p. 270).

Originally, non-EU countries that had to agree to adopt the *acquis communautaire* in the areas covered by the legislation were able to participate in the Agency through operational arrangements (Paladini & Castellucci, 2019, p. 84). ENISA's ICT-related security incident response capabilities were natural element in building a comprehensive EU capability to address security threats and incidents, as the organisation was equipped with a strong mandate on Computer Emergency Response Teams (CERTs)[2] to improve the capacity of the EU, participant stated and consequently the business community to combat and respond to network and information security issues.

[1] The United Kingdom applied for annulment, arguing that the Regulation should have been adopted based on Article 308 of the European Commission Treaty, which covers measures necessary to achieve Community objectives not provided for in the founding Treaties. Having assessed the UK's arguments, the Court of Justice concluded that the legal basis of the Regulation establishing ENISA was correct and that reliance on Article 95 was appropriate (Court of Justice of the European Union, 2005).

[2] Computer Emergency Response Teams (CERTs), also referred to as Computer Security Incident Response Teams (CSIRTs), can be defined as the primary response units of the national authorities responsible for addressing all forms of cybersecurity incidents. These units are tasked with the detection of security vulnerabilities, the investigation of cyber threats, the formulation of response plans, the dissemination of information to users, and the implementation of measures to address these issues. CERT-EU was established in 2011 to carry out these activities within the EU in 2013.



It was emphasised that a Europe-wide multi-stakeholder management framework should be built on national initiatives and ENISA's operational activities, with an action plan prepared in the context of addressing the most pressing challenges to be addressed by the critical infrastructure protection sector to ensure that these teams acted as a core constituent of national capabilities by Glorioso & Servida (2012, p. 47). ENISA pioneered the concretisation of the European Public-Private Partnership for Resilience (EP3R) as a crucial step in this context (Irion, 2014, p. 86).

On 31<sup>st</sup> of May 2006, the Commission of European Communities published a communication entitled Strategy for a Secure Information Society (Commission of European Communities, 2006), which identifies the current challenges in building a secure information society and discusses the actions to be developed to address these challenges based on dialogue, partnership, and empowerment with all relevant stakeholders. Issued immediately after the failed Constitutional Treaty, the strategy moved away from strict regulation and prescriptive measures (Dewar, 2017, p. 115) while focusing on the network and information security objectives set in 2001. The strategy reflected attempts to restrain what was then seen as the creation of a European superstate by seeking to create an approach that facilitated and encouraged voluntary action and cooperation (Bache et al., 2011, p. 212). The document, which identified the challenges through a three-pronged approach in the areas of (i) network and information security measures, (ii) privacy and data protection in electronic communications, and (iii) combating cybercrime, confirmed that ENISA was established with the mission to contribute to improving network and information security in the EU and to foster the coming into being of a network and information security for the benefit of all stakeholders across the EU. According to the Strategy, multi-stakeholder dialogue, including the private and public sectors, could facilitate better implementation of the network and information security. In this respect, partnerships between Member States and other parties are considered essential to contribute to the fight against computer-related crime, while awareness raising through a range of activities for the benefit of society and institutions, in particular education, is seen to improve the security culture (Renda, 2022, p. 476). ENISA has been invited to establish trusted partnerships with EU Member States and relevant stakeholders to explore the feasibility of establishing a pan-European system to facilitate the exchange of information on cybersecurity threats. This initiative was proposed to improve the efficiency of data collection and management of cyber threats. At the same time, Member States have been encouraged, in cooperation with ENISA, to implement awareness-raising initiatives promoting the benefits associated with the adoption of high-impact security technologies.

In May 2010, the European Commission, anticipating that the cost of cybercrime, which costs the EU €750 billion, would increase by the day (Chatterjee and Lefcovitch, 2016, p. 6), published what it called the European Digital Agenda (European Commission, 2010) to lead the way in maximising the sustainable socio-economic benefits of a Digital Single Market (DSM) based on faster internet and integrated applications. Proposals to modernise ENISA and establish a Computer Emergency Response Team (CERT-EU) for cyber incidents against EU bodies were listed among the agenda's priorities (Bisogni et al., 2011, p. 115). In November of the same year, under the coordination of ENISA and with the assistance of the EU Joint Research Centre (JRC)[3], and with the active or observer participation of all EU Member States and the European Free Trade Area (EFTA) States, the first pan-European cybersecurity exercise on the critical information infrastructures' protection, called Cyber Europe 2010, was organised to test the response of the authorised bodies of the Member States to simulated attempts by hackers to disrupt critical Internet services in different EU Member States, following several complex scenarios ranging from the European to the global level. Cyber Europe 2010 was a demonstration of support for strengthening Europe's defences against cyber-attacks as part of the European Commission-led support for Europe-wide cybersecurity preparedness exercises. The exercise, the responsibility for which was entrusted to ENISA from the outset and welcomed by the EU Member States, was perceived as a positive tool to strengthen the contingency planning and abilities of the Member States in cybersecurity (Christou, 2016, p. 127). In this context, the draft proposal (European Commission, 2010) to extend its competencies and mandate, published for consultation about a month before the exercise, has highlighted the need to adapt its mandate to respond more effectively to European needs. Indeed, the EU and the US have organised various cyber exercises to strengthen cooperation and solidarity in cybersecurity. In this context, the first transatlantic joint cybersecurity exercise, Cyber Atlantic 2011, was held in Brussels on 3<sup>rd</sup> November 2011 with the support of ENISA. The exercise built on the experience and inspiration gained during Cyber Europe 2010, the first European cybersecurity exercise organised by ENISA the previous year.

[3] The Joint Research Centre (JRC), a constituent element of the European Commission, operates in close collaboration with research organisations across all Member States, universities, European institutions, and scientific research units on the global stage. The primary objective of the Centre is to furnish EU policymakers with informed insights derived from rigorous scientific research, thereby ensuring the formulation of policies that are aligned with the best interests of society. The Centre occupies a pivotal role during the pivotal phases of the EU policy cycle. (<https://joint-research-centre.ec.europa.eu/>).



ENISA's role was to support EU Member States in organising cybersecurity exercises and developing national contingency plans through good practice examples and training sessions (Renard, 2018, pp. 9-10)[4]. However, although the need for a comprehensive reform of ENISA's mandate was already on the agenda, ENISA's mandate was only extended for three years in 2008 and three and a half years in 2011 without any change to its mandate (Voss, 2021, p. 268).

### **III. ENISA's First Structural Upgrade**

The first EU Cybersecurity Strategy, published on the 7<sup>th</sup> of February 2013 (European Commission, 2013a), which aimed to promote a trustworthy, secure, and open cyber ecosystem across the EU, was the cornerstone of the EU's cybersecurity policy and was based on the premise that the EU's core values, which also set out the fundamental principles of cybersecurity, should also apply to the information society (Popescu, 2017, p. 105). It brought together the various nuclei of the comprehensive acquis on cybersecurity, which had previously been formed by expanding on the same plane, albeit in different lanes. It pointed out that the relations between individuals in the administration's physical and virtual environments should be within the scope of the same principles and values (Dewar, 2017, p. 127). The document published together with the proposal (European Commission, 2013b) for a Network and Information Security Directive (NIS Directive), prepared by the European Commission to strengthen and secure the network and information systems in the EU, emphasised the need to modernise and strengthen ENISA to achieve cyber resilience, one of the strategic priorities to address the challenges faced by the EU due to the increasing threat environment in cyberspace (Ruohonen et al., 2016, pp. 746-756). It was stated that negotiations on a separate draft regulation for the update are underway. The strategy paper defined European cybersecurity policy along three structural axes: building cyber defences, fighting cybercrime, and improving network and information security, and assessed that EU cybersecurity governance is limited to Member States but supports capacity building, facilitates coherence, coordination, and access between Member States, and promoted decentralised organisation (Ramunno, 2014, p. 1).

[4] Numerous scenario-based tabletop exercises have been conducted to enhance coordinated cooperation between the EU and the US, the latest of which was the 9<sup>th</sup> EU-US Cyber Dialogue held in Brussels on 6-7 December 2023. The Dialogue brought together the G7 and G20, as well as international and regional organisations such as the UN, OSCE and ASEAN Forum. It exchanged views on international cyber policy discussions and cooperation. ENISA and its transatlantic partner, the US Infrastructure Security Agency (CISA), exchanged information on cyber awareness and training, sharing of best practices and joint situational awareness (EEAS Press Team, 2023). ENISA's partnerships with similar organisations in the international arena show that the Agency is recognised within the same framework.

In the context of all these developments, Regulation (EU) No 526/2013 of 21<sup>st</sup> of May 2013 (Official Journal of the European Union, 2013) abolished the Agency established under Regulation (EC) No 460/2004 and re-established ENISA under the corporate name EU Agency for Network and Information Security (ENISA) with new powers and a mandate until 2020. With an extensive archive of information on its mandate since its establishment (Szádeczky, 2020, p. 86), the updated statute strengthened ENISA's ability to combat cyber-attacks and other information security threats and added comprehensive tasks and responsibilities for the protection of critical infrastructures to ENISA's more detailed mandate (Kafitz & Burgers, 2013, p. 209).

The revised regulation did not change the organisational structure of ENISA. Still, it was decided that the Management Board would also establish an Executive Board to contribute to improving the efficiency and effectiveness of ENISA's functioning and that the Executive Board would meet at least quarterly, like the members of the Management Board. It was decided that the Agency would continue to be led by an Executive Director, whose independence and duties would remain unchanged and who would be asked to support the Management Board and the Executive Committee with staff and other resources as needed (Szádeczky, 2018, p. 291). However, as stakeholders were sufficiently represented and it was agreed to consult the representative group on some issues, it was considered that stakeholder representation on the Steering Board was no longer necessary and that this would avoid some (mainly political) accountability of non-EU stakeholders and at the same time reduce executive control (Voss, 2021, p. 271).

ENISA was granted increased influence in shaping EU cybersecurity policies and strategies upon the Regulation's entry into force. The Agency's tasks have been further elaborated to improve Member States' cybersecurity capacities and to assist Member States and EU institutions by carrying out preparatory studies and analyses on all relevant issues for the achievement of upper tiers of network and information security in the EU in general, including the development and updating of policies and legislation; to organise training activities and provide advice; to analyse and publish publicly available network and information security strategies; and to promote the evolution and exchange of best applications. Thus, ENISA began to take its first steps towards transforming itself from an administrative body into a quasi-regulatory body, in addition to its role in information and coordination (Craig, 2012, 152-153; Voss, 2021, 251).

As part of the tasks defined in the previous Regulation, in addition to the development of high-level network and information security capabilities through

CERTs, ENISA was to encourage collaboration with third countries and entities at the international level through the organisation of various exercises and the establishment of an EU early warning system to be integrated into the competent authorities of the Member States, thereby furthering the Commission's commitment to dialogue and information exchange. In addition, ENISA's supporting role became more important in analysing and reporting on the results of international exercises, advising Member States at their request in the event of a security breach or loss of integrity with a significant impact on the functioning of services and national exercises, voluntary cooperation and awareness raising among stakeholders, cooperation against cybercrime with an increased budget, and working with supranational structures to make the EU market sustainable (Attström, 2017, p. 10; Pauri, 2017, p. 104).

#### **IV. Strengthening ENISA Through the NIS Directive**

ENISA's role has been significantly expanded in cooperation support, coordination of national CSIRTs, establishing cybersecurity strategies, and standardisation. ENISA's role significantly expanded in cooperation support, coordination of national CSIRTs, formulation of cybersecurity strategies and standardisation. This was made mandatory by Directive (EU) No 1148/2016 (Official Journal of the European Union, 2016), which established measures to ensure the standard and sustainable security of communication networks, critical infrastructure, and information systems across the EU (Kamara, 2020, p. 26). It was decided that ENISA would be represented in the Co-operation Group established to maximise co-operation and exchange of information between EU Member States in the field of cybersecurity under the NIS Directive, which meant that Member States can benefit from ENISA's assistance under the Regulation whenever they wish. In addition, ENISA was entrusted with the secretariat of the CSIRTs Network, which was given an active role in responding to cybersecurity incidents at the technical level between Member States, and ENISA was empowered to actively support cooperation between CSIRTs, which was an important opportunity for the institutionalisation of the Agency (Holzleitner & Reichl, 2021, p. 17). The NIS Directive required Member States to promote the use of European or internationally recognised standards and specifications relating to network and information security, rather than being limited in the field of technology and specified that ENISA, in cooperation with Member States, should develop recommendations and guidelines on the technical areas required as well as on existing standards to ensure that these areas were covered. (Calliess and Baumgarten, 2020, p. 1167). In addition, to facilitate the seamless progression of national cybersecurity strategies, ENISA has formulated a four-stage proposal, delineating the procedural steps essential for ensuring the effective implementation of cybersecurity measures. This process, consisting of prevention, preparedness, response and recovery phases, includes recommended best practices for effectively managing cybersecurity crises (ENISA, 2024c).

In 2016, the European Commission published a Communication on the completion of the evaluation of ENISA by the end of 2017, detailing ENISA's mandate as well as measures to strengthen the European system for cyber resilience and to promote a sustainable, innovative and efficient cybersecurity industry in Europe (European Commission, 2016). The importance of cooperation between stakeholders, information sharing, additional measures to strengthen EU resilience, and the need to review Regulation 526/2013 became even clearer considering ENISA's public assessments, given the possibility of a Europe-wide cybersecurity crisis. However, there were also legitimate criticisms that ENISA's limited mandate, even if extended, significantly weakens its competence, hampers long-term planning, adversely affects the situation of the organisations to which its services were directed, and contradicted the NIS Directive, which gave ENISA specific tasks (Radoniewicz, 2022, p. 91). Furthermore, the EU Council adopted the Cyber Diplomacy Toolbox[5] in June 2017, confirming that ENISA is at the centre of the EU's cybersecurity policy as one of the key actors to strengthen the EU's capabilities in this area and to develop a coordinated defence against cyber threats to Europe from the international arena, in close cooperation with its allies (Vlajic, 2023, p. 202). Regulation (EU) No 526/2013 defined a cybersecurity certification scheme that includes rules, standards, and procedures to assess a product's or service's cybersecurity features. It covers various categories and specifies requirements, assessment types, and assurance levels (Kohler, 2020, p. 8).

Introduced as a landmark initiative to strengthen a harmonised cybersecurity posture across EU Member States, the NIS Directive (EU) No 2016/1148 aimed to establish a common level of network and information security and was the first pan-EU legislation (Singh, 2023, p. 257) that focused primarily on enhancing the cyber resilience of essential or digital service operators and providers, recognising the interconnectedness of critical infrastructure in the digital age. This legislation was a major step in identifying the challenges and ensuring a coordinated and coherent response to the growing threat of cyber incidents in EU Member States and laid the foundations for a collaborative approach to cybersecurity within the EU by encouraging risk management practices and requiring incident reporting.

[5] The Cyber Diplomacy Toolbox, a common framework adopted in 2017, was developed to enhance the EU's capacity to impede, deter, and react to malevolent cyber activities by employing diplomatic measures, including implementing sanctions. This strategic instrument is designed to advance a rules-based international order in cyberspace by facilitating collaboration and accountability between EU Member States and international partners.

In 2017, the new cybersecurity strategy document 'Resilience, Deterrence, and Defence in Cybersecurity' (European Commission, 2017a), published as a more elaborated version of the 2013 strategy, highlighted the need for a more comprehensive European response to cyber threats and provided an important framework for the need to strengthen cybersecurity across the EU, including the institutionalisation of ENISA and the progress of policies and practices in cybersecurity. By providing a reference point for ENISA to develop cybersecurity standards and identify best practices, the strategy document contributed to the harmonisation of standards in the field of network and information security. It underlined ENISA's role in providing the necessary support and guidance to ensure cyber-attack resilience, including developing preparedness and response plans for cyber-emergencies (Kasper, 2020, p. 172). In this context, the European Commission also presented a new draft regulation to complement the strategy paper, which aimed to give ENISA an unlimited mandate and a more active role in reducing cybersecurity risks both within the EU and globally, providing support to cybersecurity stakeholders in all key areas, including the general framework of the NIS Directive and the cybersecurity certification (European Commission, 2017b). It was underlined that ENISA would raise the bar by continuing to organise annual pan-European cybersecurity exercises integrating different levels of response, improve Europe's preparedness for cyber-attacks, support the development of an EU policy on cybersecurity certification for ICT tools in support of the digital single market and that cybersecurity measures will play an important role across the EU (Carrapico & Barrinha, 2018, p. 300; Markopoulou et al., 2019, p. 8).

