Central European Journal of International and Security Studies
On-line first

DOI: 10.51870/ILUJ7632
Research article

The Institutionalisation of Security Norms in the Context of Cyber Alignments: The Transatlantic Alignment in the Cyber Domain

Mahmoud Hosh
Damascus University, Syria, ORCiD: 0009-0000-8677-1452, corresponding address: mahmoud.housh@damascusuniversity.edu.sy

Numeir Issa
Damascus University, Syria, corresponding address:
numeir.issa@damascusuniversity.edu.sy

Abstract

Realists argue that security alliances are established to confront military threats posed by one state to others. In contrast, this study argues that nonmilitary cyberthreats have become a factor in establishing new security arrangements that do not necessarily take the form of an alliance, but rather emerge in the form of alignments. Cyberthreats lie in the political, economic, societal and military repercussions caused by the employment of cyber technologies, not these technologies themselves. Therefore, alignments are not automatic reflections of cyber capabilities, but depend on common perceptions and meanings that identify a certain behaviour as a security threat. The transatlantic alignment in the cyber domain, having been produced by common EU and US cyber norms, represents this type of security alignment. These norms have constructed common meanings and perceptions of cyberthreat patterns, which are primarily embodied in Chinese and Russian policies and behaviour in the cyber domain, involving a set of alternative and competing norms to those adopted by the former two, and through which China and Russia seek to alter the structure of the prevailing international order.

© 2024 Author/s. Article is distributed under Open Access licence: Attribution – NonCommercial 4.0 Unported (cc by-nc 4.0).

***Keywords**: cyberthreats, security alignments, transatlantic alignment, cyber norms, international order*

First published online on 29 February 2024

Introduction

Security alliances are studied through the realist theory, especially the 'alliance theory' presented by Snyder (1990), as a formal grouping of states for the purpose of employing (or not employing) military power, one which is designated for either security or maximising the influence of its members against nonmember states. Alliances achieve alignment among members, which organises their mutual expectations with respect to behaviours that ought to be taken by one member to support other members in times of conflict or war with nonmember states, and their ultimate end is to achieve security against enemies.

The realist emphasis on the military nature of threats that prompts states to establish security alliances has made alliances appear as if they automatically reflect the balance of powers between major states. Mearsheimer (2001) views alliances as a tool of maintaining state power, and since neorealism focuses on the structure of the international system as a unit-of-analysis of international interactions (Waltz 1979), alliances become the primary means of maintaining state power under an international system lacking a high authority (Jones 1999).

This study differs with the realist theory in dealing with the subjects of security arrangements, the mechanism of their establishment, and the patterns of threat they confront. First, alliances are not the only form of security arrangements between states, which, instead, emerge in several forms, such as security complexes (Buzan & Waever 2003), alignments (Miller & Toritsyn 2005), coalitions (Pierre 2002) and strategic partnerships (Kay 2000). Even though these patterns (including alliances) are established to confront a certain threat, no threat exists without the prior existence of a vision that deems a phenomenon or issue a security threat in the first place, indicating that perceptions and meanings applied to phenomena are in effect what leads to viewing issues as security threats. Constructivists, such as Wendt (1992), express this perspective. Wendt argues that the meanings and perceptions states adopt of the capabilities of one another are the deciding factor in determining whether or not the behaviour of any one state poses a security threat. Similar views are also expressed by Buzan, Weaver and de Wilde (1998), referring to the 'securitisation of phenomena' as caused by perceptions that view an ordinary issue as one of existential threat.

Security alignments arise only when a group of states have similar threat perceptions towards a phenomenon or behaviour that represents a security threat. Such a similarity of perceptions is produced by a number of factors discussed by constructivists; Rousseau and Retamero (2007) view identity as the deciding factor in having common threat perceptions, since it represents the border line between one group and another. In a different context, Retamero, Müller and Rousseau (2012) argue that both divergence and convergence of values greatly influence the extent to which the economic and military behaviour of other actors or states is perceived as a threat. Additionally, there is an approach, represented by Farrell (2002), that focuses on the role of norms in shaping similar threat perceptions among several actors. Farrell holds the view that norms adopted by an actor shape the meanings of the actions of others with respect to whether or not they are suitable, and hence whether or not they pose a threat, which essentially relies on their accordance or conflict with social roles and the social environment. This relevance of norms in identifying security threat situations stems from the fact that norms are the desired behaviours to states through which their perceptions, ends and the instruments to achieve these ends are shaped (Florini 1996), and are also the fundamental rule in shaping state interests (Walling 2013). The more divergent the norms, the more divergent the ideas and ideologies, and hence the more intense the conflict of interests, leading to the emergence of mutual threat perceptions (Hass 2005). Moreover, norms determine which power instruments are best suited for dealing with perceived threats; Finnemore (2004) explains that the various instruments employed in confronting threats differ according to social purposes, which determine the benefit of these instruments by increasing their legitimacy, i.e., through aligning them with social norms.

Second, given that the nature of threats is identified through perceptions and meanings applied to ordinary issues, consequently viewing them as existential threats, then not only military issues are the subject of security studies, which now involve subjects as diverse as threat perceptions, ranging from societal risks embodied in identity clash (Posen 1993) to economic risks caused by basic-resources dependence (Cable 1995). This relative difference between states in identifying security issues is due to differences in their visions and valuations of the most significant issues that pose an existential threat, which necessitates the inclusion of nonmilitary elements. The Copenhagen School responds to such necessity by introducing the concept of 'expanded security' and including the political, economic, military, societal and environmental sectors as subjects of security studies (Buzan & Hansen 2009) and, at a later stage, by including cyberthreats (Hansen & Nissenbaum 2009). These diverse threat patterns are currently being employed in competition between major powers and represent the line between war and peace, and in dealing with such diverse patterns, states resort to, inter alia, security alignments (Monaghan 2022).

Third, this study differs with the realist focus on the structure of the international system as the primary unit-of-analysis in explaining the establishment of security alliances. Realism argues that states seek to maximise gains in the international system and maintain the balance of powers to their interests through alliances.

However, this argument fails to explain the establishment of security alignments in confrontation of nonmilitary threats, especially cyberthreats, since a state posing this type of threat in its behaviour does not directly influence the balance of powers in the international system. These 'hyper threats', as termed by Monaghan (2022), are aimed at threatening, circumventing and sabotaging the rules and norms on which international interactions are based. Therefore, the level of analysis through which it becomes possible to analyse the rationale behind the establishment of security alignments in confrontation of such threats is the level of the international order, which refers to the set of norms, values and institutions governing mutual interactions between major actors in the international system (Mazarr et al. 2016). In this sense, the ultimate purpose of state-grouping in security partnerships becomes the preservation of the prevailing international order, designed to serve and promote their interests in the international system.

The presented differences with the realist approach raise a major question that constitutes the focus of this study: what are the factors that led the US and EU to assume that the behaviour of China and Russia in the cyber domain poses a security threat, despite the fact that cybertechnologies do not in and of themselves pose security threats? This study argues that common, transatlantic cyber norms have created a common threat perception between the US and EU towards Chinese and Russian behaviour in this domain, since this behaviour is driven by cyber norms that counter those adopted on the transatlantic level. This, in turn, has made the cyber domain into a security threat domain, and prompted the establishment of transatlantic security arrangements. In order to prove this argument, the study relies on the Tracing Model, which establishes causal links between variables of the study and traces them through the studied case. The conflict of cyber norms between the two parties of the Atlantic on one hand, and China and Russia on the other, represents the independent variable, whereas forming the transatlantic alignment in confrontation of perceived cyberthreats constitutes the dependent variable. The links between the two variables can be traced by relying on previous literature, documents, strategies, laws and initiatives of all actors that this study is concerned with, and this shall be achieved by examining several issues: First, the emergence of US and European norms and the values and practices they involve towards the cyber domain. Second is the endeavour to generalise liberal cyber norms on the international level, and the inability to align Russian and Chinese behaviour with the requirements of such norms due to their adoption of counter-norms that incentivise them to put forth initiatives and policies influential to the prevailing international order. Last, it will be achieved by examining the emergence of a common threat perception between states of the Atlantic towards Chinese and Russian behaviour due to a conflict of norms, which prompted the strengthening of Atlantic rapprochement by forming a cyber alignment and overcoming the contentions sparked by the cyber domain.

Perceiving Cyberthreats and Establishing Security Alignments

The influence of cyberthreats on the orientation towards forming security alignments should be analysed by identifying the premonitions that are the basis of perceiving the cyber domain as a security issue. States neither join nor establish alignments unless they perceive that they are facing threats that require collective confrontation alongside other states adopting the same vision. Therefore, special attention must be given to the nature of the elements of the cyber domain, which characterise this domain as either a threat or nonthreat, and to the role of norms in identifying the form of common threat premonitions themselves, hence institutionalising them by transforming them into security alignments.

Cybertechnologies: A State of Threat or Inter-threat

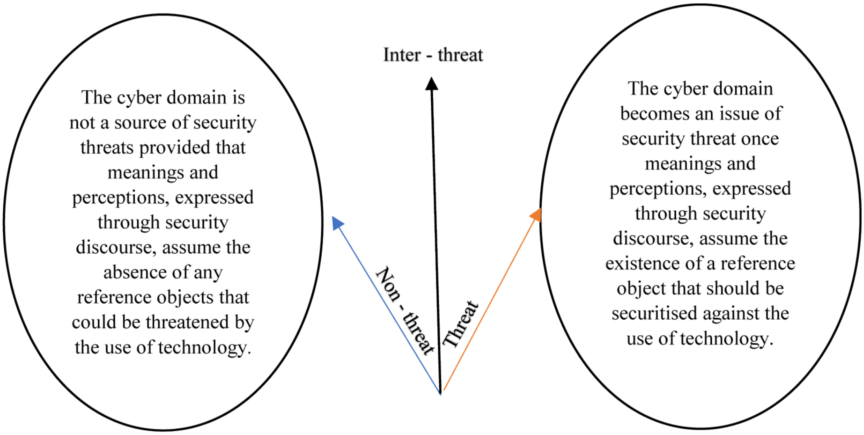
Nissenbaum (2005: 64) defines cybersecurity as the

> threats posed by the use of networked computers as a medium or staging ground for antisocial, disruptive, or dangerous organisations and communications. These include, for example, the websites of various racial and ethnic hate groups, . . . threats of attack on critical societal infrastructures, including utilities, banking, government administration, education, healthcare, manufacturing and communications media. . . . Potential attackers include rogue US nationals, international terrorist organisations, or hostile nations engaging in 'cyber-war'.