## **V. ENISA as European Cybersecurity Agency and Certification Authority**

Approximately one and a half years after the publication of the draft, the EU adopted the Cybersecurity Act on 17 April 2019, marking a significant milestone in the EU's cybersecurity framework. The objective of the Act was to establish a standardised and certified framework to enhance cybersecurity within the European Union. This legislative act encompasses a wide range of ICT tools applicable within the EU, aligning with the overarching objectives of the Digital Single Market (Enescu, 2020, p. 279). The primary objective of this legislative act is to further enhance cybersecurity efforts across the EU (Official Journal of the European Union, 2019). Throughout its 15-year history, ENISA has undergone continuous renewal to evolve into a centralised model with permanent duties and responsibilities, now renamed the Cybersecurity Agency. It has become a leading authority for the EU, guiding all Member States on cybersecurity matters. Consequently, in addition to the increased duties, powers and responsibilities compared to previous versions, it has become institutionalised and has become an indispensable centre for cybersecurity standards and authorisations.

No changes have been made to the Agency's budget and organisational structure (Vlajic et al., 2023, p. 202; Voss, 2021, pp. 269-275), but an ENISA Advisory Group has been set up to bring stakeholder issues to ENISA's attention, and a network of National Liaison Officers (NLOs) has been established, with representatives from all Member States, to facilitate the exchange of information between ENISA and the Member States and to help publicise ENISA's work (Seatzu & Santarelli, 2024, p. 18; Voss, 2021, pp. 276-277). It was also agreed to establish a Stakeholder Cybersecurity Certification Group, consisting of members selected from among experts representing relevant stakeholders, which is envisaged to advise ENISA and the European Commission upon request on issues related to the ICT sector, cybersecurity certification and standardisation and to play a role in the process of determining certification schemes (Polčák, 2022, p. 215).

### **A. A new cybersecurity certification framework for Europe**

Under the Act, which sets out key tasks such as improving the EU's cybersecurity capabilities, providing technical assistance to Member States, and developing policy recommendations on cybersecurity, a European Cybersecurity Certification Framework, organised by ENISA, has been established to prevent potential disruptions to the internal market, and ensure user confidence by enhancing the security of the digital market. The framework provides a standardised methodology for the security levels of digital tools across the EU. It eliminates the financial and bureaucratic difficulties of obtaining separate certificates (authorisation to use) from each EU country, bringing benefits to all businesses using ICT to drive digital transformation, especially new initiatives (Radoniewicz, 2022, p. 91).

ENISA has been responsible for setting the standards for the certification required to protect the DSM across the EU, and for the accreditation of Member States' competent national authorities, creating an area where security concerns are assessed indirectly, directly and supranationally. (Paladini & Ignazio Castellucci, 2019, p. 84). Stakeholders such as the European Cybersecurity Certification Group (ECCG)[6] have also been structured to work with ENISA in a framework arising from the desire to regulate and support public authorities in cybersecurity through certification (Blaese, 2019, p. 2). The ECCG will be responsible for advising, assisting and cooperating with the Commission and ENISA on the ongoing work plan of the EU, policy issues related to cybersecurity certification, coordination of policy approaches, maintenance and review of existing cybersecurity certification and the preparation of new cybersecurity certification schemes (Gajewski, 2020, p. 114).

[6] European CommissionCG, consisting of representatives of national cybersecurity certification authorities or other relevant national authorities, has been established to ensure consistent implementation and enforcement of the Cybersecurity Act.



The subject of ENISA's working model is any threat and any person or object that causes, carries, transmits or supports (or has the power to act) this threat, taking into account the fact that communication networks and information systems can be compromised by accidents, attacks or errors, which can lead to significant financial losses (Craig, 2011, p. 106; Popescu, 2017, p. 106). Some of the main threat elements in cyberspace are companies, cybercriminals, employees, hacktivists, nation states and terrorists (Lehto, 2015, p. 9). The Regulation characterises cybersecurity as a collection of actions aimed at safeguarding ICT tools, along with their users and others impacted by cyber threats and cyber threats as any possible circumstances, events, or actions that may harm, incapacitate, or otherwise negatively influence tools and the individuals (Kasper, 2020, p. 169). In the extreme synthesis, with the statute significantly increasing ENISA's mandate, powers, and resources (Lonardo, 2021, p. 1086), It is envisaged that ENISA's role will go beyond providing technical advice and that ENISA will raise awareness of cybersecurity at the highest level, including digital hygiene and literacy, to be promoted among citizens, organisations and businesses (Negreiro, 2019, p. 9).

Providing strategic advice and policy support to EU institutions and Member States in the development of cybersecurity policies, coordinating collaborative work between Member States in times of major crisis, including the organisation of large-scale EU-wide cybersecurity exercises to enhance the EU's ability to respond rapidly to cybersecurity incidents, and contributing to the training of cybersecurity experts and the next generation of security professionals by organising various events and training programs to raise awareness of cybersecurity across the EU (Voss, 2021, p. 270).

The Cybersecurity Act sets out the standards for cybersecurity-related competencies that will apply across Europe, the levels of assurance that the European Cybersecurity Certification Scheme can provide on declarations of compliance with these standards and that declarations of compliance may initially be voluntary and later mandatory (Brass & Sowell, 2021, p. 1101; Nwankwo et al., 2022, p. 965). According to European legislation, the certification process provides three levels of assurance for ICT products, services, and processes. The 'basic' level fulfils security requirements for products used in low-risk contexts, the 'important' level includes more comprehensive security requirements for medium-risk situations, and the 'high' level fulfils the highest security requirements for critical infrastructure and high-risk contexts. When evaluating these processes, it is important to consider each level's relevant legislation and specific requirements (Fowler et al., 2022, p. 6; Khurshid et al., 2022, p. 129942). The standardisation process is theorised to occur in three distinct phases: programme development, certification and review and renewal (Purser, 2014, p. 98).



The regulation establishing the cybersecurity certification organs of the Member States creates a European cybersecurity certification system at the EU level in the form of a comprehensive set of regulations applicable to the certification or assessment of conformance of specific ICT services, products, or processes. (Verhelst & Wouters, 2020, p. 162). Thus, a European Cybersecurity Certificate has been established, proving that a relevant organisation has assessed specific ICT services, products, or processes for compatibility with specified security requirements in a European Cybersecurity Certification Plan (Mitrakas, 2018, p. 411).

ENISA is responsible for implementing legal provisions on cybersecurity at the EU level and developing cross-border communities to enhance the resilience of critical information infrastructures in the EU (Moise, 2023, p. 276). Furthermore, ENISA prepares candidate schemes adopted by the European Commission and certifies that products, services and processes assessed by such cybersecurity certification schemes comply with specified security requirements (Kohler, 2020, p. 8). Moreover, the Agency is expected to ensure that the cybersecurity certification framework, which has emerged as a key tool for enhancing the security of innovative technologies such as the Internet of Things (IoT) devices, artificial intelligence and cloud computing, increases trust in digital services, enables the adoption of innovative technologies in the EU's DSM and enables the EU to play a leading role in setting cybersecurity standards at the global level (Moise, 2023, p. 276).

## **VI. Further ENISA Tasks with The New Decade: NIS 2 Directive, The Cyber Resilience Act, The Cyber Solidarity Act**

In 2020, the digital transformation of societies, because of the actions undertaken by public officials in response to the COVID-19 crisis that affected the whole world, extended the diversity of threats to cyberspace, presenting new challenges that require innovative responses. As a result of greater dependence on the internet, the number of cyber-attacks has increased, becoming more sophisticated and originating from a wide variety of sources, inside and outside the Union. Accordingly, the EU's Cybersecurity Strategy for the Digital Decade (European Commission, 2020) was published in December of the same year to lead efforts for secure digitalisation, to establish norms for world-class solutions and cybersecurity standards for essential services and critical infrastructures, and to more effectively guide the development and implementation of new technologies and share responsibility for the provision of a secure digitalisation. The document explains how the EU can use and strengthen its tools and resources to achieve technological dominance and discusses the need to increase cooperation with partners worldwide who share the EU's founding core values.

The strategy document begins by describing the threats that can arise in cyberspace. It states that the classic conflicts that arise in real life can now be transferred to cyberspace, increasing the distance between states worldwide and threatening the ease of free use of the Internet, where indispensable opportunities for humanity are gathered. While all kinds of daily life services can be provided via the Internet, it is pointed out that European values, particularly democracy, are gradually weakening. It is stated that in today's highly insecure cyberspace, it is essential to improve cybersecurity efforts, practices and services to protect fundamental rights and freedoms, including the evaluation of cybersecurity practices in a broader framework, from critical infrastructure to privacy and the involvement of all segments of society in these processes (Renda, 2022, p. 486). Recognising ENISA as a key body for establishing common cybersecurity in the EU as new technologies are deployed, the strategy document emphasised the importance of cybersecurity for economic relations and social activities to be conducted over an open and secure internet from 2020 onwards (Dragomir, 2021, p. 39). In line with previous strategies, it included concrete proposals to ensure a safe and secure open internet for everyone living in Europe through robust and consistent security measures that prevent threats to fundamental rights. It also promoted the EU's commitment to new technologies and industrial policy, calling for significant investments in the digitalisation process from 2027 onwards. It can be said that the European Commission's multi-year strategic objectives with the new regulation are to increase the cyber resilience of the EU as a whole, to harmonise the EU's internal market with the relevant rules for the use of ICT products and services, to make the presence of EU ICT companies felt in the global arena, and to harmonise Member States' cybersecurity legislation.

A comprehensive and adaptable cybersecurity framework is imperative, considering the perpetual evolution of cyber threats. To this end, a unified cybersecurity regulatory body has been proposed to undertake more comprehensive measures to enhance the scope of cybersecurity within the EU. Recent developments in the international arena have served to exacerbate this necessity further. A case in point is the breach of the Orion network management system, a product of SolarWinds, a US-based management and monitoring software provider, which occurred in December 2020. The attackers implanted malware in the service that provides update software for the product, thereby infiltrating the networks of Orion users who had installed a new product update. The subsequent investigation revealed that the attackers, possibly from Russia, used social engineering to gain access to the SolarWinds network by exploiting a zero-day vulnerability in a third-party application or device and collecting information over an extended period.

In response to the attack, which affected over 18,000 organisations worldwide, CERT-EU confirmed that 14 EU organisations were using SolarWinds Orion software. ENISA expressed solidarity with the United States and broadly framed the idea that the military alliance also applies in cyberspace (ENISA, 2021).

Within the scope of the studies carried out within the framework of all these developments, it was envisaged that EU Member States would strengthen their cybersecurity capacities by establishing relevant units and harmonise the rules on cooperation, information sharing, auditing and sanctions, as well as new measures and reporting requirements on cybersecurity risk management covering all sectors. In this framework, after protracted discussions, Directive (EU) 2022/2555 (NIS 2 Directive) entered into force on 16 January 2023. This new regulation extends the scope of the NIS Directive, strengthens existing measures, and introduces several new organisations to protect essential services and critical sectors from cyber threats within the critical infrastructure framework. The NIS 2 Directive, one of the flagships of the EU's network and information security policy, also imposes some important new tasks on ENISA, ranging from the maintenance of several critical cybersecurity-related registers at the EU and EU level to the secretariat of the European Cyber Crisis Liaison Organisation Network (CyCLONE) was founded by the Directive. ENISA supports the transposition of the NIS 2 Directive into Member States' national legislation, provides technical expertise to the different work streams of the NIS Cooperation Group, provides secretariat services to the network of CSIRTs, organises CyberEurope exercises and identifies best practices in Member States' implementation of the Directive. It also supports EU-wide reporting processes on cybersecurity incidents, seeks agreement on common approaches and procedures, and helps Member States to address common cybersecurity challenges. This plays an important role in the effective implementation of the NIS Directive. In addition, the European Cybersecurity Certification Framework is also integrated into the NIS 2 Directive. It will be considered when Member States decide on the circumstances in which they can require certified products, processes, and services (Vandezande, 2024, p. 105890). On 31 January 2024, the European Commission launched a voluntary European Common Criteria (EUC) cybersecurity certification scheme, led by ENISA, providing for the first time EU-wide cybersecurity certification at significant or high assurance levels for many hardware and software products, including components in the form of chips and smart cards (Chiara, 2024, pp. 96-97). This includes standards and requirements for mutual recognition agreements with non-EU member countries, primarily focused on evaluating EUC certificates, as well as detailed rules for national cybersecurity certification programs under the EUC framework (<https://eur-lex.europa.eu/>, 2024).

At the same time, two additional ENISA cybersecurity certification schemes have been implemented under the European Cloud Certification Scheme (EUCCS) and the European Cybersecurity Certification Scheme for 5G networks (EU5G) (D'Alterio, 2024, p. 2). The European Cybersecurity Certification, which is broadly equivalent to the conformity assessment requirements for ICT products, has been assessed as eliminating potential fragmentation, raising security awareness across the board, and increasing stakeholder confidence through a collaborative framework to build a competitive and resilient EU DSM both between Member States and internationally (Chiara, 2024, p. 97; Kalogeraki & Polemi, 2024, p. 100).

Concerns have been raised that certification processes for cloud services do not consider sector-specificities, that existing rules may burden businesses and limit economic benefits, and that some rules may negatively affect the growth potential of Europe's technology sector, e.g. proposals on geographic data localisation may limit the international sharing of data and cyber threat intelligence. (Swire, et al., 2024, 14-16). With the view that the Regulation promises standardisation efforts, albeit mainly within the limits of the EU's market-oriented competencies (Kasper, 2020, p. 173 ), a more harmonised and centralised European certification system should be adopted instead of national certification mechanisms, and political disputes should be resolved. Technical standards should be implemented quickly, more flexible regulations should be developed to reduce the burden on SMEs (Hoong & Rezania, 2024), and the EU's cybersecurity framework should be designed to aim for global leadership, not just standards within Europe (Gao & Chen, 2022, pp. 690-691). In this context, the EU Council called for greater transparency regarding the EU cybersecurity certification schemes developed by ENISA (Morgan, 2024).

In recent years, "cyber resilience," which has emerged as a complement to the more traditional "cybersecurity" discourse and is even poised to replace it, is believed by some policymakers to be the primary goal of information systems development. Although it is referenced numerous times in many policy documents, including the European Commission's first cybersecurity policy strategy from 2013, cyber resilience has not been fully defined. The General Data Protection Regulation (GDPR), which effectively treats resilience as a feature of security, and the NIS 2 Directive, which defines "the security of network and information systems" in terms of resilience, have failed to provide a consistent explanation of the concept (Bygrave, May 2022, 31-32). Cyber resilience refers to an organisation's ability to prepare for cyber-attacks and recover from them. The EU aims to support this concept with the Cyber Resilience Act (CRA), which seeks to ensure that products comply with cybersecurity standards (Kamara, 2025, 1442). This act, the regulation (EU) No 2024/2847, adopted on 23<sup>rd</sup> of October 2024, covers the cybersecurity obligations of companies manufacturing such products, including rules for the placing on the market of products containing digital

elements, procedures for cybersecurity practices related to vulnerabilities that arise during the use of products, and rules for market surveillance (Official Journal of the European Union, 2024). The Cyber Resilience Act requires manufacturers and retailers to ensure the cybersecurity of their products throughout their life cycle by raising cybersecurity standards for products containing digital components. So it will be ensured that any security breach of a product containing digital elements and any cyber threat that could affect the risk profile of a product containing digital elements will be reported to ENISA through the CSIRT network, creates a reporting platform within ENISA to receive these notifications. Under the act, ENISA has a reporting obligation to the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) established under NIS 2 Directive in cases where the reported information relates to the coordinated management of large-scale cybersecurity incidents and crises at the operational level[7]. In addition, the European Commission, supported by the European Cybersecurity Competence Centre and ENISA, will also undertake initiatives to develop institutional and technological tools to provide enough qualified professionals to enhance cybersecurity skills and support the activities of market surveillance authorities and conformity assessment bodies as stated in the Cyber Resilience Act (Carrapico, & Farrand, 2024, 6).