It becomes clear from this perspective that cybersecurity is of varying nature and dimensions. In order for security in the cyber sense of the word to exist, there must exist something to securitise against the risks of technology, which Dunn Cavelty (2013) terms 'cybersecurity representations'. This means that cybersecurity subjects vary in response to the variety of actors defining cyberthreats and producing various objects and references of security, which can be observed by analysing security discourse. Therefore, the cyber domain cannot absolutely be considered a security threat, but rather it is an issue of inter-threat, and that is since, in principle, technology itself is not an issue of security threat, and the cyber domain is viewed as one only when perceptions of the political authority assume that there is a reference object exposed to risks due to the misuse of technology.

The cyber domain, as illustrated in Figure 1, is determined whether or not it represents a security issue depending on how it is perceived. Eriksson and Giacomello (2007) argue that this state of threat is related to the meanings and perceptions political authorities apply to technology and communications technologies and on the manner in which they are used. Their analysis concludes that identifying the actors responsible for cyberthreats and the entity that ought to deal with them depends on the contexts and frameworks in which these threats are involved, which, ultimately, reflect the nature of the perceptions and meanings applied to the cyber domain.

Figure 1. An illustrative figure of the manner in which the cyber domain becomes an issue


The cyber domain is not a source of security threats provided that meanings and perceptions, expressed through security discourse, assume the absence of any reference objects that could be threatened by the use of technology.
Inter - threat
Non - threat
Threat
The cyber domain becomes an issue of security threat once meanings and perceptions, expressed through security discourse, assume the existence of a reference object that should be securitised against the use of technology.

Source: Authors

The matter of greatest relevance to this study is the case in which the cyber domain becomes an issue of security threat. Figure 1 illustrates this case. Since the cyber domain is of a neutral nature, these threat patterns emerge and derail it from its neutrality, characterising it as a threat domain, and hence they represent distinct threat patterns. One analysis approach holds that the distinct domain around which perceived threats emanating from the cyber domain centre is related to the idea of 'conflict' in the military sense. Threats, in this sense, are perceived through what Branch (2020) terms 'foundational metaphors', which refers to using the experience of a different phenomenon as a reference to understand the opportunities and threats associated with the cyber domain. This is the case with the US military perspective, which views the cyber domain as a new dimension of conflict alongside the three traditional dimensions (land, sea and air), i.e., the metaphors that established the understanding of this domain as a space of conflict are essentially derived from US military experience in conflict over the three mentioned dimensions. Additionally, there is another approach, e.g., Gomes and Whyte (2021), that deals with malicious activities and attacks negatively impacting infrastructure differently, and that is through the context of their political and social risks. Although such impacts on the political and social structure are limited, the lack of experience in this regard often leads to excessive securitisation of the cyber domain, and makes it into a threat issue involving greater risks than what reality indicates.

This lack of experience is evident in what Lawson (2013) terms 'scenarios of cyber doom', which are the supposed stories that warn of the potential impacts of cyberattacks, especially the supposed concerns about technology escaping human control. Such scenarios contradict what facts relating to cyberattacks indicate, and the capacity of these attacks to impact infrastructure, the economy and society appears to be exaggerated, consequently leading to overly exaggerated policies. Therefore, the process of building scenarios is related to a different process that Dunn Cavelty and Wenger (2019); and Balzacq and Dunn Cavelty (2016) term 'knowledge production', which refers to the specific knowledge forms resulting from the interaction between technical and political impacts. These knowledge forms work to include a certain cyber event in a specific social context, since the technical impacts of malicious cyberactivity are not by themselves sufficient to prove the political relevance of cybersecurity, dictating that there must be a technical matter rhetorically-linked to a different matter that has a social or political value.

Contrary to the two aforementioned approaches, which deal with identifying the threats associated with cyberactivity, there exists a third approach that associates cyberactivity with the threat of penetrating the privacy of computers and communications devices for the purpose of collecting confidential and sensitive information. For instance, Lindsay and Gartzke (2020) hold the view that cyber operations exploit technical vulnerabilities in order to achieve their goals of intelligence gathering (surveillance and espionage), network disruption (sabotage and covert action), or indirect influence (sabotage and disinformation).

It can be concluded that threats emanating from the cyber domain fundamentally revolve around either activity related to military conflict, malicious activity that has political and social impacts, or activity related to espionage and intelligence. Additionally, there is a threat pattern associated with employing the cyber domain in international competition. This pattern is of greater relevance than the former three, since they only emerge after such employment of the cyber domain takes place; the course of events is as follows. First, one state, or states, seeks to develop its technological base, and to own and employ the necessary cybertechnology for the purpose of maximising its political, economic and military gains at the expense of others. Second, a targeted state, or states, perceives or securitises this behaviour. Ultimately, once this behaviour is perceived or securitised, competition between the states in concern arises, and the three aforementioned threat patterns emerge in their mutual relations. Such a perception of competition is related to the degree of convergence or divergence of norms, and that is since norms represent the fundamental standard for explaining the behaviour of others in the cyber domain as to whether or not it represents a threat and competition, and also since they prompt states to follow specific behaviour patterns in confronting the activity of competing states adopting different norms.

Cyber Norms and Shaping a Common Threat Perception

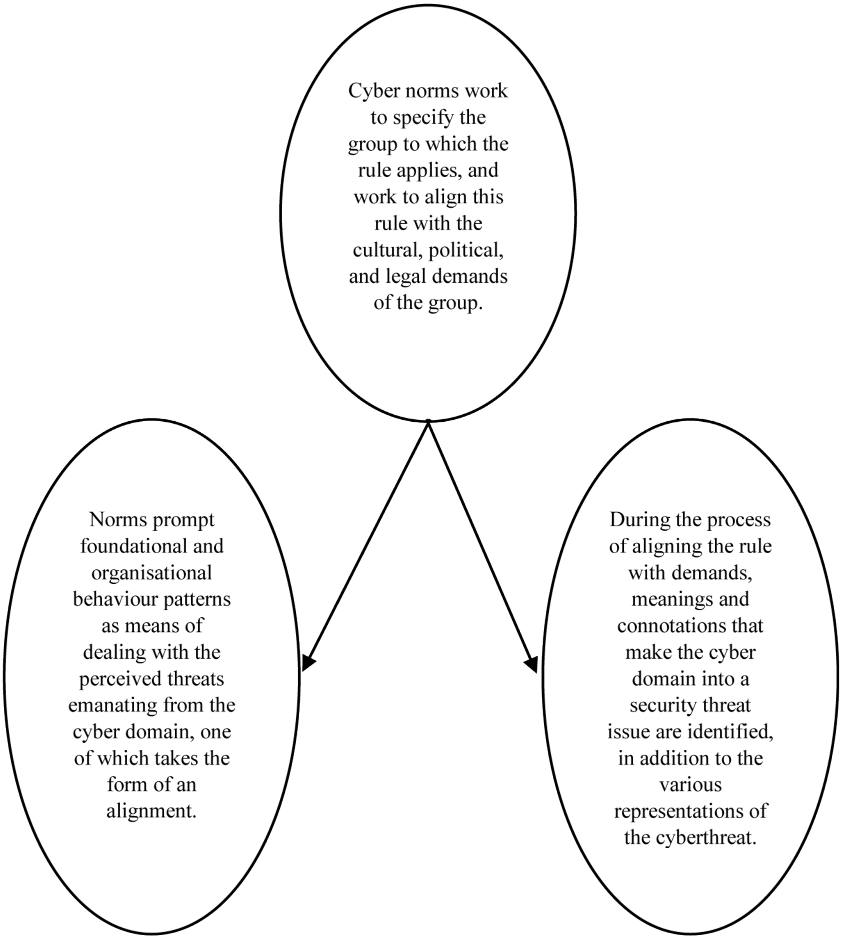
Several approaches that discuss cyber norms have emerged, i.e., that discuss the role of principles and notions in directing state behaviour towards the usage of cybertechnologies and the manner in which it is perceived. These approaches differ in establishing a suitable definition of cyber norms that best describes their nature, and can be divided into four major approaches. The first approach, termed the 'behaviour approach', starts with the idea that cyber norms achieve uniformity in the behaviour of states with respect to identifying the limits of using communications and internet technologies. This approach is represented by Kuebris and Badiei (2017), who conclude that norms are essentially a process consisting of a set of state efforts that aim to produce a common language for the behaviour of other states, which indicates achieving uniformity of behaviour towards cyberactivity. The second approach, known as the 'strategic construction approach', views cyber norms as notions that frame the costs and returns of employing cyber tools in achieving political interests of the state. Cyber norms, according to this approach, are more than just a means for coordination and cooperation. Instead, they serve the function of 'the normative saturation of strategic action', i.e., aligning strategic behaviour and rendering it justified and consistent with norms and notions (Kurowska 2014, 2019; Subotic 2016). The third approach is the 'regulation approach', which deals with cyber norms in terms of their capacity or incapacity to impose legal obligations on states, and views them as a necessary initial step, although not legally binding; Mačák (2017) argues that norms could be turned into a law that gives them a binding status through international agreements and treaties, which are considered binding sources of state behaviour that entail legal responsibilities in the event they are violated.

The fourth approach, termed the 'constructive approach', views cyber norms as collective expectations of what behaviour on the part of actors of certain identities in the fields of technology and communications ought to be, and considers norms to be essential for achieving cybersecurity; Finnemore and Hollis (2016) argue that norms consist of four major elements. First, there is the element of identity, i.e., the group to which the rule applies. Second is the element of behaviour, which refers to the measures that must be taken in order for norms to become effective, and these measures could be either regulatory (regulating the limits of the behaviour of actors), or foundational (establishing new institutions or acting entities). Third is the element of propriety – that is, the capacity of norms to meet the political, legal or cultural demands of the group adopting them, thereby advancing and strengthening these norms. Last but not least, is the element of collective expectations, and the capacity of norms to create common perceptions and understandings among members of the group with respect to the value that their behaviour towards one other involves. From this standpoint, the constructive approach appears to be the most suitable approach for dealing with the role of norms in the cyber domain, since it involves explaining two basic characteristics, namely convergence and divergence – that is, why some actors might adopt similar norms, whereas others might not. The three former approaches, however, deal with norms from a different perspective, which is the perspective of what their existence or creation achieves, whether it is uniformity in the behaviour of states, or framing the strategic action of the state. In contrast, the constructive approach focuses on how state behaviour in the cyber domain is shaped, and on the factors that lead to either a similarity of norms and thereby to cooperative behaviour, or to a conflict of norms and thereby to mutual threat perceptions and conflicting behaviours.

The emerging cyber norms within the framework of the NATO provide a clear model on how convergence and similarity of norms among members of a group arise, and on how the behaviour of a group of states towards the cyber domain is shaped. Atlantic norms arose among NATO states as the group to which these norms apply, and as a group of a distinct identity that reflects the adoption of common liberal values. These norms meet the cultural demands of NATO member states, which are to promote a free, open and peaceful cyberspace, in addition to the political demands of confronting the Chinese and Russian threat, which are adopting counter-norms and behaviours that pose a threat to the values of a free and open internet (North Atlantic Treaty Organization 2023). Moreover, these norms have produced a security behaviour that involves determining the actions and activity that the alliance is permitted to conduct, as was declared during the 2014 'Wales Summit' that cyberattacks constitute an operational field and a part of collective defence activity against potential enemies (North Atlantic Treaty Organization 2014), and also in 2020 when the 'Allied Joint Doctrine for Cyberspace Operations' considered the cyber domain to constitute the fourth operational dimension of the alliance alongside the land, air and sea dimensions (North Atlantic Treaty Organization 2020). Moreover, Atlantic norms have also produced a foundational behaviour that involves establishing new structures and institutions as acting entities that perform a certain role in the cyberdefence of the alliance, such as the establishment of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and the Cyberspace Operation Centre (CYOC) in 2018 (Maigre 2022).

The reviewed model clarifies the role of norms in creating collective behaviour expectations among group members of similar identities. However, it remains relevant, through this model, to point out the role of norms in creating a common threat perception. In this respect, arguably, identity works to specify the group that seeks to align cyber norms with their own cultural, political and legal demands. This produces common perceptions towards the behaviour and norms of other groups with respect to whether or not they align with these demands (particularly, as will become clear later on, during the stage in which the first group seeks to generalise its norms on the international level). In the event they contradict, not align, the first group is led to perceive the behaviour of others as a threat, prompting it to follow a foundational and organisational counter-behaviour. This behaviour would be consistent with mutual expectations between its members with respect to establishing joint security arrangements to deal with the perceived

Figure 2. An Illustrative figure of the role of cyber norms as rules that govern the meanings, connotations, and representations of cyber-threats, and their role in incentivising behaviour in confrontation of the perceived threat



Cyber norms work to specify the group to which the rule applies, and work to align this rule with the cultural, political, and legal demands of the group.

Norms prompt foundational and organisational behaviour patterns as means of dealing with the perceived threats emanating from the cyber domain, one of which takes the form of an alignment.

During the process of aligning the rule with demands, meanings and connotations that make the cyber domain into a security threat issue are identified, in addition to the various representations of the cyberthreat.

Source: Authors

state of insecurity caused by the behaviour of competitors. Norms, in this sense, serve as a governing rule, since they determine the meanings and connotations that states apply to the cyber domain, making it into an issue of security threat in the process. Furthermore, norms identify the various threat representations related to this domain, and work to produce a suitable behaviour among states of similar norms to confront the perceived threat situation in the cyber domain caused by adversaries, i.e., establishing joint security arrangements.

Cyber Alliances or Alignments

Common cyber norms, as illustrated in Figure 2, prompt certain multidimensional action patterns to confront various threat patterns posed by enemies or competitors using such technologies. However, of greater relevance is the resulting unified behaviour of a group of states having similar threat perceptions towards the cyber domain, i.e., the coordinated, organised behaviour that is based on the distribution of roles in confronting nonmilitary cyberthreats. Such security arrangements could be considered to either have the nature of an alliance or to constitute an alignment, and the latter appears to be more suitable for dealing with rapprochement in the cyber domain. The reason for such suitability, as expressed by Wilkins (2012), is that alliances are established for the purpose of using military-power resources under certain conditions, whereas 'alignment' is a broader, more fundamental term that indicates mutual expectations with respect to coordinating policies in dealing with situations involving multifaceted, multidimensional threats not limited to the military dimension under certain conditions. Moreover, alignments by nature depend on the degree of political, cultural and economic compatibility of the states between which they arise, and hence contradict alliances in terms of the mechanisms of their emergence. Whereas the existence of alliances as a military phenomenon is related to the balance and distribution of powers between states, the basis of alignments is the compatibility of national characteristics (values, norms and identities) that prompts states to establish this pattern of security arrangements (Erkomaishvilli 2019).

The proposed 'T10' grouping represents an alignment pattern the US and UK are seeking to form in confrontation of Chinese and Russian cyberthreats. This alignment is based on mutual expectations, produced by common liberal-values identities, of the behaviour that each state would follow in support of other states constituting this grouping. Confronting the mentioned threats would be achieved by coordinating security and intelligence policies aimed at ensuring that China does not gain leadership in emerging technologies, e.g., artificial intelligence and quantum computing, in addition to deterring cyberattacks, and enhancing the promotion of democratic norms to counter 'authoritarian technology' promoted by Chinese firms (Feldstein 2020). The 'Chip 4' grouping provides yet another example on alignment patterns. First proposed in 2022, this alignment consists of the US, South Korea, Taiwan and Japan, and aims to cooperate and coordinate policies among firms and governments of party states with respect to ensuring the security of the global semiconductor supply chain and blocking Chinese access to it (Davies, Jung, Inugak, & Waters 2022).

The major issue of concern remains to analyse the manner in which such a pattern of security arrangement arises. Arguably, the first step towards forming alignments between states is the existence of common norms that produce a common perception of cyberthreats. For this purpose, it is appropriate to use the model presented by Finnemore and Sikknik (1998) to simulate the manner in which common norms are transformed into security alignments under the presence of competing norms adopted by a different group. This model suggests that norms go through three stages leading to their institutionalisation. In the first stage, termed '*emergence of norms*', governments face mounting pressure from some domestic agencies that have their own notions of what appropriate behaviour in society ought to be (civil society organisations, political parties, etc.), and norms emerge domestically as governing rules of state behaviour towards certain issues and reflect the values it adopts. The second stage, termed *'norms cascade'*, involves the transition of norms from a domestic to an international level. States seek to generalise their norms on other states and impose them as governing rules of their behaviour, which is achieved through various means, such as diplomatic support and economic sanctions or incentives. Norms, during this stage, experience both adoption and opposition, and this stage is characterised by the emergence of competing norms pushed towards generalisation on the international level. Ultimately, norms in the final stage are 'internalised' and transformed into certain institutional structures, i.e., international institutions that resemble frameworks under which a group of states adopt common behaviour rules towards one another, and these frameworks reflect the values these states adopt towards certain issues.

The framework of analysis through which forming security alignments or partnerships in the cyber domain can be explained, particularly the '*transatlantic alignment*', is obtained by applying the mentioned model. First, cyber norms emerged domestically in the US and EU as behaviour rules, and reflected the values they adopt towards this domain. These norms are fundamentally a framework that governs perceptions of national security threats, which can be inferenced from the security strategies of both parties towards the cyber domain. Subsequently, norms began to cascade, and the US sought to generalise its cybersecurity model on the international level based on its own perceptions of this field of security, leading to a conflict of norms with China and Russia, which simultaneously seek to generalise their own norms and impose them as behaviour rules on other states, i.e., a pattern of international competition occurred on what norms governing the cyber domain ought to be. During the final stage, US norms were internalised and transformed into institutional structures that include EU members of similar orientations towards the rules and values ought to govern the cyber domain. This type of institution represents a security alignment between the US and EU, and aims to prevent China and Russia from generalising their cyber norms, an endeavour that poses a threat to American and European national security.

The Emergence of American and European Cyber Norms

Analysing US and EU cyber norms is a prerequisite of understanding the common meanings, connotations and perceptions through which the two parties identify the form of cyberthreats. These norms reflect American and European values, and establish rules that govern their behaviour in confronting cyberthreats and risks. Moreover, norms are used as a standard for determining the existence or absence of these types of threats, i.e., behaviours opposing norms are perceived as a security threat, since they violate the rule that governs behaviour and the values this rule involves. Therefore, discussing American and European norms necessitates analysing their origin and emergence on the domestic level by observing the cybersecurity strategies of each party.

American Norms and the Form of Cyberthreats

Cyberthreats were first identified as a threat to the US national security in the 2010 'National Security Strategy' (The White House 2010). Thereafter, norms governing the cyber domain have been continuously emerging in the US. These norms reflect American cyber values, and identify the meaning of threats the cyber domain poses to the US national security, in addition to being rules that govern US behaviour towards cyberthreats. Furthermore, this strategy establishes that values related to cybersecurity are primarily embodied in the protection of civil liberties and personal privacy, i.e., values of liberal, individual freedom. It also identifies cyberthreats as the use of technology for the purpose of damaging the US economy, such as hacking communications networks and e-commerce and intellectual property theft, in addition to inflicting damages on the military sector by hacking military networks, all of which are threats posed by various entities, from terrorist groups, to competing or hostile nations.

The 2011 'International Strategy for Cyberspace' discussed in greater detail the meaning of values related to the cyber domain, embodied in civil liberties and personal privacy, by indicating that they provide the rules of state behaviour towards this domain (The White House 2011). These values, as will be noticed, have played a major role in the US endeavour to generalise its norms on the international level. To the US, the nature of the cyber domain, and the communications networks and internet it involves, represents a technical and a social decentralised pattern, i.e., no central entity exercises its authority on it, whether this entity is the political authority, or any other actor; instead, it is a multi-actor, multiclass domain, rendering it an open, free domain that must not be dominated by any one party. This characteristic is viewed as both important and necessary. The US considers that drafting international rules ought to be done through the 'multistakeholder approach', since this approach, as opposed to other approaches, requires states to involve private sector entities (communications and technology firms) in the process of drafting rules, which resembles the open and comprehensive nature of the cyber domain.

European Norms and their Transition to the Level of the European Union

Cyber norms began to emerge domestically in European states as values and rules that identify behaviour towards the cyber domain, and were then transitioned to and generalised on the level of the EU. European norms are closely related to those adopted by the US. For instance, the 'UK Cybersecurity Strategy'[1] of 2011 (Cabinet Office 2011) laid the foundation of the norms, values and rules that guide UK behaviour towards the cyber domain, all of which appear to be derived from the values of liberal freedom that it adopts. This is reflected in the strategy's affirmation that values involved in the cyber domain should be derived from British 'traditions' and guided by the values of freedom, justice and rule of law. Furthermore, it expressed that the widespread, expansive and interconnected nature of the cyber domain should lead to the promotion of these values.