In addition, on 19 December 2024, the Cyber Solidarity Act (EU) 2025/38 was adopted. It contains various measures to strengthen the EU's resilience to cyber threats and its capacities to prepare for, respond to and recover from cyber incidents. In particular, the Act emphasises the need to strengthen the cybersecurity framework, considering the frequency and impact of cyber-attacks (Official Journal of the European Union, 2025)[8]. The Act establishes a European Cybersecurity Alert System to coordinate the detection, analysis, and response to cyber threats (Villani, 2025, p. 489). Member States must also designate a National Cyber Centre if they join the system. Concurrently, the Cybersecurity Emergency Mechanism was established under the oversight of the ENISA to ensure preparedness for the impact of significant and large-scale cybersecurity incidents. It has also been agreed that the European Cybersecurity Incident Review Mechanism, with the ENISA at its core, will examine and assess cyber threats, known exploitable vulnerabilities, and mitigation actions and prepare investigation reports about specific significant cybersecurity or large-scale cybersecurity incidents.

[7] Regulation entered into force on 10<sup>th</sup> December 2024, and the main obligations introduced will take effect on 11th December 2027.

[8] The effective date of the regulation in question was determined as 04/02/2025.

This will be undertaken after the conclusion of the investigation and assessment of an incident, in collaboration with all pertinent stakeholders, to derive lessons learnt to prevent or mitigate future incidents. (European Commission, 2025).

## Conclusion

ENISA publishes a series of reports on cyber incidents and cyber threats across the EU to inform cybersecurity policy and practice. In this respect, the ENISA 2030 Foresight Threats Report, published on the occasion of the 20th anniversary of the establishment of the European Union Cybersecurity Agency (ENISA), aims to harmonise cybersecurity practices across the EU and sets out the potential threats and challenges to be faced in the coming years. Factors contributing to these threats in Table 1 include the increasing complexity of IT environments, supply chain vulnerabilities, advanced threat actors and new vulnerabilities introduced by technologies such as AI, IoT and 5G. The report emphasises the importance of user education and awareness initiatives and the need for robust incident response strategies and resilience planning in response to increased attacks (Mattioli et al., 2023). Also, the ENISA Threat Landscape 2024 report observes a significant number of cyber incidents targeting organisations in the public administration, transport and financial sectors in the period from July 2023 to July 2024. The report identifies seven main cyber threats that have threatened Europe in the last year: ransomware, malware, social engineering, threats to data, threats to availability, information manipulation and interception, and supply chain attacks. The report focuses on developing preventive strategies against these threats and analyses the cybersecurity situation in EU Member States. Financially motivated attacks by threat actors are at the top, with cybersecurity training and awareness programs recommended (ENISA, 2024b). The financial sector was the most targeted and suffered the highest losses. The EU aims to improve coordination and cooperation between Member States and relevant institutions by strengthening institutional structures and legal frameworks to deal with cyber threats more effectively (Pawlak, 2018, p. 103).

Considering the findings on cyber threats, the primary objective of ENISA, as delineated in its founding statute, is to promote cybersecurity awareness throughout Europe and develop cybersecurity measures within all sectors. This mission has been reiterated in subsequent updated statutes. It has been contended that ENISA, as a nascent cybersecurity governance instrument whose primary task is to guide EU bodies and pertinent national institutions and which mirrors the EU's transition to creative governance strategies (Seatzu & Santarelli, 2024, p. 3), possesses greater autonomy in its operations (Robinson, 2012, p. 164),



in contrast to the European Commission or the Council. In contrast to conventional methodologies employed in addressing cybersecurity concerns, ENISA has been a potential candidate for becoming one of the EU's indispensable institutions as a policy-making instrument designed to fortify Europe's digital security infrastructure. It has exhibited a distinct perspective characterised by governance that differentiates it from extant EU institutions. However, it has become evident that ENISA lacks the authority to develop and/or deploy autonomous cybersecurity capabilities, nor is it intended to make strategic decisions. Instead, the expertise of cybersecurity (technical) experts working within or for the Agency should be utilised. The discourse surrounding ENISA has focused predominantly on the supranational powers it will assume in place of national institutions, as opposed to the nature of the security it is expected to provide or the policy instruments it will employ. (Cavelty and Max Smeets, 2023, pp. 1336-1338).

The EU Cybersecurity Act does not direct any responsibility of Member States regarding security and law, but expects that cybersecurity should be a strategic issue for the EU as a key topic and that the Regulation should be considered both in shaping legislation and in setting standards and establishing and maintaining a certification framework for various goods and services. It underscores the significance of ENISA's expertise, thereby ensuring its ongoing contribution to developing and implementing EU policy and legislation in the cybersecurity domain. This contribution is manifested through a range of activities, including the provision of expertise, advice, and analysis. The problems ENISA has had to overcome during its institutional development regarding its cybersecurity expertise have also raised important implications for power, authority, and legitimacy. The question of who has, who does not have, and who should have expertise in cybersecurity has become an important issue for democratic politics (Cavelty & Smeets, 2023, p. 1357).

As an important milestone in strengthening the EU policy on cybersecurity, the EU Cybersecurity Act sets out the basic requirements for developing cybersecurity standards and certification. It provides for the harmonisation of cybersecurity certifications and the use of EU Declarations of Conformity in all Member States, further modifies ENISA's competencies, establishes a cybersecurity certification framework and makes an undeniable contribution to strengthening the EU's digital security infrastructure and ensuring security in the digital market. This framework recognises that internationally recognised organisations from different digital service sectors can provide input on the specific requirements and needs for secure ICT tools as well as good practices, and that certification can be used for all sectors facing cybersecurity challenges (Vavousis et al., 2020, pp. 233-234).



This framework, which is of great importance in the certification of ICT product security, has played an important role in increasing trust and security in cyberspace and has ensured the implementation of specific and risk-based EU certification programs. Considering the different certification programs for cybersecurity products in the EU, without a common cybersecurity certification framework within the EU, there is a risk of increasing negativities and incompatibilities between the practices of Member States and, thus, a failed cybersecurity policy (Ciekanowski et al., 2023, p. 785). ENISA, which has a specific privileged position in this field due to its mandate in the field of information and cybersecurity, has also been recognised by organisations such as the CISA, which is part of the US Department of Homeland Security's mission to reduce security risks in cyberspace and the physical world, and the National Institute of Standards and Technology (NIST). This organisation develops measurement science, standards and technology to increase innovation and industrial competitiveness in the US (Kolouch et al., 2023, p. 285).

While the EU cybersecurity certification framework provides significant benefits in enabling the EU to compete in the international cybersecurity arena by preventing the risk of loss in the EU cybersecurity market, it has also been criticised by some quarters. Despite the harmonisation efforts at the EU level, the fact that some countries, such as France, the Netherlands, and Germany, add their control procedures for national security reasons, especially in the certification processes related to cloud services, limits the system's effectiveness. This has made it challenging to implement a genuinely Europe-wide certification regime and has led to the dominance of national interests (Propp et al., 2021). The fact that the framework was not finalised for a long time, in particular because of the geographical restrictions that these states wanted to impose on outsourced cloud service providers, was also criticised, and it was stated that the security benefits of these requirements were questionable and could weaken the EU's competitiveness. (European Business Review, 2023) As a result, the system delays negatively affected the EU's role in the global cybersecurity race.

The EU Cybersecurity Act, the expansion of ENISA's mandate and the increase of its powers have brought some challenges, including shortcomings in the implementation process and inadequacies that need to be improved. These challenges have also increased the agency's human resources and technical capacity requirements, thus requiring more financial resources for ENISA to effectively carry out all its tasks (Giantas, 2019, p. 18). In the same context, the differences in the cybersecurity capacities of EU Member States have also been assessed as complicating ENISA's coordination task and hindering the establishment of a common cybersecurity framework across all Member States (Pâris, 2021, p. 15).

While there is still a need to increase ENISA's resources and ensure the necessary coherence in cooperation for the effective implementation of standardization, it is possible to say that the Regulation is a crucial tool for the EU to achieve its goal of becoming a global leader in the field of cybersecurity due to various factors, such as the realization that the existing legal infrastructure framework could not respond quickly to specific threats, as demonstrated by the cyberattacks that occurred during the period of its entry into force (Fantin, 2024).

Although ENISA is responsible for shaping cybersecurity policy across the EU and providing guidance to national regulators, the fact that the agency does not have the authority to make binding decisions and impose sanctions on Member States has prevented the uniform implementation of EU-specific cybersecurity issues, leading to the emergence of inconsistencies at the national level, which has emerged as one of the agency's main weaknesses (Markopoulou et al., 2019, pp. 6-7). In this context, it is considered that ENISA's powers should be further strengthened and empowered to make binding decisions on specific issues, thus strengthening the harmonisation, coordination, and standardisation it aims to achieve in cybersecurity across the EU.

The extension of ENISA's competencies has also highlighted some challenges, such as the overriding competencies of Member States around national security, legislative competencies between Member States, resource constraints, and cybersecurity-related expertise. To increase the effectiveness of ENISA and the European cybersecurity certification framework, it is important to enhance cooperation and coordination between Member States while not neglecting information sharing and policy harmonisation, including best practice examples, further clarifying areas of expertise, prioritising critical sectors, and cooperating with sector-specific information sharing and cooperation bodies. It is also an important requirement for the EU to become more effective in cybersecurity-related legislative development and policy-making processes, and it has become necessary to avoid duplication of EU cybersecurity-related tasks and to ensure clarity in the proportional allocation of resources. Again, the recommendations of the Joint Public-Private Expert Unit should be considered when developing strategies to mitigate and respond to cyber threats, as increased cooperation between the public and private sectors increases resilience to cyber threats. It is important to base the impact assessment on an expert-driven perspective to prioritise the existence of a European cybersecurity certification framework. In this context, the Stakeholder Cybersecurity Certification Group (SCCG) should be allowed to interact with the ECCG in a result-oriented manner by including its views and playing a more proactive role in the meetings.

Although ENISA's institutionalisation process is long-term, the Cybersecurity Presidency of the Republic of Türkiye was established by Presidential Decree No. 177, which came into force on 8 January 2025 (Siber Güvenlik Başkanlığı hakkında Cumhurbaşkanlığı Kararnamesi No:177, 2025). The Presidency is expected to closely follow the work of ENISA, the cybersecurity agency of the EU, with which Türkiye is conducting full membership negotiations, and to work in coordination with ENISA within the framework of its institutional structure, which has been legally and institutionally updated for over twenty years. According to its founding decree, the Presidency will establish policies, strategies, and objectives to ensure cybersecurity in Türkiye and prepare action plans. It will also conduct studies to identify cybersecurity vulnerabilities by bringing together cybersecurity activities in the public and private sectors under one roof. The main objectives of the Presidency include preparing emergency and crisis management plans related to cybersecurity, conducting awareness, education, and training activities related to cybersecurity, developing IT products for the cybersecurity ecosystem in accordance with international standards, and participating in standardisation and certification activities when necessary (Avcioğlu, 2025; Özdemir, 2025).

Following this, the Cybersecurity Code No. 7545 (Siber Güvenlik Kanunu No: 7545, 2025), which came into effect approximately three months after the establishment of the Cybersecurity Presidency, became the second legal regulation directly related to cybersecurity adopted by the Republic of Türkiye. This law established a legal framework for all cybersecurity-related activities and transactions of public institutions and organisations, professional organisations with public institution status, individuals, and public or private legal entities, as well as non-legal entities (Bilgehan, 2025, p. 67). The code contributed to the necessary legal infrastructure for the Cybersecurity Presidency to fulfil its duties, thereby ensuring that comprehensive measures were taken to protect public institutions and organisations in Türkiye, as well as individuals and legal entities, against cyber attacks. Furthermore, the code has established a Cybersecurity Council (Şenol, 2025, p. 170) to define the responsibilities of relevant state institutions for the regulation of cyberspace and to determine strategies and policies to strengthen Türkiye's cybersecurity, thereby defining cybersecurity as an integral part of national security. The Cybersecurity Council, whose secretariat services will be carried out by the Cybersecurity Presidency, has been assigned more political tasks, such as making decisions on policies, strategies, action plans, and other regulatory procedures related to cybersecurity.

The law, which covers nine types of crimes and two misdemeanours (Şenol, 2025, p. 203), also defines new duties and authorities for the Cybersecurity Presidency that are different from those specified in the establishment decree.

The duties of the Cybersecurity Presidency are defined as regulating the procedures and principles that individuals, institutions, and organisations operating in the field of cybersecurity must comply with, detecting cyber attacks, establishing and supervising cyber incident response teams, establishing the necessary infrastructure for the cybersecurity of public services, and conducting certification procedures for services in the field of cybersecurity. conducting cybersecurity audits and imposing sanctions based on audit results, determining the qualifications of the organisations that will conduct the audits and appointing them, as well as identifying critical infrastructure and taking measures related to it (Karaman & Oğultürk, 2025, p. 60). As can be seen, the Cybersecurity Code has made the Cybersecurity Presidency more operational, and the operational powers of the Presidency are shaped as follows in the Code: taking necessary measures against cyber-attacks and transferring the data collected in this context to the Presidency's information system, providing support for responding to cyber incidents, collecting and sharing daily logs from information systems, and authorising independent auditors to conduct inspections.

The Cybersecurity Law, which is still in its infancy, is expected to develop a comprehensive framework to detect and eliminate all common cyber threats and to be preventive and design-based, given Türkiye's status as a candidate for full membership in the EU. In this way, Türkiye will lay the groundwork for joint operations and activities with the EU and EU member states through the Cybersecurity Presidency, which has legal personality (Yönt, 2025).

In addition, the Cybersecurity Presidency, which is expected to establish various working groups and operational units with the participation of stakeholders from all cybersecurity-related circles, is expected to coordinate with EU cybersecurity institutions, organisations, and structures such as CERT-EU, ENISA, and the CSIRTs Network supported by ENISA, the NIS Cooperation Group, EU-CyCLONe, and other EU cybersecurity agencies, institutions, organisations, and structures.

In conclusion, strengthening ENISA's powers, responsibilities, and mandate with the EU Cybersecurity Act is an important step in forming the EU's standard cybersecurity policy. However, to increase its effectiveness, the Agency needs to increase its resources and participation in decision-making processes and strike a balance between active participation in national policies and EU strategies. Otherwise, achieving the desired success in establishing a standard cybersecurity policy for the EU will not be possible. It is estimated that the EU Cybersecurity Code and ENISA, which have developed as a model for states in the international arena, can lead to the legal and institutional structures and regulations being made in the rest of the world and will continue to develop in coordination with them.

## **Bibliography**

Attström, K., Ludden, V., Lessmann, F., Weström, P., Conrads, J., Carrapico, H. F., ..., de la Maza, C. (2017). Study on the evaluation of the European Union Agency for Network and Information Security. Luxembourg: Publications Office of the European Union.

Avcioğlu, M. (2025). Türkiye establishes a new body to tackle cyber threats. <https://www.aa.com.tr/en/turkiye/turkiye-establishes-new-body-to-tackle-cyber-threats/3444618> (Accessed: 10<sup>th</sup> May 2025)

Bache, I., George, S. & Bulmer, S. (2011). Politics in the European Union. Oxford: Oxford University Press.

Baladari, V. (2025). Unraveling the 2024 CrowdStrike Incident: How a Security Patch Led to Global System Failure and Blue Screen of Death. *International Journal of Advanced Research in Science, Communication and Technology*, 5(8), 171–177. <https://doi.org/10.48175/IJARSCT-24524>

Benedikt, K. (2021). New act on privacy and electronic communications. *European Data Protection Law Review (EDPL)*, 7(2), 2021, 254–259. <https://doi.org/10.21552/edpl/2021/2/17>

Bigo, D., Boulet, G., Bowden, C., Carrera, S., Jeandesboz, J. & Scherrer, A. (2012). Fighting cybercrime and protecting privacy in the cloud. Brussels: European Parliament.