The 2011 'Cybersecurity Strategy for Germany' laid the foundation of German norms that identify the values and behaviour of Germany towards the cyber domain, which are to a great extent similar to those adopted by the US and UK in terms of the freedom of this domain and state behaviour towards entities that should perform their respective roles within it (Federal Ministry of the Interior 2011). This strategy expressed that cybersecurity is derived from the values of freedom, and that ensuring cybersecurity leads to ensuring freedom and development in Germany, since state institutions, its vital infrastructure (energy, transportation, communications, etc.) and German firms are increasingly reliant on communications and information technologies, which consequently turns any threat posed to these technologies into threats to social and political life. Moreover, the rule that identifies the desired behaviour of Germany in achieving cybersecurity is based on the fact that the interactions governing the neutralisation of threats emanating from the cyber domain must involve partnerships between governmental institutions and political authorities on one hand, and

[1] It is worth noting that the reason for mentioning UK cyber norms within the context of discussing EU norms is that norms of the UK were produced prior to its withdrawal from the EU, i.e., when it had exercised an influential role in transitioning cyber norms from the national level to the level of the EU.

private sector firms and society on the other, with the deviation from this rule leading to an incapacity to achieve cybersecurity. Other European states, such as the Netherlands and Czech Republic, have also adopted cyber norms similar in nature to those adopted by Germany and the UK (The European Network and Information Security Agency 2012).

Domestic norms specific to each European state were transitioned to the level of the EU in 2013 when the 'EU Cybersecurity Strategy' was first adopted (The European Union 2013), which involved the same norms adopted by each state individually. This can be observed in the strategy's five guiding principles of EU policies towards cybersecurity, representing the values and behaviour rules the Union adopts towards issues of the cyber domain. First, core values of the EU apply to the 'cyberspace' to the same extent they apply to the 'physical world'. Second is preservation of fundamental rights, freedom of speech and protection of personal data of EU citizens, and that is since in order for cybersecurity to be effective, it must be based on the fundamental rights and freedoms enshrined in the 'Charter of Fundamental Rights of the European Union'.[2] Third is freedom of accessibility to the internet, i.e., all individuals residing in the EU should be able to access the internet. Fourth, management of the cyber domain ought to be in accordance with the 'democracy' and 'multistakeholder' approach, which affirms the central role of the private sector in achieving cybersecurity, and the absence of a single dominant party (political authorities of EU member states, primarily). Lastly, the strategy refers to the joint responsibility in ensuring security, implying that all parties – governmental, individuals and firms – are jointly responsible for responding to cybersecurity threats.

The Cascade of Cybersecurity Norms and Emergence of their Competing Counterparts

Shifting the discussion on the emergence of norms from a domestic level to the level of international interactions requires analysing how these norms cascaded, i.e., analysing how the US sought to generalise the behaviour rules it adopts, the means it has employed to this end, the accompanied consent and dissent towards these norms, and the emergence of competing norms that China and Russia seek

[2] The core idea of the Charter of Fundamental Rights of the European Union refers to the group of natural, civil and political individual rights that EU citizens enjoy. These rights include, interalia, the right of dignity, freedom, equality and solidarity, and they reflect the values and principles of liberalism, which generally serves as the core of western democracies. Moreover, referring to these rights in the 'EU Cybersecurity Strategy' makes clear the extent to which the values that the EU adopts influence its perception of the nature of threats emanating from the cyber domain and the extent to which they identify the rules governing its behaviour towards this domain. For further details on the Charter of Fundamental Rights, see European Parliament 2000.

to generalise. Since generalising norms, accepting and opposing them, and the emergence of competing norms are in effect what led to the establishment of the transatlantic alignment, such analysis of the cascade of norms is of great relevance.

Generalising American Cyber Norms and the Endeavour to Construct an International Order

The generalisation of US cyber norms on the international level can be analysed through the context in which the US seeks to construct an international cyber order, i.e., transform the norms it adopts into international rules and institutions of the cyber domain that promote its interests as a dominant power in international interactions. In this context, the 2011 'International Strategy for Cyberspace' indicates the manner in which the US has been seeking to establish rules that identify the behaviour of other states in the cyber domain (The White House 2011). This strategy expressed that the nature of norms and rules ought to govern international cyber interactions is defined in achieving peace and global stability (preserving the stability of the international liberal order and ensuring the absence of any alterations that might affect its status in it), and in establishing the fundamental rule that determines the mutual rights and duties of states. These rules include:

1. Upholding fundamental freedoms: states must respect the fundamental rights of individuals, entities and other states to speech and to connect through the internet.
2. Respect for property: states must, through domestic laws, respect the rights of intellectual property of individuals and firms, including patents and trade secrets.
3. Valuing privacy: which refers to protecting individuals from arbitrary or illegal state interference with their privacy.
4. Protection from crime: States must identify and prosecute internet criminals.
5. Right of self-defence: In accordance with the Charter of the United Nations, states have the right to defend themselves in the event of hostilities or attacks in the cyberspace.

Pursuing this vision, the US has resorted to various means to generalise these norms on the international level. One such attempt was to build a consensus within the United Nations, through its Groups of Governmental Experts, towards establishing rules that govern the cyber domain; it was able to achieve this end in 2011 by building a consensus on three fundamental principles of cybersecurity. These principles, as Mazarr et al. (2022) argue, represent behaviour rules that states must abide by, and entail three matters. First, they entail that states recognising these norms under the framework of the United Nations must neither support nor by themselves launch cyberattacks that undermine or damage the vital infrastructure of any state. Second, states must not hinder any response to cyber emergencies, and, lastly, should mutually cooperate in prosecuting internet crimes launched from within their respective lands.

The US endeavour to build international consensus on norms of cybersecurity was not limited to its efforts within the United Nations. Similar attempts can be observed in the 'Wassenaar Arrangements' between 2013 and 2015, which are agreements concluded by the US with 40 other states for the purpose of setting a multilateral export control regime on some cybersecurity products and technologies, including the exchange of software and physical communications technologies of a dual use, i.e., that could either be used in developing the vital technological and digital infrastructure, or as a means of espionage and censorship. The usage of these export-controlled technologies is what primarily leads to potential human rights violations, e.g., censorship on associations and opposition political parties (U.S. Department of Commerce 2017), which indicates that rules and norms established by the 'Wassenaar Arrangements' are nothing but a reflection of American domestic norms embodied in the principle 'freedom of the internet'.

It is worth noting that the US efforts to establish norms and rules of the cyber domain on the international level comprise only one part of its endeavour to construct an international cyber order, i.e., to establish a set of rules, norms and institutions that govern the cyber domain and reflect US interests as the dominant power of the international system. This has been necessitated by the existence of competing states seeking to construct an alternative order. China represents the major competing power, since it seeks to generalise its norms and construct an order that contradicts US norms, thereby prompting the latter to add a new cyber suborder to the prevailing international order, which was constructed in the post-WWII period and comprises of three suborders: the international economic order established by the Bretton Woods System and the World Trade Organisation, the international security order established by a series of treaties and rules, and the international human rights order (Kundnani 2017). What this all implies is that in the event the US fails to construct an international cyber order whereas China succeeds in doing so, both the prevailing liberal order and the status of the US as the sole dominant power of the international system could potentially become threatened.

The Competing Chinese and Russian Cyber Norms

Parallel to the US endeavour, competing Chinese norms, embodied in the notion of 'cyber sovereignty', have emerged and are being pushed towards generalisation on the international level as well. Such dissimilarity of norms and visions does not merely imply a difference in identifying the technical rules of managing and functioning the cyber domain and the various internet and communications technologies it involves, but rather signifies contradictory visions of the international political order of the cyber domain (Lindsay 2014), i.e., competition over identifying the rules, norms and institutions of the cyber domain that each state seeks to establish. Consequently, the two states have been involved in an intense competition thereafter.

'Cyber sovereignty' is a notion that was adopted by Chinese ruling elites first on the domestic level, and at a later stage was pushed towards generalisation on the international level as the basis of the international order that China seeks to construct. It refers to the idea that the internet and all processes related to technology and communications developments must be subject to state sovereignty, that this domain is within, not outside of state control and is subject to its authority. Moreover, it implies that each state should respect the right of other states to choose their own course of developing their cyber capabilities and technologies with respect to the methods of managing this domain and the public policies through which it is organised and guided. Therefore, norms of 'cyber sovereignty' are designed to serve four major purposes of China. The first purpose is to preserve its critical infrastructure, which has become increasingly reliant on the developments of technology. Second, to preserve the ideology of the Chinese political system, i.e., to ensure that no anti-communist values and principles are promoted through the internet and communications networks. Third, to preserve high economic technology and technology industries of an economic aspect, and, lastly, to employ such industries in constructing an international cyber order as an alternative to the liberal order that the US is proposing (Wang 2020).

To achieve compatibility between these ends, a prerequisite of putting 'cyber sovereignty' norms into practice, China has taken advantage of its initiatives. One clear example of efforts aimed at establishing international institutions and rules of the cyber domain that reflect Chinese norms is the 'World Internet Conference' (WIC). Launched in 2014, this initiative emerged as an annual conference held in China. Participants of the WIC are states adopting similar visions of what principles and rules ought to govern the cyber domain, such as members of the Shanghai Cooperation Organisation, and the states targeted by the 'Digital Silk Road' initiative. The first conference, held in 2014, promoted 'cyber sovereignty' norms by affirming that the challenges posed to national sovereignty by the cyber domain represent the most prominent issue to the WIC, which should prompt the international community to establish a pluralist 'global governance system', i.e., since the cyberspace is subject to state sovereignty, then states are the only actors with the right to shape the rules by which their behaviour in this space is governed (China Daily 2014). This approach represents an alternative to the US approach, which is based on partnership between the state and stakeholders of the private sector in establishing cyber domain rules.

Chinese norms have been presented as an alternative through various other initiatives, including the 'Digital Silk Road' initiative of 2015. This initiative aims to establish a set of international rules and norms with China at the centre, and involves Chinese investments in building the necessary technological infrastructure in various Asian, African and European states, e.g., building 5G networks, installing fibre optic cables, and installing submarine communications cables. However, the 'Digital Silk Road' also has a political aspect primarily embodied in promoting regional and international correlation (Dekker, Heijmans, & Zhang 2020). This would be achieved through, first, building infrastructure and promoting trade and finance between China and participating states, and second through promoting Chinese innovations and technologies in these states, i.e., to render China the global source of technology. Last, it would be achieved through altering global technology supply chains so as to start from China rather than western states (the US, in particular), implying further integration between Chinese technology firms and African and Asian states targeted by the initiative.

Unsurprisingly, the US views both initiatives as a threat to its international interests, since China, through generalising 'cyber sovereignty' norms, seeks to become a 'great cyber power'. This latter term was first introduced by Chinese president Xi Jinping in 2015, when he implied that if China aspires to be influential in shaping international policies, then it must become the leading power in technology and control its global courses. Such a perspective is the product of associating dominating the 'waves of civilisation' with state power. For instance, Great Britain dominated the wave of industrial civilisation in the 18th century and became a dominant power on the international level, allowing it to construct an international order that serves its interests. China applies this experience to the wave of digital civilisation (Hemmings 2020), and dominating the age of 'information revolution' is considered by Chinese ruling elites to render China a dominant power with the capacity to construct an international order that serves its interests and dispose of the 'humiliation' it suffered in the 'Opium Wars' (Doshi et al. 2021). Therefore, by employing the information revolution to its interest, China would become an influential power in shaping the structure of the international system and order, instead of being influenced by the policies of the prevailing great power, as was the situation during the 18th century. Achieving this status is a threat to the US, since the latter would cease to be the sole great power, and the structure of the international order it has been constructing since the end of WWII would be altered.

Russia adopts cyber norms that are similar in nature to those of China, particularly the ones related to 'cyber sovereignty' (Security Council of the Russian

Federation 2016). However, this sovereignty involves different matters to each party, resulting in different ends to be achieved by employing cybertechnologies, and different mutual threat perceptions between the two states. Chinese cyber sovereignty involves state control over the cyber domain, and employing this domain towards establishing new rules and institutions of the international order, whereas Russian understanding of cyber sovereignty involves employing cybertechnologies to politically influence the West. This indicates a Russian preference of ‘cyberattacks’ and ‘cyber warfare’ to politically destabilise targeted states, an approach that has been used by Russia on several occasions, such as employing its cybertechnologies to influence the results of the 2016 US presidential elections, and also the results of the BREXIT referendum (Broeders, Adamson, & Creemers 2019).

Therefore, Russian notions focus on achieving superiority in ‘cyber warfare’ instead of focusing on the Chinese notion of ‘great cyber power’. To Russia, ‘cyber warfare’ refers to a confrontation between two or more states in the cyberspace for the purpose of causing damage to the information systems, resources and critical infrastructure of opponents, thereby undermining their political, social and economic systems; it constitutes a psychological system that aims to destabilise the state and society (Pijović 2021). The cyberattack on Estonia in 2007 provides an example on how dependent Russia is on the pattern of cyber warfare. Subsequent to a political dispute between the two states, Russia launched a series of cyberattacks that targeted Estonian critical infrastructure and aimed to disrupt the country’s banking sector (Ottis 2007).

Perspective differences between China and Russia on cyber sovereignty have also impacted Russian preferences with respect to its behaviour within regional security institutions and complexes in which both states participate (BRICS and SCO), as Russia appears to be unwilling to integrate its norms into such institutions. Whereas Chinese activity within the ‘Digital Silk Road’ initiative and the ‘WIC’ aims to generalise its antiliberal cyber norms, Russian behaviour has been primarily directed towards generalising the norms of ‘cyber warfare’ within the Collective Security Treaty Organisation (CSTO) (Flonk 2021). This has led to a militarisation of Russian norms, which is consistent with the Russian perspective on what cyber sovereignty involves, giving norms a different aspect from the economic aspect of the cyber domain that China promotes within the mentioned blocs and initiatives. Integrating norms in this manner aims to reduce the military technological gap between Russia and the West, and achieve superiority in this field. The CSTO guidelines for internet and information security provide clear evidence on this. According to these guidelines, Russia provides training for information security specialists, and prepares military cadres for member states in the fields of information and cybersecurity (Sukhankin 2018).

The Internalisation of American Norms and the Transatlantic Alignment in the Cyber Domain

American and European cyber norms were internalised and made into institutional structures that resemble a security alignment, aiding the two sides to overcome their previous contentions raised by the cyber domain. These institutions have been putting forth their own alternative initiatives, and aim to contain and isolate China and Russia from technology that is necessary to build their cyber capabilities. This is related to the 'cascade' of American norms. Through this 'cascade', the US has sought to generalise its cybersecurity model on the international level. In response, competing Russian and Chinese norms emerged, through which the latter seeks to influence the structure of the prevailing international order. Such Russian and Chinese influence alters the current status of the US, and affects its endeavours to construct an international cyber order, hence the reason the latter perceives this influence as a threat. In this context, the transatlantic alignment has evolved from one form into another, that is, from the 2014 'EU-US Cyber Dialogue' (European Union Websites 2014), into the 'EU-US Trade and Technology Council', which was established in 2021.

The Evolution of Transatlantic Cyber Relations

Establishing the CCDCOE in 2008 represented the first wave of US-EU cooperation within NATO in confronting the Russian behaviour of employing the tools of 'cyber warfare'. This response is consistent with how Russia defines the cyber domain, i.e., an aspect of military conflict. Therefore, the major purpose of establishing the CCDCOE was to manage potential cyber warfare and conflict between NATO and adversaries, particularly Russia. Despite this cooperation, however, the cyber domain has for a relatively long time raised contentions between the two sides, hindering any attempts to deepen this cooperation, let alone form an alignment. These contentions are embodied in US misconduct in terms of employing the cyber domain against allies, in concerns related to data privacy, and in economic competition. Nonetheless, with the establishment of the 'US-EU Trade and Technology Council', the two sides appear to be working towards overcoming their contentions and reaching a mutual understanding. Such an understanding constitutes both a test and a decisive result of the role of similar norms in producing a similar form of threat perception towards Chinese and Russian behaviour in the cyber domain, consequently working to form a transatlantic alignment to confront these threats.

The first point of transatlantic contention was embodied in US misconduct with respect to data privacy breaches and the conduction of espionage activities against several EU members. Edward Snowden, a former US National Security Agency (NSA) officer, exposed this behaviour through what became known as the 'Snowden leaks' or the 'Snowden incident'. The leaks revealed that the NSA had been collecting phone records and using a spy programme called PRISM to collect and transfer data on Facebook and Google users in Europe (Solms & Heerden 2015), and to spy on EU diplomats for the purpose of gaining influence during the talks on reaching a 'Transatlantic Trade and Investment Partnership' agreement with the EU, which were scheduled in July of 2023, leading to calls by European Parliament members to cancel the talks (European Union Centre for North Carolina 2014). Consequently, trust between the two sides was undermined, and the EU began to perceive the risks of excessive dependence on US technology and networks, leading to a shift in views on cybersecurity, data protection and privacy (Renard 2018). This was evident in the European endeavour to issue new rules aimed at limiting questionable data transfers from EU member states to the US (Traynor 2013).

The issuance of such rules in 2016 under the 'General Data Protection Regulation' (GDPR) revealed the second transatlantic contention, that is, concerns over data privacy. Data protection mechanisms of the GDPR contradict the US vision on how employing data in competition with adversaries ought to be. Under the GDPR, which represents the European approach to data protection, the EU exercises a central role with respect to data belonging to its members, whether in terms of preventing unauthorised access by third parties to information stored on the internet and servers located in EU member states, or in terms of restricting data transfers to nonmembers by requiring prior approval of the European Commission (EC) (The European Parliament, The Council of the European Union 2016). On the other hand, the US strategic approach divides data into three areas: the 'blue cyberspace', 'red cyberspace' and 'gray cyberspace'. According to this approach, achieving superiority over adversaries in this field requires the US not only to protect the 'blue cyberspace' (networks, data and internet servers owned and controlled by the US), but also to exercise influence on the 'red cyberspace' (networks, data and internet servers owned by adversaries), and to employ the 'gray cyberspace' (internet infrastructure owned by allies, but used as a conduit for data outgoing towards adversaries or enemies) in serving its interests. Within the 'gray cyberspace', the US has worked towards accessing data of enemy parties through the digital infrastructure of allied states, e.g., the US Cyber Command deleted ISIS propaganda material from German servers without obtaining prior consent, leading to tensions between the two states (Smeets 2020). Such approach differences had disrupted any attempt to regulate the flow of data between the US and EU, as was the case when the Court of Justice of the European Union invalidated the proposed 'Privacy Shield' framework between the two sides on grounds of the absence of adequate guarantees within US law, and data surveillance on the part of the latter during transfers (Marconi 2023).

The third transatlantic contention is economic competition in the digital domain, particularly with respect to the tax policies known as 'digital services taxes' (DSTs). First proposed by the EC in 2018, these taxes would be imposed on US technology firms operating in the EU and included a tax rate of 3%, but faltered due to disagreement between party states (Lowry 2019). Nonetheless, European states have individually adopted a digital tax outside the framework of the EU. For instance, France imposed a 3% tax on gross revenue resulting from digital interfaces and targeted advertisements, which applies to large firms generating 25 million euros in revenue from their operations in France and 750 million euros from global operations (Frieden & Stephanie 2021). Similarly, other European states followed suit by adopting similar tax rates, such as Spain and Italy, in addition to Austria and Hungary adopting a 5% and 7.5% tax rate, respectively; the French measures remain the most relevant as the only measures that were put into effect (Geringer 2021). These measures led to tensions between France and the US, and prompted the latter to announce in 2020 that it would impose a tax with a value of 1.3 billion USD in 2021 in the event France resumes collecting the DST (Asen 2021).

Establishing the 'EU-US Trade and Technology Council' represented a major step towards overcoming these contentions and forming a transatlantic alignment between the two sides, in which the similar form of EU and US cyber norms was a major factor. Through these norms, Chinese and Russian behaviour in the cyber domain has been identified as a security threat, since it is driven by norms that counter those adopted on the transatlantic level. In confrontation of this threat, both sides have followed a behaviour of launching several initiatives under the framework of the transatlantic alignment, such as investing in developing 5G technologies, installing submarine cables and investing in critical infrastructure. These initiatives appear to be designed as a means of competing with the aforementioned Chinese initiatives, through which China seeks to promote its norms and construct an international order that serves its interests. Furthermore, the semiconductors initiative appears to be aimed at isolating China and Russia from this technology, thereby impeding the development of their cyber capabilities. Arguably, the transatlantic alignment, in its entirety, is ultimately designed as a means of increasing EU and US influence, and hence containing China and Russia, in the cyber domain.