Bilgehan, A. D. (2025). Siber Güvenlik Başkanlığının düzenlenişine dair değerlendirme. *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 12(1), 63–88. <https://doi.org/10.46547/imuhfd.2025.12.1.3> Bisogni, F., Cavallini, S. & Di Trocchio, S. (2011). Cybersecurity at European level: The Role of Information Availability. *Communications and Strategies*, 1(81), 105–124.

Blaese, J-D. (2019). Cybersecurity at EU and national level – the expansion of economic policy. *Zei Insights*, 65. Bonn: Center for European Integration Studies. Brass, I. & Sowell, J. H. (2021). Adaptive governance for the internet of things: Coping with emerging security risks. *Regulation & Governance*, 15(4), 1092–1110. <https://doi.org/10.1111/rego.12343>

Brun, L. (2018). The role of the European Union Agency for Network and Information Security (ENISA) in the governance strategies of European cybersecurity. *Faculté des sciences économiques, sociales, politiques et de communication, Université catholique de Louvain, Bellanova, Rocco*. <http://hdl.handle.net/2078.1/thesis:16234> (Accessed: 12<sup>nd</sup> May 2025)

Bygrave, L. A. (May, 2022). Cyber resilience versus cybersecurity as legal aspiration. 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Tallinn, CCDCOE Publications, 27-44. [https://ccdcoe.org/uploads/2022/06/CyCon\\_2022\\_book.pdf](https://ccdcoe.org/uploads/2022/06/CyCon_2022_book.pdf) (Accessed: 7<sup>th</sup> August 2025).

Calliess, C. & Baumgarten, A. (2020). Cybersecurity in the EU the example of the financial sector: A legal perspective. *German Law Journal*, 21, 1149–1179. <https://doi.org/10.1017/glj.2020.67>

Carrapico, H. & Barrinha A. (2018). European Union cybersecurity as an emerging research and policy field. *European Politics and Society*, 19(3), 299–303. <https://doi.org/10.1080/23745118.2018.1430712>

Carrapico, H. & Farrand, B. (2020). Discursive continuity and change during Covid-19: The case of EU cybersecurity policy. *Journal of European Integration*, 42(8), 1111–1126. <https://doi.org/10.1080/07036337.2020.1853122>

Carrapico, H. & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *Journal of Common Market Studies*, 00, Annual Review, 1–12. <https://doi.org/10.1111/jcms.13654>

Cavelty, M. D. & Smeets, M. (2023). Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority. *Journal of European Public Policy*, 30(7), 1330–1352. <https://doi.org/10.1080/13501763.2023.2173274>

Commission of European Communities. (2000). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a safer information society by improving the security of information infrastructures and combating computer-related crime, COM(2000) 890 final, Brussels, 26.1.2001.

Commission of European Communities. (2001). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and information security: Proposal for a European policy approach, COM(2001) 298 final, Brussels, 06.06.2001.

Commission of European Communities. (2003). Proposal for a Regulation of the European Parliament and of the Council establishing the European Network and Information Security Agency (presented by the Commission), COM(2003) 63 final, 2003/0032 (COD), Brussels, 11.2.2003.

Commission of European Communities. (2006). Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A strategy for a secure information society – Dialogue, partnership and empowerment, COM(2006) 251 final, Brussels, 31.5.2006.

Chamon, M. (2014). The empowerment of agencies under the Meroni doctrine and article 114 TFEU: comment on *United Kingdom v Parliament and council* (short-selling) and the proposed single resolution mechanism. *European Law Review*, 39(3), 380–403.

Chatterjee, C. & Lefcovitch, A. (2016). Cybersecurity, Diplomacy and International Law, *Amicus Curiae*, 108, 2–12. <https://doi.org/10.14296/ac.v2016i108.4945>



Chiara, P.G. (2024). The internet of things and EU law. Law, governance and technology series 67. Switzerland: Springer. <https://doi.org/10.1007/978-3-031-67663-5>

Christou, G. (2016). Cybersecurity in the European Union: Resilience and adaptability in governance policy, Hampshire: Palgrave Macmillan. <https://doi.org/10.1057/9781137400529>

Ciekanowski, Z., Gruchelski, M., Nowicka, J., Żurawski, S., Pauliuchuk, Y. (2023). Cyberspace as a source of new threats to the security of the European Union. European Research Studies Journal, 26(3), 782–797. <https://doi.org/10.35808/ersj/3249>

Court of Justice of the European Union. (2005). United Kingdom of Great Britain and Northern Ireland v European Parliament and Council of the European Union, Case C-217/04. EU:C:2006:279.

Craig, P. (2012). EU administrative law, Oxford: Oxford University Press.

Craig, P. P. (2011). Shared administration and networks: Global and EU perspectives. In Anthony, G., Auby, J.-B., Morison, J. & Zwart, T. (Eds.), Values in Global Administrative Law, 81-116, Bloomsbury Publishing.

Cornish, P. (2009). Cybersecurity and politically, socially and religiously motivated cyber-attack, Brussels: European Parliament.

Cosic, J., & Jukan, A. (2024). Deciphering cyber-security certifications: An ontological journey through composite systems and their certification. 2024 IEEE International Conference on Engineering, Technology, and Innovation (ICE/ITMC), Funchal, Portugal, 2024, 1-6, <https://doi.org/10.1109/ICE/ITMC61926.2024.10794255>.

D’Alterio, F., Rotunno, M., Settembre, M., Bernardini, A. & Sagratella, L. (2024). Navigating 5G security: Challenges and progresses on 5G security assurance and risk assessment, 2024 AEIT International Annual Conference (AEIT), Trento, Italy, 2024, 1-6, <https://doi.org/10.23919/AEIT53387.2021.9627014>

Dewar, R. S. (2017). The European Union and Cybersecurity: A Historiography of an Emerging Actor’s Response to a Global Security Concern. In O’Neill, M. & Swinton, K. (Eds.), Challenges and Critiques of the EU Internal Security Strategy: Rights, Power and Security, 113-148, Cambridge Scholars Publishing.

Dragomir, A. (2021). Cyber diplomacy. International Journal of Information Security and Cybercrime, 10(2), 37-50. <https://doi.org/10.19107/IJISC.2021.02.05>

Duic, D. & Petrusevic, T. (2023). Data protection and cybersecurity: case-law of two European courts. EU and Comparative Law Issues and Challenges Series, 7 (Special Issue), 94-118.

Dupré, L. (2014). EP3R 2010-2013: Four years of Pan-European public-private cooperation. Atina: ENISA.



Duvvur, V. (2022). Securing the Future: Strategies for Modernizing Legacy Systems and Enhancing Cybersecurity. *Journal of Artificial Intelligence & Cloud Computing*, 1(3), 1–3. [https://doi.org/10.47363/JAICC/2022\(1\)299](https://doi.org/10.47363/JAICC/2022(1)299)

EEAS Press Team. (2023). US: The European Union and the United States hold the 9<sup>th</sup> Cyber Dialogue in Brussels. [https://www.eeas.europa.eu/eeas/us-european-union-and-united-states-hold-9th-cyber-dialogue-brussels\\_en](https://www.eeas.europa.eu/eeas/us-european-union-and-united-states-hold-9th-cyber-dialogue-brussels_en) (Accessed: 25<sup>th</sup> March 2025).

El-Maissi, A. M., Kassem, M. M., & Mohamed Nazri, F. (2024). Resilient critical infrastructures: An innovative methodological perspective for critical infrastructure (CI) integrated assessment models by inducing digital technologies during multi-hazard incidents. *MethodsX*, 12, 102561. <https://doi.org/10.1016/j.mex.2024.102561>

ENISA. (2021). ENISA threat landscape for supply chain attacks. <https://doi.org/10.2824/168593>

ENISA. (2024a). ENISA threat landscape 2024. <https://doi.org/10.2824/0710888>

ENISA. (2024b). The ENISA Threat landscape (ETL) report is the annual report of the European Union Agency for Cybersecurity, ENISA, on the state of the cybersecurity threat landscape. <https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape> (Accessed: 15<sup>th</sup> May 2025).

ENISA. (2024c). Best practices for cyber crisis management. <https://doi.org/10.2824/767828>.

Enescu, S. (2020). A Comparative Study On European Cybersecurity Strategies. (Ed. Adrian Lesenciuc), International Conference RCIC'20: Redefining community in intercultural context, 7-9 May 2020, 9(1), (277-282), Brasov: 'Henri Coanda' Air Force Academy Publishing.

European Business Review. (2023). France and Germany are increasingly drifting apart on digital sovereignty of the cloud sector. <https://www.europeanbusinessreview.eu/page.asp?pid=6989>, (Accessed: 30<sup>th</sup> May 2025).

European Commission. (2010a). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A digital agenda for Europe, COM(2010) 245 final, Brussels, 19.5.2010. Publications Office of the European Union.

European Commission. (2010b). Proposal for a regulation of the European Parliament and of the Council Concerning the European Network and Information Security Agency (ENISA), Brussels, 30.9.2010, COM(2010) 521 final, 2010/0275 (COD). Publications Office of the European Union.

European Commission. (2013a). Joint communication to the European Parliament, the Council, the European Economic And Social Committee and the Committee Of The Regions, Cybersecurity Strategy of the European Union: An open, safe and secure cyberspace, JOIN(2013) 1 final, Brussels, 7.2.2013. Publications Office of the European Union.

European Commission. (2013b). Proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final, 2013/0027 (COD), Brussels, 7.2.2013. Publications Office of the European Union.

European Commission. (2016). Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry, COM(2016) 410 final, Brussels, 5.7.2016. Publications Office of the European Union.

European Commission. (2017a). Joint Communication to The European Parliament and The Council, Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, JOIN(2017) 450 final, Brussels, 13.9.2017. Publications Office of the European Union.

European Commission. (2017b). Proposal for a regulation of the European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) No 526/2013, and on information and communication technology cybersecurity certification ("Cybersecurity Act"), COM(2017) 0477 final, 2017/0225 (COD), Brussels, 13.9.2017. Publications Office of the European Union.

European Commission. (2020). Joint Communication to the European Parliament and the Council: EU cybersecurity strategy for the digital decade, JOIN(2020) 18 final, Brussels, 16.12.2020. Publications Office of the European Union.

European common criteria-based cybersecurity certification scheme (EUCC). (2024). <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4737205> (Accessed: 15<sup>th</sup> May 2025).

Fantin, S. (2024). Weighting the EU Cybersecurity Act: Progress or missed opportunity?, <https://www.law.kuleuven.be/citip/blog/weighting-the-eu-cybersecurity-act-progress-or-missed-opportunity/> (Accessed: 10<sup>th</sup> May 2025).

Fowler, D. S., Epiphaniou, G. & Maple, C. (2022). Cybersecurity assurance and certification for systems, 1–9. <https://doi.org/10.13140/RG.2.2.11527.16805/1>

Gao, X. & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, 22(4), 689-708. <https://doi.org/10.1080/14702436.2022.2110485>

Gajewski, T. (2020). Towards resilience: European cybersecurity strategic framework. *Ante Portas – Security Studies*, 1(14), 103–122. <https://doi.org/10.33674/3201911>

Gercke, M. (2009). Europe's legal approaches to cybercrime. *ERA Forum: Journal of the Academy of European Law*, 10(3), Berlin: Springer-Verlag, 409–420. <https://doi.org/10.1007/s12027-009-0132-5>

Giantas, D. H. (2019). Cybersecurity in the EU: Threats, frameworks and future perspectives. *Laboratory of Intelligence & Cyber-Security Working paper*, 1, University of Piraeus.

Glorioso, A. & Servida, A. (2012). Infrastructure sectors and the information infrastructure. In J. Lopez, R. Setola & S. D. Wolthusen (Eds.), *Critical infrastructure protection: Information infrastructure models, analysis, and defenses*, 39–51, Springer Publishing. [https://doi.org/10.1007/978-3-642-28920-0\\_3](https://doi.org/10.1007/978-3-642-28920-0_3)

Hoong, Y. & Rezania D. (2024). Balancing talent and technology: Navigating cybersecurity and privacy in SMEs. *Telematics and Informatics Reports*, 15, September 2024, 100151. <https://doi.org/10.1016/j.teler.2024.100151>

Huddleston, J., Ji, P., Bhunia, S., & Cogan, J. (2021). How VMware exploits contributed to SolarWinds supply-chain attack. *2021 International Conference on Computational Science and Computational Intelligence (CSCI)*, 760–765. <https://doi.org/10.1109/CSCI54926.2021.00190>

Irion, K. (2012). The governance of network and information security in the European Union: The European public-private partnership for resilience (EP3R). In J. Krüger, B. Nickolay & S. Gaycken (Eds.), *The Secure Information Society: Ethical, Legal and Political Challenges*, 83–116, Springer Publishing. [https://doi.org/10.1007/978-1-4471-4763-3\\_4](https://doi.org/10.1007/978-1-4471-4763-3_4)

Hoff, R. M., & Chester, M. V. (2023). Preparing infrastructure for surprise: fusing synthetic network, interdependency, and cascading failure models. *Environmental Research: Infrastructure and Sustainability*, 3(2), 025009. <https://doi.org/10.1088/2634-4505/acd07d>

Holzleitner, M.T. & Reichl, J. (2017). European provisions for cybersecurity in the smart grid – an overview of the NIS-directive. *Elektrotechnik & Informationstechnik*, 134(1), 14–18. <https://doi.org/10.1007/s00502-017-0473-7>

Kafitz, W. & Burgers, V. (2013). Security in critical infrastructures – Future precondition for operating license?. (Ed. Reimer, H.), in *ISSE 2013 Securing electronic business processes*, 205–216, Berlin: Springer Publishing. [https://doi.org/10.1007/978-3-658-03371-2\\_18](https://doi.org/10.1007/978-3-658-03371-2_18)

Kamara, I., Leenes, R., Stuurman, C., & van den Boom, J. (2020). The cybersecurity certification landscape in the Netherlands after the Union Cybersecurity Act. *Final Report*, Netherlands: National Cybersecurity Centre.

Kamara, I. (2025). European cybersecurity standardisation: a tale of two solitudes in view of Europe's cyber resilience. *Innovation: The European Journal of Social Science Research*, 37(5), 1441–1460, <https://doi.org/10.1080/13511610.2024.2349626>

Kalogeraki, E. M. & Polemi, N. (2024). A taxonomy for cybersecurity standards, *Journal of Surveillance, Security and Safety*, 5, 95–115. <https://doi.org/10.20517/jsss.2023.50>

Karaman, İ., & Oğultürk, M. C. (2025). Şehir jeopolitiği ve İstanbul'un kritik altyapılarının korunması: Katılımcı kent güvenliği yaklaşımı. *Güvenlik Stratejileri Dergisi*, 21(50), 49–72. <https://doi.org/10.17752/guvenlikstrtj.1596452>

Kasper, A. (2020). EU cybersecurity governance – stakeholders and normative intentions towards integration. In *The future of the European Union - Demisting the debate*, 166–185, The Institute for European Studies, University of Malta.