Alternative Initiatives under the Framework of the Transatlantic Alignment

The 'EU-US Trade and Technology Council' is based on, inter alia, 'cooperation on emerging technologies', 'building resilient semiconductor supply chains', 'promoting values worldwide and reaching out to partners', 'further growing transatlantic trade', 'enhancing security through export controls and investment screening', and investing in 'digital infrastructure and connectivity', i.e., initiatives in the cyber domain, such as 5G communications (European Commission Website 2022). To these ends, various working groups operate, such as the working groups of 'Technology Standards', 'Misuse of Technology Threatening Security and Human Rights', 'Cooperation on Export Controls of Dual Use Items', 'Secure Supply Chains', 'Data Governance and Technology Platforms' and other groups that deal with different cybersecurity issues (U.S. State Department Website 2022).

Investing in critical and emerging infrastructure involves investing in developing 5G technologies and the necessary infrastructure for advanced technology, and installing submarine cables in the US, the EU and third-party states, which represents a parallel initiative to the 'Digital Silk Road'. Investments in such technologies and launching initiatives thereof are considered by the US and EU a prerequisite of exercising international influence. The absence of these investments renders both parties incapable of shaping policies and establishing the required rules, norms and institutions of the cyber domain, and only states that invest in critical and emerging technology would then be able to exercise such influence (primarily China) (Torreblanca & Ricart 2022). Therefore, it is necessary for the transatlantic alignment to invest in producing and developing such technologies in its two parties and in third-party states, since this both enhances the tendency of these third parties to accept the rules of the cyber domain that are established by the alignment, and balances Chinese influence in this domain.

This vision has prompted the 'EU-US Trade and Technology Council' to invest in building and developing technology infrastructure in third-party states since 2022, primarily targeting Jamaica and Kenya (The White House Website 2022b). Projects in Jamaica aim to encourage and support the use of digital technology by all governmental and nongovernmental institutions, expand the wireless communications infrastructure and support the wide usage of communications networks provided by EU and US 'trusted' technology firms. On the other hand, the initiative towards Kenya aims to provide the necessary technical support for the purpose of developing and modernising the Kenyan 'Information and Communications Act'. It also aims to form a strategy of building 5G networks in line with the principles and standards of global infrastructure projects.

The indication that such investments and initiatives must be undertaken by 'trusted' EU and US technology firms implies that balancing and undermining Chinese influence in the cyber domain requires undermining the capacities of Chinese technology firms – Huawei and ZTE, in particular- and limiting their international expansion. These firms represent the major tool of implementing Chinese initiatives and achieving its vision of constructing an international order. The joint statement of the second meeting of the 'EU-US Trade and Technology Council' in 2022 expressed this perspective (U.S. Department of

Commerce 2022) by affirming that building, developing and installing the announced 6G communications networks, besides from 5G networks, whether in alignment parties or in third-party states, must involve diversifying the suppliers of these technologies, which should be as limited as possible to 'non-high-risk', 'trusted suppliers' of technology projects.

Isolating China and Russia and Reshaping the Global Semiconductor Supply Chain

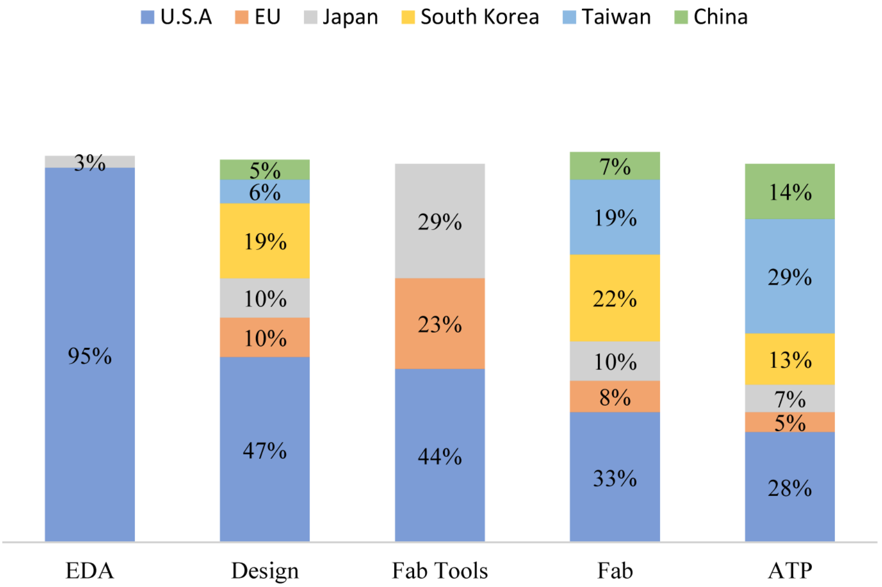
The second end of the transatlantic alignment, lying at its core, is to boost US and EU capacity to manufacture semiconductors and control their major stages of production. Semiconductors are the basis of all technology projects and initiatives launched by the alignment. They also represent the foundation of all Chinese technology industries, and are the basis of its ability to trigger political alterations. The idea of 'building resilient semiconductor supply chains' aims to render China neither capable of accessing this technology nor affecting its production process, and to prevent Russia from owning and employing these technologies in developing its military capabilities and capabilities related to information warfare.

A global supply chain refers to all economic institutions, entities and individuals existing in different states and having a certain role in producing a certain good, starting from its raw materials, to the final product delivered to the end consumer (Hayes 2022). 'Bottlenecks', as they are often referred to, are the most important link of any supply chain, and in the case of the semiconductor supply chain, they are, in order, as follows (Ragonnand 2022):

1. Electronic design automation (EDA): the software and applications installed on semiconductors fabrication machinery.
2. Design: determining the specifications of semiconductors, such as their production materials and sizes.
3. Fabrication tools: refers to producing the required machinery and technology for semiconductors fabrication.
4. Fabrication: in this stage, designs take a physical form as ‚semiconductor wafers'.
5. Assembly, testing and packaging (ATP).

Figure 3 illustrates production shares within the global semiconductor supply chain. These statistics indicate the dominant role of the US within the first two links (EDA and design), whereas the EU plays a major role alongside the US within the third link (fabrication tools), e.g., the Dutch firm ASML is recognised as one of the most important global suppliers of highly sophisticated and complicated machinery used in fabricating semiconductors (Shead 2021). China, in contrast, plays a somewhat puny role that is limited to the fourth and fifth links (fabrication and ATP), which prevents it from increasing its own production of semiconductors and enhancing its position in this industry so long as it remains reliant on the first three links primarily dominated by the US.

Figure 3. Production shares within bottlenecks of the global semiconductor supply chain



Source: Ragonnand (2022)

Whereas blocking Russian access to these technologies is unchallenging, since Russia has no capabilities within the bottlenecks of the supply chain, achieving the pronounced end of 'building resilient semiconductor supply chains', one the other hand, requires two things: first, to ensure that China is unable to enhance its existing capacities within the fourth and fifth chain links, and second, to ensure its inaccessibility to the technologies of the first three links so as to render it incapable of manufacturing semiconductors on its own. The US and EU have taken various measures with respect to the first requirement, so as to enhance their capabilities in 'design' and 'ATP'. Such measures would simultaneously increase their capacities within all links of the supply chain, which necessitates reshaping this chain by shifting fabrication and assembly from east Asia (Japan, Taiwan and South Korea) to the US and EU, thereby rendering the supply chain centred around the transatlantic alignment. This approach can be concluded from the US 'CHIPS and Science Act' passed by the US Senate in 2022, and 'European Chips Act' passed by the European Commission in 2021.

The US 'CHIPS and Science Act' aims to boost US semiconductor manufacturing capacity, i.e., enhance its capacities within the fourth link (Fabrication). It also provides the necessary investment incentives that work to promote US leadership in developing and manufacturing semiconductors, promote its current leading position within the technology domain, and reduce reliance on vital technology sourced from China and other states that could experience tensions disruptive to the supply of semiconductors (The White House Website 2022a). To this end, 52.7 billion USD were allocated, including 39 billion USD as financial incentives to boost US semiconductor manufacturing capacity, and 11 billion USD for research and development. These incentives primarily target foreign firms desiring to contribute to increasing US production of semiconductors, in return for their commitment to not expand any activity related to the semiconductor industry in China for a duration of ten years (Dorsey and Whitney Lep Website 2022). In response, Taiwanese semiconductor manufacturer TSMC, the largest manufacturer of semiconductors globally, announced that it would build two fabrication plants in the US, the first of which is to start production in 2024 and is set up to produce 5nm semiconductors, while production in the second plant is due to start in 2026 and will produce 3nm semiconductors (Taiwan Semiconductor Manufacturing Company 2022).

Passed by the European Commission in 2021, the 'European Chips Act' sets objectives that are similar in nature to those implied by its US counterpart, i.e., to promote the position of the EU within the global semiconductor supply chain and overcome any flaws it experiences in this respect. To this end, the 'European Chips Act' puts forth the 'Chips for Europe' initiative, which allocates 43 billion euros as investment incentives for technology firms (Council of The European Union 2022), and aims to build highly developed capabilities in semiconductor designing and ATP, further boost the manufacturing capacity of existing firms and establish new ones, and develop the capabilities of SMEs to manufacture semiconductors by facilitating their access to designs (Council of The European Union Website 2022). In this respect, it is of a great necessity for the EU to become oriented towards firms that are capable of supporting its aims. The US semiconductor manufacturer Intel, for instance, announced in 2022 that it would invest a total of 80 billion euros in EU member states, which includes establishing fabrication plants in Germany, a designing facility in France, and an additional fabrication plant in Ireland, not to mention other investments in Italy, Poland and Spain. Similar tendencies can be observed in the negotiations currently underway between semiconductor manufacturing giant TSMC and Germany for the purpose of establishing a new fabrication plant in the latter (Cherney 2022).

It becomes clear that the US and EU have been pursuing a policy of providing investment incentives that attract foreign investments at the expense of China, thereby preventing it from boosting its semiconductor manufacturing capacity.