Kermabon-Bobinnec, H., Jarraya, Y., Wang, L., Majumdar, S., & Pourzandi, M. (2024). Phoenix: Surviving Unpatched Vulnerabilities via Accurate and Efficient Filtering of Syscall Sequences. *Proceedings 2024 Network and Distributed System Security Symposium*, 1–18. <https://doi.org/10.14722/ndss.2024.24582>

Kizza, J. M. (2020). Introduction to Computer Network Vulnerabilities. In *Guide to Computer Network Security* (pp. 87–103). Springer. [https://doi.org/10.1007/978-3-030-38141-7\\_4](https://doi.org/10.1007/978-3-030-38141-7_4)

Khurshid, A., Alsaaidi, R., Aslam, M. & Raza, S. (2022). EU Cybersecurity Act and IoT certification: Landscape, perspective and a proposed template scheme, *IEEE Access*, 10, 129932-129948. <https://doi.org/10.1109/ACCESS.2022.3225973>

Kohler, C. (2020). The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*, 1, 7–12. <https://doi.org/10.1365/s43439-020-00008-1>

Kolouch, J., Tovarnak, D., Plesnik, T. & Javornik, M. (2023). Cybersecurity: Notorious, but often misused and confused terms, *Masaryk University Journal of Law and Technology*, 17(2), 281–305. <https://doi.org/10.5817/MUJLT2023-2-5>

Lehto, M. (2015). Phenomena in the cyber world. In M. Lehto & P. Neittaanmäki (Eds.), *Cybersecurity: Analytics, technology and automation*, 3–29, Springer Publishing. [https://doi.org/10.1007/978-3-319-18302-2\\_1](https://doi.org/10.1007/978-3-319-18302-2_1)

Lonardo, L. (2021). EU Law against hybrid threats: A first assessment. *European Papers*, 6(2), 1075-1096. <https://doi.org/10.14454/3w3z-sa82>

Lu, I. F. (2022). To subdue the enemies without fighting: Chinese state-sponsored disinformation as digital warfare. *Digital War*, 3(1–3), 96–106. <https://doi.org/10.1057/s42984-022-00052-7>

Mohapatra, K. K. (2025). Digital authoritarianism in India: Surveillance, control, and resistance. *International Journal for Multidisciplinary Research (IJFMR)*, 7(3), 1–13.

Markopoulou, D., Papakonstantinou, V. & De Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation, *Computer Law & Security Review*, 35(6), 105336. <https://doi.org/10.1016/j.clsr.2019.06.007>

Markow, W. (2024, October). The lightcast quarterly cybersecurity talent report. <https://Lightcast.io/Resources/Research/Quarterly-Cybersecurity-Talent-Report-Oct-24> (Accessed: 9<sup>th</sup> August 2025).

Mattioli, R., Malatras, A., Hunter, E. N., Biasibetti P., Marco G., Bertram, D. and Neubert, I. (2023). Identifying emerging cybersecurity threats and challenges for 2030. ENISA. <https://doi.org/10.2824/117542>

Mitrakas, A. (2006). Information security and law in Europe: Risks checked. *Information & Communications Technology Law*, 15(1), 33-54. <https://doi.org/10.1080/13600830600557984>

Mitrakas, A. (2018). The emerging EU framework on cybersecurity certification, *Datenschutz und Datensicherheit*, 42, 411-414. <https://doi.org/10.1007/s11623-018-0969-2>

Mohapatra, K. K. (2025). Digital authoritarianism in India: Surveillance, control, and resistance. *International Journal for Multidisciplinary Research (IJFMR)*, 7(3), 1-13.

Moise, A. C. (2023). The European Union strategy in the field of cyber-security, *International Journal of Legal and Social Order*, 3(1), 273-279. <https://doi.org/10.55516/ijlso.v3i1.168>

Negreiro, M. (2019). ENISA and a new cybersecurity act, European Parliamentary research service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS\\_BRI%282017%29614643\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2017/614643/EPRS_BRI%282017%29614643_EN.pdf) (Accessed: 21<sup>st</sup> May 2025).

Nwankwo, I., Stauch, M., Radoglou-Grammatikis, P., Sarigiannidis, P., Lazaridis, G., Drosou, A. & Tzovaras, D. (2022). Data protection and cybersecurity certification activities and schemes in the energy sector. *Electronics*, 11(6), 965. <https://doi.org/10.3390/electronics11060965>

Official Journal of the European Union. (2004). Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (Text with EEA relevance). L 077, 13.03.2004, 1-11.

Official Journal of the European Union. (2013). Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004 (Text with EEA relevance). L 165, 18.06.2013, 41-58.

Official Journal of the European Union. (2016). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. L 194, 19.7.2016, 1-30.



Official Journal of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (Text with EEA relevance). L 151, 7.6.2019, 15–69.

Official Journal of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). L 333, 27.12.2022, 80–152.

Official Journal of the European Union. (2024). Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act). L, 2024/2847, 20.11.2024.

Official Journal of the European Union. (2025). Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act). L, 2025/38, 15.1.2025.

Özdemir, A.B. (2025). Siber Güvenlik Başkanlığı Türkiye için ne ifade ediyor?. <https://www.aa.com.tr/tr/analiz/siber-guvenlik-baskanligi-turkiye-icin-ne-ifade-ediyor/3449616> (Accessed: 9<sup>th</sup> January 2025).

Pâris, C. (2021). Guardian of the galaxy? Assessing the European Union's international actorness in cyberspace. EU Diplomacy Papers, Belgium: College of Europe, Department of EU International Relations and Diplomacy Studies

Paladini, S. & Castellucci, I. (2019). The EU agencies and other European security-related institutions and arrangements. In European Security in a Post-Brexit World (Brexit Studies Series), Leeds: Emerald Publishing Limited, 59-94. <https://doi.org/10.1108/978-1-78769-837-620191004>

Pauri, E. (2017). Agency Reform in the time of cybersecurity governance: ENISA, LUISS Law Review, (2), 95–108.

Pawlak, P. (2018). Protecting and defending Europe's cyberspace. In N. Popescu, & S. Stanislav (Eds.), Hacks, leaks and disruptions. Russian cyber strategies, Chaillot Paper, 148, 103-114, European Union Institute for Security Studies,

Polčák, R. (2022). Cybersecurity certification and compliance in financial services. In J. Lee, & A. Darbellay (Eds.), Data governance in AI, FinTech and LegalTech, 212-236, Edward Elgar Publishing.

Popescu, A. (2017). The right to information and cybersecurity. Journal of Law and Public Administration, 3(6), 104-111.

Propp, K., Swire P. & Fox, J. (2023). Oceans apart: The EU and US cybersecurity certification standards for cloud services. <https://www.crossborderdataforum.org/oceans-apart-the-eu-and-us-cybersecurity-certification-standards-for-cloud-services/> (Accessed: 15<sup>th</sup> May 2025).

Purser, S. (2014). Standards for cybersecurity. (Ed. Hathaway, M.E.), in *Best practices in computer network defense: Incident detection and response*, 97-106. IOS Press. <https://doi.org/10.3233/978-1-61499-3727>

Radoniewicz, F. (2022). Cybersecurity in the European Union law. In K. Chałubińska-Jentkiewicz, F. Radoniewicz & T. Zieliński (Eds.), *Cybersecurity in Poland*, 73-92, Springer.

Ramunno, G. (2014). EU cyberdefence strategy. European Union Military Committee, 6, 1-2.

Renard, Thomas. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19(3), 321-337. <https://doi.org/10.1080/23745118.2018.1430720>

Renda, K. K. (2022). The development of EU cybersecurity policy: From a coordinating actor to a cyber power?. *Ankara Avrupa Çalışmaları Dergisi*, 21(2), 467-495. <https://doi.org/10.32450/aacd.1226890>

Robinson, N. (2012). European cybersecurity policy. (ed. Kim Andreasson), in *Cybersecurity: Public sector threats and responses*, 159-192, Boca Raton: CRC Press.

Ruohonen, J., Hyrynsalmi, S. & Leppänen, V. (2016). An outlook on the institutional evolution of the European Union cybersecurity apparatus. *Government Information Quarterly*, 33(4), 746-756. <https://doi.org/10.1016/j.giq.2016.10.003>

Ruohonen, J. (2024). The Incoherency risk in the EU's new cyber security policies. *Conference on e-Business, e-Services and e-Society*, Cham, Springer Nature Switzerland, 284-295. [https://doi.org/10.1007/978-3-031-72234-9\\_24](https://doi.org/10.1007/978-3-031-72234-9_24)

Seatzu, F. & Santarelli, N. C. (2024). On the law, work and functioning of the EU agency for cybersecurity, *Peace & Security – Paix et Sécurité Internationales*, 12, 1-26. [https://doi.org/10.25267/Paix\\_secur\\_int.2024.i12.1204](https://doi.org/10.25267/Paix_secur_int.2024.i12.1204)

Siber Güvenlik Başkanlığı hakkında Cumhurbaşkanlığı Kararnamesi No: 177. (2025, 8<sup>th</sup> January). Resmi Gazete, (Issue 32776). <https://www.resmigazete.gov.tr/eskiler/2025/01/20250108-1.pdf> (Accessed: 16<sup>th</sup> May 2025).

Siber Güvenlik Kanunu No: 7545. (2025, 19<sup>th</sup> March). Resmi Gazete, (Issue 32846). <https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm> (Accessed: 16<sup>th</sup> May 2025).



Sindhwad, P., & Kazi, F. (2022). Exploiting Control Device Vulnerabilities: Attacking Cyber-Physical Water System. 2022 32nd Conference of Open Innovations Association (FRUCT), 270–279. <https://doi.org/10.23919/FRUCT56874.2022.9953826>

Singh, C. (2023). The European approach to cybersecurity in 2023: A review of the changes brought in by the Network and Information Security 2 (NIS2) Directive 2022/2555, *International Company and Commercial Law Review*, 5, 251-261.

Stodolnik, M. (2025). Cyber threats as hybrid activity against the European Union in light of the current geopolitical situation. *Terroryzm, Special Issue*, 225–248. <https://doi.org/10.4467/27204383TER.25.021.21524>

Swire, P., Kennedy-Mayo, D., Bagley, D., Krasser, S., Modak, A. and Bausewein, C. (2024). Risks to cybersecurity from data localization, organized by techniques, tactics and procedures. *Journal of Cyber Policy*, Published online: 26 Aug 2024. <https://doi.org/10.1080/23738871.2024.2384724>

Szádeczky, T. (2018). Cybersecurity authorities and related policies in the EU and Hungary. *Central and Eastern European eDem and eGov Days*, 331, 287-299. <https://doi.org/10.24989/ocg.v331.24>

Szádeczky, T. (2020). Governmental regulation of cybersecurity in the EU and Hungary after 2000. *AARMS*, 19(1), 83–93. <https://doi.org/10.32565/aarms.2020.1.7>

Şenol, C. (2025). 7545 sayılı Siber Güvenlik Kanunu'nda düzenlenen suçlar. *Türkiye Adalet Akademisi Dergisi*, 63, 169–206. <https://doi.org/10.54049/taad.1751122>

Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, 105890. <https://doi.org/10.1016/j.clsr.2023.105890>

Vavousis, K., Papadopoulos, M., Polley, J., Xenakis, C. (2020). A compliant and secure IT infrastructure for the National Library of Greece in consideration of internet security and GDPR. *Qualitative and Quantitative Methods in Libraries (QQML)*, 9(2), 219-236.

Vercher-Moll, J. (2014). Towards a European supervisory authority. *Connecticut Insurance Law Journal*, 21(1), 173-208. <https://opencommons.uconn.edu/cilj/137>

Verhelst, A. & Wouters, J. (2020). Filling global governance gaps in cybersecurity: International and European legal perspectives, *International Organisations Research Journal*, 15(2), 141–172. <https://doi.org/10.17323/1996-7845-2020-02-07>

Villani, S. (2025). The Cyber Solidarity Act: Framework and perspectives for the new EU-wide sybersecurity solidarity mechanism under the EU legal system. *European Journal of Risk Regulation*, 16(2), 485–497. <https://doi.org/10.1017/err.2025.24>

Vlajic, I. B. (2023). Legal aspects of fighting cyber crime in the European Union revised paper. *ODITOR - Journal for Management, Finance and Law*, 2, 193-207. <https://doi.org/10.5937/Oditor2301017B>

Voss, W. G. (2021). The concept of accountability in the context of the evolving role of ENISA in data protection, ePrivacy, and cybersecurity, In A. Arcuri, & F. Coman-Kund (Eds.), *Technocracy and the Law: Accountability, Governance and Expertise*, 247-284, Routledge. <https://10.2139/ssrn.4290558> (Accessed: 15<sup>th</sup> January 2025)

Yönt, Ş. (2025). AI Regulation in Türkiye: Bringing International Laws into the Discussion. Discussion Paper, TRT Training and Research Department, January 2025. <https://researchcentre.trtworld.com/wp-content/uploads/2025/01/AI-Regulation-in-Turkiye-2.pdf> (Accessed: 15<sup>th</sup> January 2025)



Hacer KAYA  
Kırıkkale University



**Received/Geliş Tarihi**

02 February 2025

**Accepted/Kabul Tarihi**

24 August 2025

**Publication/Yayın Tarihi**

31 August 2025

**Corresponding**

**Author/Sorumlu Yazar**

Hacer KAYA

hcrkya95@gmail.com

**DOI:** 0.69494/jirps.1631596

**Cite this article**

İKaya, H. (2025). The Balance of Power Theory, Alliances as Both Cause and Shield of War: NATO and SCO. Journal of International Relations and Political Science Studies, (14), 65-88.



Content of this journal is licensed under a Creative Commons Attribution-Noncommercial 4.0 International License.

**Research Article - Araştırma Makalesi**

**THE BALANCE OF POWER THEORY, ALLIANCES  
AS BOTH CAUSE AND SHIELD OF WAR:  
NATO AND SCO**

In an anarchic international system, states form alliances in order to feel more secure. These alliances, which may be for the purpose of balancing their power or preventing the emergence of a hegemonic power, also create a contradiction as to whether the balance of power leads to war or peace. Therefore, there is a distinction in the literature as to whether the balance of power leads to war or peace. This distinction is basically between realists, who argue that alliances prevent war, and liberals, who argue that the balance of power further spreads war. While realists argue that alliances prevent war and guarantee peace through the balance of power, liberals argue the opposite, that is, alliances cause war or expand the scope of existing war.

The study addresses the aforementioned debate in the literature. Both theses are examined through the example of the North Atlantic Treaty Organization (NATO) for the sake of completeness and accurate comparison, and a comparative analysis is made with the Shanghai Cooperation Organization (SCO). Especially after Russia's invasion of Ukraine on February 24, 2022, Finland and Sweden's initiatives to become NATO members and Russia's clear stance against Ukraine's membership in the Alliance brought NATO's deterrence back to the agenda. This is directly related to the fifth article of the Alliance. Because Ukraine's membership means that Russia's attacks will be limited. This study examines this debate in the literature with a special focus on NATO's Article 5, which is seen as its greatest deterrent.

**Keywords:** Balance of power, Alliances, Liberalism, NATO, Realism.

## **Introduction**

Since the concept of 'power' has an important place in the discipline of international relations, most issues are dealt with within the scope of this concept. 'Balance of Power Theory', which is a strategic method frequently used by states, is only one of these issues. Therefore, this theory constitutes the conceptual framework of the study. The theoretical framework of the study is shaped around the perspectives of realists and liberals on the balance of power. In this context, a comparative analysis of the realist and liberal perspectives on alliances is made with a special focus on NATO. In order to better understand NATO's deterrence, a comparative analysis with the Shanghai Cooperation Organization (SCO) is employed, as well. While realists argue that alliances create deterrence by enabling states to establish a balance of power and thus block the path to war, liberals argue that alliances increase the risk of war through the balance of power and spread war by drawing the entire alliance into the war. Thus, it is aimed to deepen the subject by revealing the differences and similarities between the two alliances in terms of structure, membership and deterrence mechanisms.

Based on the question of whether alliances are the cause or the shield of war, this study focuses on the general trend in the literature and the reason for this general trend. In doing so, the deterrence mechanisms of NATO and SCO are compared as a case study. The hypothesis of the study is that alliances are a shield against war. In other words, according to the study, being a member of NATO is one of the most important obstacles to war. Because although NATO's Article 5 has been used only once in history, it remains the most effective deterrence method. Russia is particularly opposed to Ukraine and Georgia becoming NATO members. This shows that the deterrence of this article is effective even today.

Realists argue that in an anarchic international system, states are forced to maximize their power in order to feel secure and this puts them in a security predicament<sup>[1]</sup>, while liberals argue that states get themselves into this predicament because they misperceive each other's actions. Therefore, these two views diverge in analyzing the relationship between wars and alliances, too. While realists argue that alliances create deterrence by enabling states to establish a balance of power and thus block the path to war, liberals argue that alliances increase the risk of war through the balance of power and spread war by drawing the entire alliance into the war.