This well achieves the first component of 'building resilient semiconductor supply chains', that is, to undermine Chinese capabilities within the fourth and fifth links of the supply chain (fabrication and ATP). However, towards achieving the second component, namely ensuring the inaccessibility of China to the technologies of the first three link (EDA, design and fabrication tools), the US has taken different measures; In 2022, the Bureau of Industry and Security established new export controls that regulate the exportation of design, automation and fabrications tools to China. Under this regime, US technology firms, and all foreign firms within the supply chain using US technology, face licensing requirements for the exportation to China of advanced semiconductors and the necessary tools, technology and equipment to manufacture them (machinery, designs, software, etc.). This includes 14nm to 16nm logic semiconductors, 18nm DRAM memory semiconductors and NAND memory semiconductors of 128 layers or more, all of which are crucial and key technologies in artificial intelligence and advanced technology industries (The U.S. Bureau of Industry and Security 2022). In this context, the US initiated negotiations with the EU at the end of 2022 for the purpose of integrating these export controls into the framework of the 'EU-US Trade and Technology Council', and that is since some European states produce semiconductor manufacturing machinery, particularly the Netherlands with its ASML plant (Financial Post Website 2022).

Similar export controls were imposed on Russia under the framework of the 'EU-US Trade and Technology Council' during its second meeting in 2022, when the Russian invasion of Ukraine was first launched. Aiming to undermine Russian military and industrial capabilities, these controls included restrictions on the exportation of semiconductors used in the development of military capabilities or the development of capabilities related to cyberattacks and surveillance (European Commission 2022). However, although controls imposed on Russia are similar in their form to those proposed under the framework of the Council to be imposed on China, these controls represent different responses based on how each targeted party perceives the cyber domain under prevailing norms. Russia understands building its cyber capabilities from the perspective of achieving superiority in information warfare against the West, and hence the imposition of export controls coincided with its war on Ukraine so as to block its access to critical technologies that would allow it to develop its cyber-military capabilities and achieve such a superiority. China, on the other hand, views building its cyber capabilities from the perspective of attaining the status of a 'great cyber power', and hence the US endeavour to impose controls on the exportation of semiconductors to China aims to influence Chinese initiatives and projects in the cyber domain that would allow it to attain such a status. Therefore, despite following a similar behaviour towards Russia and China, embodied in export controls, the ultimate ends pursued are not similar whatsoever, and they differ according to how each targeted party perceives these technologies.

Conclusion

The main findings of this article can be summarised as follows. First, norms represent the deciding factor in the arising of common perceptions and meanings of threat, which transform the cyber domain from a neutral issue into one of a security threat, and prompt the establishment of a security alignment between states adopting common norms. Second, the similarity of the form of US and European cyber norms, defined in 'internet freedom' and 'cyber democracy', has produced a similarity in the perceptions and meanings of cyberthreats, defined as violating these norms by third parties adopting counter-norms and behaviour.

Third, the US endeavour to generalise its liberal norms and construct an international cyber order, through establishing a group of international arrangements, was a prompting factor for the existence of competing Russian and Chinese norms embodied in the notion of 'cyber sovereignty', which advocates an alternative vision to the international liberal order. Fourth, perceiving the norms and behaviour of Russia and China to be producing a security threat has incentivised the US and EU to overcome their contentions in the digital domain, and to adopt a common behaviour within a security alignment between the two sides in order to confront these perceived threats.

Funding

This research is funded by Damascus University – funder No. 501100020595.

Acknowledgements

The authors thank the CEJISS editors and two anonymous reviewers for their valuable notes and suggestions that helped improve the initial version of this article, also we thank the head of the International Relations Department at Damascus University Dr. Khaled Al Masri for his academic guidance, and we extend our gratitude to Mr. Muhammad Omar Al Hamwi for his translation of this article.

Mahmoud Hosh is a master's student in international relations – Faculty of Political Sciences – Damascus University, his research interests are primarily focused on security studies, especially on the study of nontraditional security, he has an article 'Fifth Generation Technologies and their Impact on the Chinese-American Strategic Competition' (in Arabic), published in 'International Journal' of the Syrian International Academy – Damascus.

Dr. Numeir Issa is an assistant professor in the Department of International Relations – Faculty of Political Sciences – Damascus University, he holds a master's degree in political systems from Université Nice Sophia Antipolis, and a PhD from Université de Montpellier, his research interests are primarily focused on European Union studies, and he is currently working on research on 'The Rise of the French Extreme-Right and its Implications for the European Union' (in progress).

References:

Asen, E. (2021): Digital Tax Collection Triggers New U.S. Tariffs on France. *Tax Foundation*, 7 January, <accessed online: https://taxfoundation.org/blog/us-tariffs-on-french-goods-digital-tax-collection/>.

Balzacq, M. & Dunn Cavelty, M. (2016): A Theory of Actor Network for Cyber - Security. *European Journal of International Security,* 1(2), 176–198.

Branch, D. (2020): What's in a Name?: Metaphors and Cybersecurity. *International Organization,* 75(1), 1–32.

Broeders, D., Adamson, L. & Creemers, R. (2019): *A Coalition of the Unwilling?: Chinese & Russian Perspective Cyberspace.* The Hague: The HAGUE Program for Cyber Norms, Leiden Asia Center, & University of Leiden.

Buzan, B. & Hansen, L. (2009): *The Evolution of International Security Studies.* Cambridge: Cambridge University Press.

Buzan, B. & Waever, O. (2003): *Regions and Powers: The Structure of International Security.* Cambridge: Cambridge University Press.

Buzan, B., Weaver, O. & de Wilde, J. (1998): *Security: A New Framework For Analyses.* London: Lynne Rienner Publisher.

Cabinet Office (2011): *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World.* London: Cabinet Office.

Cable, V. (1995): What is International Economic Security. *International Affairs,* 71(2), 305–324.

Cherney, M. (2022): Intel Just Committed Billions to Make Chips in Europe, TSMC Might be Next. *Protocol Website*, 15 March, <accessed online: https://www.protocol.com/enterprise/intel-tsmc-europe-chip-manufacturing>.

China Daily (2014): Key Internet Leaders Agree on Cyber Sovereignty Security. *China Daily,* 21 November, <accessed online: http://www.chinadaily.com.cn/business/tech/2014-11/21/content_18953736.htm>.

Council of The European Union (2022): *Regulation Establishing a Framework of Measures For Strengthening Europe's Semiconductor Ecosystem (Chips Act).* Brussels: Council of The European Union.

Council of The European Union Website (2022): CHIPS ACT: Council Adopts Position. *Council of The European Union*, 1 December, <accessed online: https://www.consilium.europa.eu/en/press/press-releases/2022/12/01/chips-act-council-adopts-position/>.

Davies, C., Jung, S., Inugak, K. & Waters, R. (2022): U.S. Struggles to Mobilise Its East Asia "Chip 4 Alliance". *Financial Times*, 12 September, <accessed online: https://www.ft.com/content/98f22615-ee7e-4431-ab98-fb6e3f9de032>.

Dekker, B., Heijmans, M. & Zhang, M. (2020): *Unpacking China's Digital Silk Road.* The Hague: The Clingendiael Institute.

Dorsey and Whitney Lep Website (2022): The CHIPS and Science Act of 2022: the Impact on China. *Dorsey and Whitney Lep*, 19 September, <accessed online: https://www.dorsey.com/newsresources/publications/client-alerts/2022/09/the-chips-and-sciences-act-of-2022>.

Doshi, R., Bruyere, E., Picarsic, N. & Ferguson, J. (2021): *China as a Cyber Great Power: Beijing's Two Voices in Telecommunications.* Washington DC: The Brookings Institution.

Dunn Cavelty, M. & Wenger, A. (2019): Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy,* 41(1), 5–32.

Dunn Cavelty, M. (2013): From Cyber Bombs to Political Fallouts: Threats Representation With an Impact in The Cyber - Security Discourse. *International Studies Review,* 15(1), 105–122.

Eriksson, J. & Giacomello, G. (2007): Introduction: Closing Gap Between International Relations Theory and Studies of Digital - Age Security. In: Eriksson, J. & Giacomello, G. (Eds.), *International Relations and Security in Digital Age*. London: Routledge, 1–28.

Erkomaishvilli, D. (2019): Alliance Index: measuring Alignment in International Relations. *International Studies,* 56(1), 28–45.

European Commission (2022): *EU-US Trade and Technology Council: strengthening our renewed partnership in turbulent times*. Retrieved from European Commission: <accessed online: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3034>.

European Commission Website (2022): EU – US Trade and Technology Council. *European Commission Website*, 30 May, <accessed online: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/stronger-europe-world/eu-us-trade-and-technology-council_en>.

European Parliament (2000): *Charter of Fundamental Rights of the Europen Union.* Brussels: Official Journal of the European Union.

European Union Center for North Carolina (2014): *The NSA Leaks and Transatlantic Relations.* Chapel Hill: European Union Center for North Carolina.

European Union Websites (2014): 1st EU – U.S. Cyber Dialogue. *European Union,* 12 May, <accessed online: https://www.eeas.europa.eu/node/6800_en>.

Farrell, T. (2002): Constructivist Security Studies: Portrait of a Research Program. *International Studies Association,* 33(2), 49–72.

Federal Ministry of The Interior (2011): *Cyber Security Strategy for Germany.* Berlin: Federal Ministry of The Interior.

Feldstein, S. (2020): How Should Democracies Confront China's Digital Rise?: Weighing the Merits of a T- 10 Alliance. *Council on Foreign Relations*, 30 November, <accessed online: https://www.cfr.org/blog/how-should-democracies-confront-chinas-digital-rise-weighing-merits-t-10-alliance>.

Financial Post Website (2022): US Suggests EU Consider Using Export Limits to Target China. *Financial Post*, 7 October <accessed online: https://financialpost.com/pmn/business-pmn/us-suggests-eu-consider-using-export-controls-to-target-china/>.

Finnemore, M. (2004): *The Purpose of Intervention: Changing Beliefs About the Use of Force.* New York: Cornell University Press.

Finnemore, M. & Hollis, D. (2016): Constructing Norms for Global Cybersecurity. *Amerian Journal of International Law,* 110(3), 425–479.

Finnemore, M. & Sikknik, K. (1998): International Norm Dynamics and Political Change. *International Organization,* 52(4), 887–917.

Flonk, D. (2021): Emerging Illiberal Norms: Russia and China as Promoter of Internat Content Control. *International Affairs,* 97(6), 1925–1944.

Florini, A. (1996): The Evolution of International Norms. *International Security Quarterly,* 40(3), 363–389.

Frieden, K. & Stephanie, T. (2021): State Adoption of European DSTs: Misguided and Unnecessary. *Taxnotes,* 100(6), 577–596.