[1] In international relations, a security dilemma is a situation in which a state's efforts to increase its security may be perceived as a threat by other states, leading them to increase their own security in response (John Herz, *Political Realism and Political Idealism: A Study in Theories and Realities*. Chicago: Chicago University Press, 1951, pp. 157).

One of the most important points determining whether alliances are a cause or a shield of war is the international conjuncture. In this context, if an alliance is made in a conjuncture where there are tensions between the parties, this will lead to misunderstandings and cause counter-alliance structuring. On the other hand, on the other hand, an alliance made within a harmonization process will not be perceived as a threat and there will be no need to take countermeasures. In fact, it is understood that the difference of opinion between realists and liberals in the literature emerged for this reason. Because according to them, the establishment of an alliance in a tense international system will either obstacle or cause war. Realists think that since states maximize their power through alliances, the other side will not dare to do so, while liberals think that this situation will disturb the other side more. How alliances are formed within the structure of the international system has also influenced the perspectives developed against them.

In the period between 1815-1870, the level of alliance was low and the frequency of war was high, while between 1871-1900, the level of alliance was high but the frequency of war was quite low (Singer and Small, 1966). These statistical data presented by Singer and Small mostly support the realists' view. Two cases can be given as examples: The first one is the European harmonization process. Since there was no trust problem between states in this process, the alliances made did not lead to war, on the contrary, they contributed to the development of relations between states. On the other hand, in a period of escalating tensions and a gradual decline in mutual trust, NATO, which was established in 1949, led to the formation of a counter-alliance in 1955, the Warsaw Pact.

Founded in 1949, NATO had no direct impact on the Korean War, which started in 1950. However, especially NATO's involvement in the Korean War led to both the formation of a counter-alliance and the involvement of all members in the war. These two defense organizations went into an arms race on the grounds of deterrence, but there was no hot conflict between the two alliances. War was prevented as alliances created deterrence for each other. As a result, alliances are not the only way for states to engage in war (Vasquez, 2009), but a way to prepare for or avoid war (Gibler, 1996).

The study focuses on how realists and liberals establish the link between alliances and wars, and examines the practical implications of their arguments. In this context, the balance of power theory is explained, followed by the approaches of realists and liberals to this theory. Then, the subject is discussed through the example of NATO, its comparison with the Shanghai Cooperation Organization (SCO). Finally, it is discussed whether NATO is still a deterrent alliance that prevents war today.

## **I. The Balance of Power Theory**

Alliances are one of the most common ways of creating a balance of power. McGowan and Rood (1975) define alliances as a situation in which at least two states make a military commitment to fight or remain neutral against at least one other state; Snyder (1997) defines alliances as formal unions formed by states to use (or not to use) military force against states other than their own members in certain situations; and Walt (1987) defines alliances as a formal or informal security cooperation relationship between two or more sovereign states. In other words, according to them, alliances emerge in the presence of an external threat (Fedder 1968).

There is a tendency in the literature that alliances are the primary instruments that foreign policy makers can use in a balance of power situation. This is because alliances enable leaders to preserve the pluralism of the system and ensure the survival of the system's main actors, even at the expense of solidarity (Dinerstein, 1965).

According to Waltz (1979), if there is a distinct political theory of international politics, it is the balance of power theory. Some scholars think that this theory is a guide for statesmen, while others think that it is a cloak that hides imperialist policies. Some believe that the balance of power is the best guarantee of state security and world peace, while others argue that it is in fact the cause of most wars (Little, 2007).

According to Kaplan (1969), there are six basic rules of a balance of power system: First, states have the incentive to increase their capacities but prefer mutual negotiations to war; second, states would rather go to war than fail to increase their capacities; third, they will stop war if it involves the elimination of a major actor; fourth, they will take action against states or coalitions that seek to become dominant in the system; fifth, they would work to limit states that tend to adhere to the principles of supranational organization; and finally, they would work for a defeated or destroyed core actor to return to the system and regain its status as a core actor or for a state that was not previously a core actor to join the core actor classification.

Morgenthau (1948) categorizes the reasons for the formation of the balance of power under four headings: policy towards a specific situation, the existence of a de facto situation, ensuring an equal distribution of power in the system and preventing any conceivable distribution of power, while Walt (1985) argues that the two main reasons for states to establish a balance are to prevent a potential hegemon or to increase their own influence by joining the weaker side.



On the other hand, Walt argues that states form alliances to balance threats rather than to counter them, but Little (2007) argues that this alliance may also lead to the formation of a counter-alliance[2].

In the United Nations (UN) Security Council, the Russia-China duo frequently confronts the US-UK-France trio. In this respect, a new East-West antagonism has emerged. In fact, by acting together in the Council, China and Russia are trying to maintain a balance of power with the West, with which they are in competition in many areas. Another example is the attempt to preserve the existing balance of power and distribution of power between Italy and Germany, Pakistan and India, and Argentina and Brazil (Demirel 2019). The US-Russia rivalry in Syria was a mutual struggle between the two sides to turn the balance of power in the region in their favor and protect it. What happened in Afghanistan, Iraq and Libya is an example of a similar situation.

Abbé de Pradt (1815) argues that the balance of power means war, while peace is identical with solving problems according to moral, economic and ethnographic virtues. Kant agrees with Pradt, calling the balance of power a *Hirngespinnst* (unattainable wish, dream, delusion) (Haas, 1953). According to Cobden, the balance of power is a monster. It is not an error, mistake or trick, but an undefined, indefinable, incomprehensible nothingness (Cobden, 1867).

In conclusion, there are opposing views in the literature that the balance of power is both positive and negative. Representatives of both views use examples from history to support their arguments. In this study, these two views are discussed. Realist and liberal views on whether the balance of power resulting from alliances between states prevents or spreads war are presented.

## **II. Alliances as “War Shields”: A Realist Perspective**

According to the realist balance of power theory, alliance building is one of the ways to avoid war and promote peace through force, as the uncertainties inherent in anarchy encourage balancing behavior (Walt, 1988). Therefore, many realists argue that alliance building as a response to threat helps to prevent war (Vasquez, 2009). Although realists see war as a natural phenomenon, they argue that there is a way to eliminate war or limit its scope and that this way is through the ‘balance of power’ (Dalkılıç, 4).

[2] An alliance formed to counter the power of a state or group of states is called a counter-alliance. This alliance is formed to balance the balance and deter a possible attack. F.i.: 1949 NATO-1955 Warsaw Pact. (Michael Sheehan, *The Balance of Power: History and Theory*, 1996, London, Routledge).

Classical realists believe that states should increase their power in the face of threats and one of the ways to do this is to form alliances (Vasquez, 2009). In other words, with the balance of power they establish against the threat, states secure themselves without the need for war.

For realists, alliances are about pooling capabilities and are often formed to balance powerful states (Waltz, 1979) or states perceived as threatening adversaries (Walt, 1987) in a process described as 'hard balancing'[3]. Schroeder (1976) and Mearsheimer (2001) also embrace the idea that alliances can be formed preemptively to restrain enemies and that states join alliances to protect themselves from threatening states or coalitions. By keeping all states under control, the balance of power system prevents the occupation of other states' territories as it does not allow any state to become more powerful (Zinnes, 1967).

In other words, the balance of power system ensures the status quo and prevents potential conflicts. In this sense, the main purpose of alliances is to prevent war by increasing the ability to deter conflict (Morrow, 1994; Fearon, 1997; Smith, 1998). Accordingly, as alliances provide information to allies, they will deter their enemies from challenging them or force them to submit to them (Leeds, 2003).

The nineteenth century was the only period in the last 500 years in which the confrontational effects of alliances were moderate. Only 44 percent of all alliances ended in war (100 percent in the sixteenth century, 89 percent in the seventeenth, 73 percent in the eighteenth and 81 percent in the twentieth), and none of the 'great power' alliances were followed by a 'great power' war within five years of their inception (Levy, 1981 Table 7). Based on these statistics, Wayman (1990) argues that in order to infer that alliances have an effect, the amount of wars after alliances must be statistically higher than the amount of wars before alliances are formed. Since the above statistics also show that the amount of alliances made before the war is small, Wayman rejects the link between alliances and war.

Wallace (1985) draws attention to the international conjuncture to explain the relationship between alliances and war. According to him, alliances in the twentieth century were formed to create winning coalitions, while alliances in the nineteenth century were formed to create balancing mechanisms in the classical balance of power sense.

[3] Hard balancing is a strategy designed to maintain the balance of power. It aims to counter the rise of other countries by using their own military and economic power. This often involves increasing military spending, forming alliances and engaging in an arms race (Robert J. Art, *A Grand Strategy for America*, 2003, Ithaca, Cornell University Press).

The two most peaceful periods of the nineteenth century, the period of European harmony of 1816-1848 and the Bismarckian period of 1871-1895, were already characterized by mutual trust between states, and therefore alliances formed during these periods were not perceived as a threat. Therefore, whether an alliance causes a war or not is also related to the period in which it was formed.

The balance of power established by the Russia-China duo against the US-UK-France triumvirate in the Syrian Civil War prevents the dominance of one side in the region and war between the parties. In conclusion, Vasquez (2015) argues that alliances can be part of a comprehensive and functioning peace system when they are used not as a means to increase power but as a means to constrain unilateral behavior and encourage states to abide by the rules of the game. Based on all the above arguments and examples, it can be concluded that alliances are a shield of war. In other words, the existence of an alliance is an important obstacle to war.

### **III. Alliances as “A Road to War”: A Liberal Perspective**

According to liberals, wars are not caused by the anarchic structure of the international system, but on the contrary by states' misperception of each other. Therefore, liberals argue that an alliance established in the international system will be misunderstood and will lead to the formation of counter-alliances by escalating the competitive environment. It is argued that there is a general tendency in the literature that “Alliances neither prevent war nor promote peace, but rather are linked to war”. Gibler argues that alliances that threaten the security of another state will neither prevent war nor promote ‘peace through strength’ as realists expect, but rather increase mistrust (Vasquez, 2009).

The liberals' claim coincides with the findings of a study conducted by Singer and Small in 1966, which examined the alliance and war behavior of states from 1815 to 1945. In this study, it was concluded that states with high levels of alliance activity also ranked high in terms of the amount of wars they fought, while states with low levels of alliance formation had low levels of involvement in war. Levy (1981) reached a similar conclusion in his study and found that the majority of alliances (56 to 100 percent depending on the type) resulted in a war involving at least one of the allies within five years of their formation. Moreover, Levy's finding that ‘great power’ alliances are more likely to lead to war than other alliances suggests that alliances involving large states are more prone to war than other alliances.

Ostrom and Hoole (1978) argue that there is usually a time lag between the alliance and the outbreak of war, so that the alliance does not directly cause the war, but nevertheless helps to worsen the situation that increases the likelihood of

war. The First World War is a classic example of this. Because every step taken to increase security was perceived as an increasing threat by the other competitor. In this competitive environment, every alliance was perceived as nothing but a threat, and counter-alliances were formed as the most obvious (and appropriate) response to this threat. The counter-alliance offsets most, if not all, of the capability advantages created by the initial alliance. This eliminates the possibility of alliances functioning as a kind of preventive (or deterrent) against wars with an overwhelming concentration of power (Dean and Vasquez, 1976; Wallece, 1973). As a result, alliances not only better prepare the parties, but also draw states into the war and cause it to escalate and spread. This both prolongs the duration and increases the destructiveness of war (Vasquez, 2009). Based on all the above arguments and examples, it can be concluded that alliances have a war-promoting feature in that they involve all members in war. In other words, rather than preventing war, the existence of an alliance increases the risk of war and expands the scope of an existing war.

Among the findings of the same study by Singer and Small (1966) is the statistical evidence that alliances make wars more deadly and longer. The data obtained through the study shows that there is a consistent correlation between being at the top levels of defense pacts, being at the top in terms of battle casualties, and the length of the war. Similarly, the longer a country stays in an alliance, the higher its combat losses and the number of years of war. These links are even stronger for pre-war alliances. Another study supporting the conclusion that alliances function to spread wars was conducted by Randolph Siverson and Joel King in 1979. They concluded that a war between two states that have not joined alliances is much less likely to spread than a war between two states that have joined alliances.

#### **IV. NATO's Deterrence from the Balance of Power Theory Perspective: A Comparative Analysis with the SCO**

After the Second World War, the European states needed an alliance in order to recover more quickly in economic, military and security matters. The USSR, which both left the war strong and geographically close to the region, accelerated the process of rebuilding the disrupted balance of power of the European continent. Therefore, the North Atlantic Treaty was signed in Washington DC on April 4, 1949 with the addition of the USA, Canada, Iceland, Norway, Denmark, Portugal and Italy to the signatories of the Brussels Treaty, and the North Atlantic Treaty Organization (NATO) was established in order to provide common defense against an attack from any external power (NATO, 2023).

At the time of NATO's creation, four main objectives were intended to be fulfilled. The first goal and the main objective was to signal the creation of a collective defense against the perceived threat of the USSR. The second was for the countries of Western Europe to take responsibility for their own security and to take back responsibility for their own security. NATO's third objective is the creation of a strong, broad society based on democratic principles, individual freedom and the rule of law, thereby creating a peaceful international community. The fourth is to create the institutional structures that will enable these objectives to be fulfilled. NATO is important both as a security belt for Western Europe and as a means for the United States to fulfill its own foreign policy objectives. The security system policy that the US tried to implement was to encircle the USSR against the threat of the USSR and communism in a 20,000-mile circle starting from Europe (Tezcan, 2012).

The Warsaw Pact, officially the Treaty of Friendship, Cooperation and Mutual Assistance, was a military alliance established on May 14, 1955 to counter the NATO threat. However, with the collapse of the Soviet Union in 1991, the pact came to an end. The dissolution of the USSR and the disappearance of the Soviet threat made NATO's existence questionable and therefore NATO changed its mission and vision, adopting a "where there is a threat, NATO is there" approach. One of the formations established as an alternative to this unipolar order of the US is the Shanghai Cooperation Organization. Because the similar problems experienced by the states that left the USSR led them to act jointly in foreign policy. Although it has differences, this new organization has become a kind of a different version of the Warsaw Pact and aimed to establish a balance of power in Asia this time against NATO.

On April 26, 1996, the Shanghai Five was formed by the Russian Federation, the People's Republic of China, Kazakhstan, Kyrgyzstan and Tajikistan and was renamed the Shanghai Cooperation Organization after Uzbekistan joined the organization at the 2001 summit meeting (Çelik, 2016). In recent years, the rise of China in the Asian region, both economically and militarily, and the desire of the United States, Russia and China to dominate the region's underground resources have pushed the states of the region to regional integration and brought common security interests and policies to the agenda. The reason for the establishment of the Shanghai Cooperation Organization is based on this background. The desire to take a common stance against the United States is the most important factor pushing Russia and China to cooperate (Eren, 2017). Russia sees NATO's expansion into Eastern Europe and the Black Sea basin as a threat, while China is uncomfortable with the US's pressure and criticism on human rights, its arms trade with Taiwan and its actions in the South China Sea (Harada, 1997).

Turkestan states, which are squeezed between Russia and China, have chosen to conduct their relations with these two states through the element of balance in order to maintain their existence. The Turkestan states' participation in the SCO is a result of these historical balancing policies. After September 11, 2001, with the US invasion of Afghanistan, the US factor emerged as a third factor in addition to the dominant position of Russia and China in Central Asia (Çolakoğlu, 2004).

In 1998, at the third Summit of Heads of State of the Organization in Almaty, Kazakhstan, it was decided to establish an anti-terrorist center in Bishkek, Kyrgyzstan. However, this counterterrorism center was transferred to Uzbekistan by the decision taken at the Tashkent summit on June 17, 2004 on the grounds that it was a move against the United States, and the bases of Khanabad in Uzbekistan and Manas in Kyrgyzstan, which were under the use of the United States, were closed upon the call of the Organization. In addition, the members of the organization, which convened in Dushanbe in 2008, discussed the South Ossetia conflict between Russia and Georgia, and the members stated that they were in favor of Russia at the summit (Eren, 2017). For China, the organization is a tool to increase its influence (Özdaşlı, 2012), while for Russia, it is a mechanism that ensures that the contacts between the breakaway Turkic Republics and China take place under its control (Andican, 2006). In addition, China is also trying to prevent interference in its dispute with Taiwan through its SCO power (Eren, 2017).

While the organization aims to restrict US military freedom of action in the Asia-Pacific, the main US suspicion of the SCO is its military power. Although both Russia and China have stated that the SCO is not a military bloc, the Peace Exercise in the Ural Mountains in 2007 and the Peace Mission exercises in 2012 and 2016, following the drills conducted after 2003, have made the US and NATO cautious (Eren, 2017). Therefore, the US, which has made regional alliances against the Shanghai Cooperation Organization with states such as Australia, the Philippines, Japan, Taiwan, Vietnam, New Zealand, South Korea and Thailand, is trying to increase its power in the Pacific by trying to attract India and Indonesia to its side (Deniz, 2013). On the other hand, Türkiye, a NATO member, became a dialogue partner of the SCO in 2013, following its application in 2011. The President of the Republic of Türkiye, Recep Tayyip Erdoğan, has stated that Türkiye's application for full membership to the EU could be withdrawn in exchange for Türkiye's acceptance as a member of the Shanghai Cooperation Organization. Can Baydarol, Vice President of the European Union and Global Studies Association, stated that the SCO is more about politics than economics and that the organization is an alternative to NATO, not the EU (Erem, 2022). Reasons such as the increase in the cultural and military activities of the organization, the shift of the focus of attention of NATO member countries towards the SCO, and the rising power of China are seen as threats by the US and NATO.



This threat perception between the SCO and NATO can be characterized as soft tension. The fact that there has not yet been a hot conflict between the parties disproves the thesis that alliances lead to war. Moreover, NATO's presence creates deterrence for the SCO and the SCO's presence creates deterrence for NATO.

In international relations, deterrence is the prevention of a possible action of an opponent through words or deeds. It is divided into two categories: deterrence by denial and deterrence by punishment. Deterrence by punishment is to keep alive the possibility of making the aggressor regret their actions by retaliating with nuclear weapons in the event of an attack. As the name suggests, the possibility of punishment creates fear in the enemy and prevents him from attacking. Defensive deterrence, on the other hand, is based on a different logic. Here, it is essential to convince the enemy that if it attacks, the cost of occupation will be as high as possible and that it will not be able to achieve its objectives on the ground. In other words, it is aimed to prevent the enemy from attacking by pushing him to make rational calculations (İlhan, 2023; Adamsky, 2018).

Wayman (1985) found that alliance polarization increased just before the Korean War. One of these alliances, and the most important one, is NATO. Although the establishment of NATO did not directly cause the Korean War, it is the biggest example of how an alliance can lead to war (Jones, 1955). Because the US and its allies were involved in the war when they had not planned to be. Türkiye sent troops to the Korean War in order to become a member of NATO, which joined the war in order to prevent a balance of power that the USSR could establish in the Asian region to the detriment of NATO, that is, America. In this context, while NATO was involved in the war with all its members, it also caused a party that wanted to be a member of the alliance to join the war. With NATO's participation, the war spread to more areas and the destructive power of the war increased. It also led to the formation of a counter-alliance-the Warsaw Pact in 1955. So, the link between the Korean War and NATO confirms the liberal thesis.

On the other hand, the idea that NATO was established not to get involved in a war but to prevent one (Huntley, 1969) confirms the realist view that alliances prevent war through deterrence. According to this idea, the existence of NATO means the absence of war. In other words, NATO, which was established against the threat of the USSR, reduced the risk of possible war by creating a balance of power. Thus, it is possible to explain the realists' argument that alliances reduce uncertainty and thus reduce the risk of war through NATO.

The deterrence umbrella that NATO provides to its members is based on punitive deterrence.

This deterrence, which finds its meaning in the famous fifth article of the alliance treaty, lies in the commitment of the entire alliance to respond militarily in the event of an attack on one of the member states (İlhan, 2023).

If we analyze the thesis of the liberal perspective that alliances cause war by spreading conflicts, again through NATO's fifth article, according to this article (NATO, 2008):

"The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

Since an attack on Europe or North America is deemed to be an attack on all members and the threat can be responded to collectively by acting in accordance with Article 51 of the UN Charter (inhak.adalet.gov.tr, 2023), which envisages the entire alliance going to war, this article increases the risk of war and spreads conflicts. This article was applied for the first and only time in NATO history for the September 11 attacks, and NATO troops were deployed to Afghanistan in the aftermath of these attacks. While this is a direct example of the liberal thesis, the fact that the article has only been used once raises questions. However, the realists' thesis is also justified in this regard, as the existence of the article continues to maintain its importance as the most important deterrence factor. This is because member states are reluctant to use this article. Their reluctance also harms the deterrent effect of the article. Thus, Russia, in particular, will not hesitate to resort to more violence when it feels the threat against it diminishing.

"The Wales Summit, which is considered as a turning point for the "New NATO", was convened on September 04-05, 2014 under the shadow of the Ukraine Crisis and a Readiness Action Plan was prepared at the Summit, which also included recommendations for Russia's aggressive actions against Ukraine. Assurance Measures, which include support for allies under imminent threat, and Adaptation Measures, which envisage long-term and structural changes, laid the foundations of the New NATO (NATO Summit in Wales, 2014).

At their meeting on 10 February 2016, NATO Defense Ministers decided to deploy troops in Eastern European countries on a rotational basis. At the meeting, the message was conveyed that the troops to be deployed would be a multinational contingent, so that an attack on allies would be considered as an attack on all allies (Oğuz, 2016), again referring to Article 5.

Despite their good relations with the Western Bloc during the Cold War, neither Finland nor Sweden became a member of NATO. After the Cold War, they joined the European Union (EU) in 1995 but did not participate in NATO's enlargement policy. Therefore, the Finnish Prime Minister, who stated that a possible NATO membership was unlikely, accelerated the steps to apply for membership after Russia's invasion of Ukraine. Following this perceived Russian threat, both countries officially applied to become NATO allies on May 18, 2022. NATO-Russia tensions centered on Ukraine have led to a new balancing act in the region. The reason for Sweden and Finland's attempts to become allies is to deter the Russian threat through NATO's presence and reduce the risk of attack.

The Russia-Ukraine crisis has led NATO's deterrence capability to regain momentum. For the alliance, which has recently focused on non-military issues such as partnership rather than military issues due to declining threats from Russia and good relations with Russia, the crisis (Young, 2014) reminded the alliance of the need to refocus on military measures. This transformation from partnership to competition has forced NATO to take measures to reassure the populations of member states and to deter Russia from further moves that could threaten the territorial integrity of the alliance (Calha, 2015). The activities of NATO's Standing Naval Forces (SNF), which patrol the Black Sea on a rotational basis, have been intensified in the Black Sea (Erol, 2012), and the allies have concluded bilateral agreements outside the scope of NATO to send troops and weapons to countries in the region for exercises and training (Harper, 2014). What is also important is the massive aid provided to Ukraine by NATO members. NATO solidarity is demonstrated to Russia through NATO's and member states' individual or group exercises in Eastern Europe and the aid provided to Ukraine (Oğuz, 2016).

The United States provided the largest aid to Ukraine. Looking at other NATO members: Greece, two C-130 military transport planes to Ukraine at the beginning of the war; Sweden, 8 military aid packages totaling 3 billion Swedish crowns (\$287 million); Luxembourg, 75 million euros worth of military aid; Denmark, 2,700 shoulder-fired anti-tank weapons, 2,000 bulletproof vests and 700 cleaning kits totaling \$117 million; Belgium, 200 M72 LAW anti-tank weapons and 5 thousand FN FNC assault rifles, totaling 57 million Euros (Euronews & AA, 2023) and Türkiye, Bayraktar TB2 UCAV and TRLG-230 Surface-to-Surface Missile System, BMC KIRPI Mine and Ambush Resistant (MRAP) Vehicle (Özbek, 2023).

The "Deterrence with Custody" activities, which include Gray Zone Conflicts, Social Resilience and the Forward Presence of military units that will prevent the occupation of Alliance territory to a limited extent, were generally developed against Russia's "New Generation War" doctrine, but the new NATO concept,

which was developed mainly on “Deterrence with Punishment”, has become an important tool in the Alliance’s defense and deterrence policies (Biçer, 2022). Especially since 2014, NATO has transformed into a security organization based entirely on deterrence. There is growing interest and focus on classical NATO defense and deterrence, including force planning, exercises and command structure (Henning, 2020).

By invading Ukraine, Russia has demonstrated that it can use proxies, resort to non-state actors, turn Russian expatriates into voluntary quasi-military forces and engage mercenaries, all of which can be used to threaten or attack many of NATO’s European allies and other countries in Russia’s sphere of interest. Russia has also demonstrated how it can use its political, military and economic power in Syria, how it can wage irregular warfare in Georgia and Ukraine, and how it can engage and develop ties even with extremist groups such as the Taliban, which has regained power in Afghanistan (Cordesman, 2017).

The recent events in Ukraine have shown that NATO and the principle of collective defense remain important, but a greater willingness on the part of European Alliance members to share their contributions fairly would help the Alliance to maintain its unity and strength. Because the United States is more preoccupied with Asia (Trine Flockhart etc. 2014). This reduces the Russian threat to NATO and gives Russia more room for maneuver in Eastern Europe. All member states need to be equally willing and able to reflect the Russian threat. Given the threats in a changing and evolving security environment and the Alliance’s right to self-defense, the NATO Alliance’s actions, defensive in nature, proportionate and consistent with international commitments, continue to be non-proliferation, disarmament, arms control and full adherence to confidence and confidence-building measures to enhance security and reduce military tensions. Deterrence, i.e. preventing conflict and war, is a fundamental element of NATO’s overall strategy to fulfill this major responsibility (Biçer, 2022).

At the 15th Summit of the Heads of State of the Shanghai Cooperation Organization held in Ufa, Russia between 8-10 July 2015, the full membership process and procedures of India and Pakistan were initiated. In order to prevent the disputes between India and Pakistan from harming the common policies of the SCO, the “Good Neighbor Agreement” was imposed on the two countries (Eren, 2017). With this defensive deterrent role, the alliance provides evidence for the realists’ thesis by attempting to soften the existing crisis between the two countries. Also, along with founding members such as Russia and China, the full membership of India, the largest state in South Asia, has added a different dimension to the Shanghai Cooperation Organization.

It is seen that this situation has made the Organization a center of attraction. In particular, Iran, which was subjected to US-based Western sanctions, turned its direction to the east, and the country became a full member of the Organization at the 21st SCO Summit held in Dushanbe, the capital of Tajikistan, on 16-17 September 2021 (Güven, 2021). Iran has become a full member of the Shanghai Cooperation Organization, despite the UN embargo that countries under the UN embargo cannot become members of the organization. This means that the Organization views the sanctions against Iran as unilateral rather than international.

The Shanghai Cooperation Organization, which has set itself the task of combating the three main and non-traditional security threats of terrorism, separatism and extremism, will serve two purposes in combating these threats are: First, it would give international legitimacy to the constituent states facing problems such as terrorism, separatism and extremism in their fight against these threats. Thus, Russia would be able to act more easily in its war in Chechnya, China in its activities in the Uighur region, Uzbekistan against the radical religious organizations it had to fight against within the country, as well as in the suppression of dissent. In addition, smaller countries like Tajikistan and Kyrgyzstan would have the support of big powers like Russia and China in combating these threats. Secondly, the founding powers of the organization tried to produce an alternative model to the American model of combating international terrorism through the cooperation mechanism within the framework of the Shanghai Cooperation Organization. It was aimed to prevent extra-regional interventions in the solution of intra-regional problems and to realize the solution within the framework of regional cooperation (Kosaçyov, 2003).

In 2001, after its intervention in Afghanistan, the US strengthened its security cooperation with all Central Asian countries and gained significant influence with the military bases it established in the region. Russia's influence has weakened. Then, the wave of "color revolutions" that started in Georgia in 2003, allegedly financed and organized by the US State Department and the CIA, extended to Central Asia (Komissina, 2016) and escalated the geopolitical struggle over the region between Russia and China on the one hand and the US on the other. In order to emerge successfully from this struggle, the members of the Shanghai Cooperation Organization have cooperated more intensively within the framework of the organization to ensure intra-regional stability. This led to the strengthening of the Shanghai Cooperation Organization (Askeroğlu, 2018). The Shanghai Cooperation Organization, which was established to solve border problems between member states, has begun to turn into a balancing factor against the emerging US dominance in the region.

Although the Shanghai Cooperation Organization lacks a collective defense mechanism, as in Article 5 of NATO or Article 4 of the Collective Security Treaty Organization, member states are ready to take any countermeasures to defend the interests of other member states, as stated in the basic principle of the organization's treaty (Lavrov, 2014). The statement "The Organization is ready to take any countermeasures" is open-ended and establishes the legitimacy for other members to respond to a threat or physical attack against one of the members. Therefore, the invasion of Afghanistan and Iraq in the early 2000s was an important factor that made Tehran, which perceived a security threat from the United States, want to become a member of the Shanghai Cooperation Organization. For the Organization, this membership shows that Iran is the pillar of the Organization in the Middle East. So, "security" has become an important issue within the organization. This geopolitical expansion of the organization creates a deterrent effect against NATO in both economic and security matters. Because, just like NATO, the Shanghai Cooperation Organization acts as a shield against possible foreign interventions against its members. Although it is not a collective defense organization, it is unlikely that a use of force will be used against the Organization and its members since it states that it will defend and protect the interests and security of its members. Moreover, after its establishment, the Organization was referred to as the "NATO of the East" (Mate, 2009) or "NATO's evil twin" (Morozov, 2006). The Organization stands as the largest and most inclusive bloc vis-à-vis NATO for several reasons, including its expansion and Turkey's close contacts with the Organization.

How would Russia be stopped in a world without NATO? The deterrence effect of NATO's Article 5 is one of the most important factors in curbing Russia's actions. This is why Russia is strongly opposed to other states joining the alliance, especially Ukraine and Georgia. On the other hand, how can the US be stopped without SOC against NATO? The structure of the international system is too large and complex to be unipolar. That is why the existence of alliances is always needed. As a result, the existence of an alliance does not cause war, on the contrary, it prevents the spread of war. However, if Russia were to attack a NATO ally, then the entire alliance would be involved in the war and the thesis that alliances spread war would once again triumph. But, Russia will not want to confront the entire alliance. Or, if one of the SOC members were attacked, the organization would be ready to respond. However, it would not be easy to wage war against the SCO, which has two nuclear-powered members.

## **Conclusion**

The balance of power theory is as important for states and the international system today as it was in the past and continues to be preferred.



For this reason, it is still relevant. The fact that states resort to balance of power when they feel insecure has brought along a debate. In the literature, there is a distinction in terms of time, space, actor elements (parties, allies) and the structure of the international system as to whether the alliances established cause war or eliminate the risk of a possible war. This distinction is between realists, who believe that the established balance of power will lead to an environment of peace, and liberals, who argue that the balance will increase the risk of war.

Considering these two different perspectives, it is seen that alliances that increase the risk of war and spread conflicts are formed in an already existing competitive environment. In times of high threat perception, states make alliances in order to balance their power and deter the threat. Therefore, the other side perceives the alliance established in such an international conjuncture as a threat and forms a counter-alliance. This leads to an increase in tensions between the parties and, moreover, the involvement of one ally in the war leads to the involvement of other allies in the war. Thus, as liberals argue, alliances increase the risk of war and even spread war. This can be explained through NATO's Article 5. Because this article seems to formalize the thesis that alliances spread war. This article, which was used in practice for the first time in history with the September 11, 2001 incident, confirms the liberals' thesis.

On the other hand, it is observed that the alliances established due to the harmonization process in the 19th century did not lead to war. Since the states did not perceive any threat in this period, the alliances made did not lead to counter-alliances. In other words, the alliances made in a period when there was no competition and there was a process of peace and harmony remained in the nature of the continuity of peace. In such an environment, the purpose of an alliance is to reduce the risk of war rather than increase it. In other words, since the existence of alliances does not always lead to war, the liberals' thesis contradicts itself at this point.