Jones, S. (1999): Realism and Security Studies. In: SNYDER, C & Carig, S (Eds.): *Contemporary Security and Strategy*. London: Palgrave Macmillan. 53–76.

Geringer, S. (2021): National Digital Taxes - Lessons from Europe. *South African Journal of Accounting Research,* 35(1), 1–19.

Gomes, M. & Whyte, C. (2021): Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly,* 65(4), 1137–1150.

Hansen, L. & Nissenbaum, H. (2009): Digital Disaster, Cyber Security, and The Copenhagen School. *International Studies Quarterly,* 53(2), 1155–1175.

Hass, M. (2005): *Ideological Origins of Great Power Politics.* New York: Cornell University Press.

Hayes, A. (2022): The Supply Chain: From Raw Materials to Order Fulfillment. *Investopedia*, 30 July, <accessed online: https://www.investopedia.com/terms/s/supplychain.asp>.

Hemmings, J. (2020): Reconstructing Order: The Geopolitical Risks in China's Digital Silk Road. *Asia Policy,* 15(1), 5–21.

Kay, S. (2000): What is Strategic Partnership. *Problem of Post - Communism,* 47(3), 15–24.

Kuebris, B. & Badiei, F. (2017): Mapping the Cybersecurity Institutional Landscape. *Digital Policy, Regulation and Governance,* 19(6), 466–492.

Kundnani, H. (2017): *What is International Liberal Order?* Washington DC: The German Marshall Fund of The United States.

Kurowska, X. (2014): Multipolarity as Resistance to liberal Norms: Russia's Position on Responsibility to Protect. *Conflict, Security & Development,* 14(4), 489–508.

Kurowska, X. (2019): *The Politics of Cyber Norms Construction Towards Strategic Narrative Contestation.* Leiden: EU Cyber Direct & Leiden University.

Lawson, S. (2013): Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics,* 10(1), 86–103.

Lindsay, J. (2014): Impact of China on Cybersecurity: Fiction and Friction. *International Security,* 39(3), 7–47.

Lindsay, J. & Gartzke, E. (2020): Politics by many other means: The comparative strategic advantages of operational domains. *Journal of Strategic Studies,* 45(5), 743–776.

Lowry, S. (2019): *Digital Services Taxes (DSTs): Policy and Economic Analysis.* Washington DC: Congressinal Research Service.

Mačák, K. (2017): From Cyber Norms to Cyber Rules: Re-engaging States as Law Makers. *Leiden Journal of International Law,* 30(4), 877–899.

Maigre, M. (2022): *NATO's Role in Global Cyber Security.* Washington, DC: The German Marshall Fund of the United States.

Marconi, M. (2023): *The EU - US Data Protection Framework: Balancing, Security and Privacy Considerations.* Roma: Istituto Affari Internazionali.

Mazarr, M., Priebe, M., Radin, A. & Cevallos, A. (2016): *Understanding The Current International order.* California: RAND Corporation.

Mazarr, M., Frederick, B., Ellinger, E. & Boudreaux, B. (2022): *Competition and Restraint in Cyberspace: The Role of International Norms in Promoting U.S. Cybersecurity.* California: RAND Corporation.

Mearsheimer, J. (2001): *The Tragedy of Great Power Politics.* New York: W.W. Norton Company Inc.

Miller, E. A. & Toritsyn, A. (2005): Bringing the Leader Back in: Internal Threats and Alignment Theory in the Commonwealth of Independent States. *Security Studies,* 14(2), 325–363.

Monaghan, S. (2022): *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice.* Helsinki: The European Center of Excellence for Countering Hybrid Threats.

Nissenbaum, H. (2005): Where Computer Security Meets National Security. *Ethics and Information Technology,* 7(2), 61–73.

North Atlantic Treaty Organization (2014): Wales Summit Declaration. *North Atlantic Treaty Organization*, 5 September, <accessed online: https://www.nato.int/cps/en/natohq/official_texts_112964.htm>.

North Atlantic Treaty Organization (2020): *Allied Joint Doctrine for Cyberspace Operations.* Brussels: NATO Standardization Office (NSO).

North Atlantic Treaty Organization (2023): Cyber Defence. *North Atlantic Treaty Organization*, 14 September, <accessed online: https://www.nato.int/cps/en/natohq/topics_78170.htm>.

Ottis, R. (2007): *Analysis of Cyber Attacks Against Estonia from the Information Warfare Perspective.* Tallinn: Cooperative Cyber Defence Center for Excellence.

Pierre, A. J. (2002): *Coalitions: Building and Maintenance.* Washington: Georgetown University.

Pijović, N. (2021): The Cyberspace "Great Game". The Five Eyes, the Sino - Russian Bloc and Growing Competition to Shape Global Cyberspace Norms. *13th International Conference on Cyber Conflict*. Tallinn: NATO CCDCOE Publications, 215–231.

Posen, P. (1993): The Security Dilemma and Ethnic Conflict. *Survival: Global Politics and Strategy,* 35(1), 27–47.

Ragonnand, G. (2022): *The EU Chips Act Securing Europe's Supply of Semiconductors.* Brussels: European Parliamentary Research Science.

Renard, T. (2018): EU Cyber Partnerships: Assessing the EU Strategic Partnerships with third Countries in the Cyber Domain. *European Politics and Society,* 19(3), 321–337.

Retamero, G. R., Müller, S. & Rousseau, D. (2012): The Impact of Value Similarity and Power on The Perception Threat. *Political Psychology,* 33(2), 179–193.

Rousseau, D. & Retamero, G. R. (2007): Identity, Power, and Threat Perception: A Cross - National Experimental Study. *Journal of Conflict Resolution,* 51(5), 744–771.

Security Council of the Russian Federation (2016): Doctrine of Information Security of the Russian Federation. *Security Council of the Russian Federation*, 5 December, <accessed online: http://www.scrf.gov.ru/security/information/DIB_engl/>.

Shead, S. (2021): Investors are Going Wild Over a Dutch Chip Firm. *CNBC Website*, 24 November, <accessed online: https://www.cnbc.com/2021/11/24/asml-the-biggest-company-in-europe-youve-probably-never-heard-of.html>.

Smeets, M. (2020): U.S. Cyber Strategy of Persistent Engagement & Defend Forward: Implications for the Alliance and Intelligence Collection. *Intelligence and National Security,* 35(3), 444–453.

Snyder, G. (1990): Alliance Theory: A Neorealist First Cut. *Journal of International Affairs,* 44(1), 103–123.

Solms, V. & Heerden, V. (2015): The Consequences of Edward Snowden NSA Related Information Disclosures. *Proceedings of the 10th International Conference of Cyber Warfare and Security (ICCES)*. Kruger National Park: Council for Scientific and Industrial Research, 358–368.

Subotić, J. (2016): Narrative, Ontological Security, and Foreign Policy Change. *Foreign Policy Analysis,* 12(4), 610–627.

Sukhankin, S. (2018): Moscow Pushes own Approaches to Cyber Security on Rest of CSTO. *The Jamestown Foundation: Global Research & Analysis*, 26 September, <accessed online: https://jamestown.org/program/moscow-pushes-own-approaches-to-cyber-security-on-rest-of-csto/>.

Taiwan Semiconductor Manufacturing Company (2022): *TSMC Announce Update for TSMC Arizona.* Taipei : Taiwan Semiconductor Manufacturing Company.

The European Network and Information Security Agency (2012): *National Cyber Security Strategy: Practical Guide on Development and Execution.* Athena: The European Network and Information Security Agency.

The European Parliament & The Council of the European Union (2016): *Regulation (EU) 2016/679 of the European Parliament and of the Council.* Brussels: Official Journal of European Union.

The European Union (2013): *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.* Brussels: The European Union.

The U.S. Bureau of Industry and Security (2022): *Commerce Implements New Export Controls on Advanced Computing and Semiconductor Manufacturing Items to The People's Republic of China (PRC).* Washington DC: The USA Bureau of Industry and Security.

The White House (2010): *National Security Strategy.* Washington DC: The White House.

The White House (2011): *International Strategy for Cyberspace: Prosperity, Security and Openness in Networked World.* Washington DC: The White House.

The White House Website (2022a): Executive Order on The Implementation of The CHIPS ACT of 2022*. The White House*, 25 August, <accessed online:https://www.whitehouse.gov/briefing-room/presidential-actions/2022/08/25/executive-order-on-the-implementation-of-the-chips-act-of-2022/>.

The White House Website (2022b): Fact Sheet: U.S. – EU Trade and Technology Council Advances Concrete Action on Transatlantic Cooperation. *The White House*, 5 December <accessed online: https://www.whitehouse.gov/briefing-room/statements-releases/2022/12/05/fact-sheet-u-s-eu-trade-and-technology-co>.

Torreblanca, J. & Ricart, R. (2022): *The U.S. – EU Trade and Technology Council (TTC): State of Play, Issues and Challenges For The Transatlantic Relationship.* Paris: Open Internet Governance Institute.

Traynor, T. (2013): New EU rules to curb transfer of data to US after Edward Snowden revelations. *The Guardian*, 17 October <accessed online: https://www.theguardian.com/world/2013/oct/17/eu-rules-data-us-edward-snowden>.

U.S. State Department Website (2022): U.S. – EU Trade and Technology Council (TTC). *U.S. State Department*, <accessed online: https://www.state.gov/u-s-eu-trade-and-technology-council-ttc/>.

U.S. Department of Commerce (2017): *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally.* Washington DC: U.S. Department of Commerce.

U.S. Department of Commerce (2022): *U.S. – EU Joint Statement of The Trade and Technology Council.* Washington DC: U.S. Department of Commerce.

Walling, C. (2013): *All Necessary Measures: The United Nations and Humanitarian Intervention.* Philadelphia: University of Pennsylvania Press.

Waltz, K. (1979): *Theory of International Politics.* Boston: Addison-Wesley Publishing Company.

Wang, A. (2020): Cyber Sovereignty at Its Boldest: A Chinese Perspective. *Ohio State Technology Law Journal,* 16(2), 396–466.

Wendt, A. (1992): Anarchy is What State Make of it: The Social Construction of Power Politics. *International Organization,* 46(2), 391–425.

Wilkins, T. (2012): ‘Alignment’, Not ‘Alliance’ - The Shifting Paradigm of International Security Cooperation: Toward a Conceptual Taxonomy of Alignment. *Review of International Studies,* 38(1), 35–76.