Realists, on the other hand, argue that alliances contribute to the creation and maintenance of peace. According to them, the balance of power created by the alliance will deter the other side and prevent it from attacking. In the study, the realists' thesis that 'Alliances prevent war' is also analyzed through NATO. "NATO's fifth article". In fact, member states are reluctant to invoke this article due to the heavy cost it would create. Therefore, the focus is on the possibility of using the article rather than its use. The article in question seems to be more functional in deterring an attack by the other side.

This is because an attack on a NATO ally will be met with the entire alliance and will be punished. Therefore, the country considering an attack will have to make its plans taking this condition into account and will have to think in more detail before the attack. This is where the war-preventing side of Article 5 comes into play, rather than the war-promoting side. This article reduces the likelihood of an attack against NATO allied countries. But what will the process be like for non-NATO countries? Having lost its *raison d'être* after the Cold War, NATO has expanded its geographical area and adopted the mission of “Where there is a threat, NATO is there”. This has paved the way for involvement in the resolution of conflicts in non-NATO countries. The most important of these is NATO’s siding with Ukraine in the Russia-Ukraine War.

Russia has always opposed Ukraine’s membership of NATO. If Ukraine was an ally of the alliance, the attack would have been less likely to take place. Russia would have to tread more carefully, as it would not want to confront NATO on the grounds of Article 5. On the other hand, the invasion of Ukraine was also seen as a security issue for Sweden and Finland, and led them to put NATO membership on their agenda to counter the Russian threat. These two countries became closer to NATO than ever before and took initiatives to become part of the alliance. As a result of these initiatives, Finland joined the alliance as the 31st member on April 4, 2023, while Sweden became the 32nd member of NATO with a ceremony held in Washington on March 7, 2024. Based on the membership initiatives of Finland and Sweden, it is seen that NATO’s deterrent effect still continues today, especially during the Cold War period. Thus, the claims put forward by realists are confirmed in this framework.

The Finnish-Swedish example given above, in particular, reveals that today, states try to be a part of the alliance in order to benefit from its deterrent power in the sense of preventing war. In other words, there is a general tendency that states join alliances to avoid war. Because states stay away from a conventional war, especially due to the costs it would create, and instead try to protect NATO’s deterrence by organizing exercises. On the other hand, Central Asian Turkic states have also joined the SCO in order to protect themselves from potential conflicts. As a member of the Shanghai Cooperation Organization, Iran wanted to create a deterrent effect against the Western threat. This aspiration is not dissimilar to the aspirations of Finland and Sweden to join NATO. Therefore, it is possible to say that participation in alliances has effects on states as a stance against war, to eliminate threats or to secure themselves. The tendency that states participate or try to participate in the balance of power to ensure and protect their own interests serves to protect themselves from the risk of war. Due to these approaches of states, the war-preventing aspect of alliances is more prominent.

In conclusion, an overall assessment shows that alliances are both a shield and a cause of war, but that this situation varies depending on the structure of the international conjuncture, and that alliance members predominantly emphasize the deterrent aspect of the alliance in order to avoid a possible war.

In the literature, there is no study that examines the relationship between alliances and wars by comparing realist and liberal perspectives and arguments and examines it in the specific case of NATO-SCO. Studies examining the relationship between alliances and wars are quite old. However, the Russia-Ukraine war has shown that alliance membership remains the most effective way to deter war. At this point, the need for NATO's existence has once again become clear. Moreover, it was Russia, which was uncomfortable with the alliance, that brought this need back to the agenda. Therefore, this study reveals that understanding and further studying the relationship between alliances and wars is of utmost importance for the measures to be taken and policies to be developed.

The Russia-Ukraine, Russia-Crimea and Russia-Georgia crises have brought to light the fact that NATO must continue to maintain the deterrent power of its fifth article. In this sense, member states should act in greater unity and solidarity and engage in joint expenditures. The United States, whose interest has shifted more and more towards Asia, needs to make its presence felt more in NATO. The Ukraine War has done this to some extent, and the US has been the alliance member that has provided the most assistance to Ukraine. However, NATO's silence on the continent before the war was perhaps the most encouraging factor for Russia.

It is hoped that this study will pioneer future research since there are not enough studies on the subject. The study is a step towards shifting attention to this issue. Examining the relationship between alliances and wars is important in order to analyze more easily how states will behave in times of crisis.

## **Bibliography**

Adamsky, D. (2018). From Moscow with coercion: Russian deterrence theory and strategic culture. *Journal of Strategic Studies*, 41.

Andican, A. (2006). Çin satrancında Orta Asya. *ASAM dergisi Avrasya dosyası*, 12(1), 7-36.

Art, R.J. (2003). A grand strategy for americ. Ithaca, Cornell University Press.

Askeroğlu, S. (2018). Şanghay İşbirliği Örgütü İran'ın güvenlik garantisi olabilir mi? edt.: Umut Başar, İran Araştırmaları Merkezi (İRAM), Ankara.

Biçer, R.S.S. (2022). NATO'nun savunma ve caydırıcılık çalışmaları ile ilgili bir değerlendirme. Güvenlik stratejileri dergisi, 18(42), 323-346.

Calha, Julio Miranda Hybrid Warfare: (2015). NATO's new strategic challenge?, General report for NATO Parliamentary Assembly Defence And Security Committee. 2015 - 166 DSC 15 E BIS - HYBRID WARFARE - CALHA REPORT | NATO PA. (accessed 13 Feb. 2025).

Çelik, İ. (2016). "Şanghay İşbirliği Örgütü ve Çin". <http://www.uiportal.net/sanghay-isbirligi-orgutu-ve-cin.html>. (accessed 13 spt. 2024).

Cobden, R. (1867). The political writings of richard cobden. London: T. Fisher Unwin Press.Cambridge: Cambridge University Press (05.05.2012).

Cordesman, A.H. (2017). NATO and the delicate balance of deterrence: Strategy versus burden sharing. CSIC Center for Startegic & International Studies, 10-12.

Çolakoğlu, S. (2004). Şanghay İşbirliği Örgütü'nün geleceği ve Çin. Uluslararası İlişkiler Dergisi, 1(1), 173-197.

Dalkılıç, L. Savaş ve barış üzerine: bir realizm-idealizm karşılaştırması. pp.1-12.

Dean, P.D & Vasquez, A.J. (1976). From power politics to issue politics: bipolarity and multipolarity in light of a new paradigm. Western political quarterly, 29, 7-28.

Demirel, E. (2019). Güç dengesi teorisi perspektifinden birleşmiş milletler. Bilecik şeyh edebali sosyal bilimler enstitüsü dergisi, 4(2), 575-601.

Deniz, T. (2013). Mekânsal güç Asya'nın siyasi gücü: Şanghay İşbirliği Örgütü. Doğu Coğrafya Dergisi, 18(30), 217-228.

Dinerstein, S.H. (1965). The transformation of alliance systems. American Political Science Review, 59(3), 589-601.

Erem, O. (2022). "Beş soruda Şanghay İşbirliği Örgütü". Şanghay İşbirliği Örgütü: Beş soruda ŞİÖ - BBC News Türkçe. (accessed 08.02.2025).

- Eren, E. (2017). Şanghay İşbirliği Örgütü ve Türk Dış Politikasında gelecek perspektifi. *Strategic public management journal*, 3(5), 77-94.
- Erol, M.S., Demir, S. (2012). Amerika'nın Karadeniz politikasını yeniden değerlendirmek. *Gazi Akademik Bakış*, 6(11), 17-33.
- Euronews & AA. "Batılı ülkeler Ukrayna'ya ne kadar askeri destekte bulundu? Hangi silahlar gönderildi?" 10 Jan. 2023, (accessed 09.02.2025).
- Flockhart, T., etc. (2014). *Liberal order in a post-Western World*, Transatlantic Academy. Washington DC.
- Fearon, D.J. (1997). Signaling foreign policy interests: tying hands versus sinking costs. *Journal of conflict resolution*, 41(1): 68-90.
- Fedder, E. (1968). The concept of alliance. *International studies quarterly*, 12(1): 65-86.
- Gibler, M.D. (1996). Alliances that never balance: the territorial settlement treaty. *Conflict management and peace science*, 1, 75-97.
- Güven, A. (2021). "İran'ın ŞİÖ üyeliği: Beklentiler ve muhtemel senaryolar". İran Araştırmaları Merkezi (İRAM), İran'ın ŞİÖ Üyeliği: Beklentiler ve Muhtemel Senaryolar - İRAM Center | İran Araştırmaları Merkezi, (accessed 18.05.2025).
- Haas, B.E. (1953). The balance of power: prescription, concept, or propaganda? *World politics*, 5(4), 442-477.
- Harada, C. (1997). *Russia and North-East Asia*. International Institute for Strategic Studies, Adelphi Paper, Issue 310.
- Harper, J. (13 August 2014). 1st cavalry soldiers headed to Poland, Baltics. *Stars and Stripes*. (accessed 14 Oct. 2024).
- Henning, F.A. (2020). *Hybrid Deterrence*. Norwegian Institute for Defence Studies. [IFS Insight 1\\_2020\\_oppdateret.pdf](#). (accessed 11 Feb. 2025).
- Herz, J. (1951). *Political realism and political idealism: A study in theories and realities*. Chicago, Chicago University Press.
- Huntley, R.J. (1969). *NATO hikayesi*. Ankara, Yarı Yayınları.

- İlhan, B. (4 Agst. 2023). "Avrupa'da caydırıcılığın geleceği ve NATO". Avrupa'da Caydırıcılığın Geleceği ve NATO | TAV. (accessed 08 Feb. 2025).
- Jones, M.J. (1955). The fifteen weeks. New York, Harcourt, Brace and World.
- Kaplan, A.M. (1969). Variants on six models of the international system, international politics and foreign policy, ed. James N. Rosenau. New York, The Free Press.
- Komissina, İ. (2016). Razmışleniya posle sammita ŞOS: Noniye realii, no viye perspektivi. Problemy Natsionalnoy Strategii, 1(34), s. 69.
- Kosaçyov, K. (Spt. 29, 2003). "ŞOS Kak Alternativa Amerikanskomu Vliyaniyu v TsA", Nezavisimaya Gazeta.
- Lavrov, S. (Stp. 10, 2014). "Sekret ŞOS", Rossiyskaya Gazeta.
- Little, R. (2007). The balance of power in international relations: metaphors, myths and models, Cambridge University Press, New York.
- Leeds, A.B. (2003). Alliance reliability in times of war: explaining state decisions to violate treaties. International organization, 57(4), 801-827.
- Levy, S.J. (1981). Alliance formation and war behaviour: an analysis of the great powers, 1495-1975. Journal of Conflict Resolution, 25, 581-613.
- Mate, R. (2009), "NATO of the East?: An international relations analysis of the Shanghai Cooperation Organization", Midwest Political Science Association 67th Annual National Conference, The Palmer House Hilton, Chicago, IL, Internet [http://citation.allacademic.com/meta/p363868\\_index.html](http://citation.allacademic.com/meta/p363868_index.html), (accessed 18.05.2025).
- McGowan J.P. & Robert M.R. (1975). Alliance behavior in balance of power systems-applying a poisson model to nineteenth-century europe. American political science review, 69(3), 859-870.
- Mearsheimer, J.J. (2001). The tragedy of great power politics. New York and London, W.W. Norton.
- Morgenthau, J.H. (1948). Politics among nations: the struggle for power and peace. New York, Alfred A. Knopf.



Morozov, E. (June 8, 2006) "NATO's evil twin?", TCS Daily, <http://www.tcsdaily.com/article.aspx?id=060806A>, (accessed 18.05.2025).

Morrow, D.J. (1994). Alliances, credibility, and peacetime costs. *Journal of conflict resolution*, 38(2), 270-97.

North Atlantic Treaty Organization (NATO). (1949). [https://www.nato.int/cps/fr/natohq/official\\_texts\\_17120.htm?selectedLocale=tr](https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=tr) (accessed 17.11.2023).

North Atlantic Treaty Organization (NATO). (Dec. 9, 2008). [https://www.nato.int/cps/fr/natohq/official\\_texts\\_17120.htm?selectedLocale=tr](https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=tr), (accessed 17.11.2023).

Sheehan, M. (1996). *The balance of power: history and theory*. London, Routledge.  
NATO, "Wales Summit Declaration", 5 September 2014,

Oğuz, Ş. (2016). Ukrayna krizi ve yeni NATO. *Karadeniz Araştırmaları Balkan, Kafkas, Doğu Avrupa ve Anadolu İncelemeleri Dergisi*, 51, 207-221.

Ostrom, W.C. & Hoole W.F. (1978). Alliances and war revisited: A research note. *International studies quarterly*, 22(2), 215-236.

Özdaşlı, E. (2012). Çin ve Rusya Federasyonu'nun Perspektifinden Şanghay İşbirliği Örgütü. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 4(6), 108-122.

Pradt, A. (1815). *Du congres de vienne*, Paris.

Schroeder, W.P. (1976). Alliances, 1815-1945: Weapons of Power and Tools of Management, ed. Karl Knorr. *Historical Dimensions of National Security Problems*, Lawrence, University Press of Kansas: 227-62.

Snyder, H.G. (1997). *Alliance politics*. Ithaca, N.Y., Cornell University Press.

Smith, A. (1998). Extended deterrence and alliance formation. *International interactions*, 24(4), 315-343.

Singer, J.D. & Small, M. (1966). National alliances commitments and war involvement, 1815-1945. *Peace research society (international) papers*, 5, 109-40.

Siverson, M.R. & King, J. (1979). Alliances and the expansion of war, ed. Joseph D. Singer and Michael Wallace. To Augur Well, Beverly Hills, Sage: 37-39.

Tezcan, E.İ. (2012). 21. yüzyılda NATO (Master's thesis, Sosyal Bilimler Enstitüsü). Tolgaozbek.com, "Türkiye'nin Ukrayna'ya gönderdiği KİRPİ'lerindeki kuleler kimin?", Türkiye'nin Ukrayna'ya gönderdiği KİRPİ'lerindeki kuleler kimin? – Tolga Özbek, (accessed 09.02.2025).

United Nations. (1945). United Nations Agreement.  
[https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm\\_01.pdf](https://inhak.adalet.gov.tr/Resimler/SayfaDokuman/2212020141836bm_01.pdf)  
(accessed 17 Nov. 2023).

Wallace, D.M. (1973). Alliance polarization, cross-cutting and international war, 1815 1964. Journal of conflict resolution, 17(4), 575-604.

Wallace, D.M. (1985). Polarization: towards a scientific conception, ed. Alfred Sabrosky. Polarity and War, Boulder, Colo, Westview: 95-113.

Walt, M.S. (1985). Alliance formation and the balance of world power. International security, 9(4), 3-43.

Walt, M.S. (1987). The origins of alliances. Ithaca, Cornell University Press.

Walt, M.S. (1988). Testing theories of alliance formation: The case of Southwest Asia. International organization, 42(2), 275-316.

Waltz, N.K. (1979). Theory of international politics. Massachusetts, Addison-Wesley.

Wayman, W.F. (1985). Bipolarity, multipolarity and the threat of war, ed. Alfred Nobles Sabrosky. Polarity and War, Boulder, Colo, Westview: 115-44.

Wayman, W.F. (1990). Alliances and war: A time-series analysis, ed. Carl Gochman and Alfred Nobled Sabrosky. Prisoners of War, Lexington, Mass, Lexington Books: 93-113.

Vasquez, A.J. (2009). Savaş bulmacası, yeniden, trans. Haluk Özdemir 1. Basım/2015. İstanbul, Uluslararası İlişkiler Kütüphanesi.

Young, de K. (19 March 2014). Russia's movesin Ukraine are'Wake-up Call', NATO's Rasmussen says in Speech, The Washington Post.

Zinnes, A.D. (1967). An analytical study of the balance of power theories. Journal of peace research, 4(3), 270-287.