**Propósitos y Representaciones**
ISSN 2307-7999
e-ISSN 2310-4635

Jan. 2021, Vol. 9, SPE(1), e850
Special Number: Educational practices and teacher training
http://dx.doi.org/10.20511/pyr2021.v9nSPE1.850

**RESEARCH ARTICLES**

# Copenhagen school and securitization of cyberspace in Turkey

## Escuela de copenhague y titulización del ciberespacio en turquía

**Didem Aydindag**
University of Kyrenia, Turkey
ORCID: https://orcid.org/0000-0002-4752-5037

**Received** 08-12-20 **Revised** 09-30-20 **Accepted** 10-13-20 **On line** 01-12-21

***Correspondence**

Email: Didem@mail.ru

**Cite as:**

Aydindag, D. (2021). Copenhagen school and securitization of cyberspace in turkey. *Propósitos y Representaciones, 9* (SPE1), e850. Doi: http://dx.doi.org/10.20511/pyr2021.v9nSPE1.e850

## Summary

With a particular rise since the turn of the millennium, cyber-security become one of the most important security sector in contemporary security politics. Despite this, the convergence of cyberspace and security has mostly been analyzed within the context of technical areas and had been neglected in the political realm and international relations academia. The article argues that in line with developments in the domestic and international arena, the AKP government shifted towards the securitization of cyberspace. Secondly the article argues that there seems to be two waves of securitization and desecuritization within the case. The first wave starts from 2006 through the end of 2017 whereby cyber securitization took place within the subunit level and very much connected to political and societal sectors. This first wave particularly heightened after the 2016 attempted coup and the eventual collapse of the peace process with the PKK. The second wave came in the 2018 onwards and instead of securitization, there is a desecuritizationn of cyber attacks took place mostly at the unit level. In both waves, the desecuritization and securitization is constructed within the national security discourse. However in the first wave, a threat to national security is constructed and hypersecuritized particularly in relation to developments at the societal level. In the second wave, the emphasis is put on the strength of national security therefore the threats and cyber-attacks at the unit level that are originated from other states is downplayed in order to construct a national pride and strength. The main goal of this article therefore is to fill the gap in the Copenhagen school related to cyber security sector. The second aim is to fill the gap specifically in Turkey's response to events in cyberspace and construction of a cybersecurity discourse and culture

**Keywords:** Copenhagen School, securitization, cyberspace, Turkey, cybersecuritization, critical security studies.

## Resumen

Con un aumento particular desde el cambio de milenio, la ciberseguridad se convirtió en uno de los sectores de seguridad más importantes en la política de seguridad contemporánea. A pesar de esto, la convergencia del ciberespacio y la seguridad se ha analizado principalmente en el contexto de las áreas técnicas y se ha descuidado en el ámbito político y la academia de relaciones internacionales. El artículo sostiene que, de acuerdo con los desarrollos en el ámbito nacional e internacional, el gobierno del AKP se inclinó hacia la titulización del ciberespacio. En segundo lugar, el artículo sostiene que parece haber dos oleadas de titulización y desecuritización dentro del caso. La primera ola comienza desde 2006 hasta fines de 2017, en la que la titulización cibernética tuvo lugar dentro del nivel de subunidades y muy conectada con los sectores políticos y sociales. Esta primera ola se intensificó particularmente después del intento de golpe de 2016 y el eventual colapso del proceso de paz con el PKK. La segunda ola se produjo en el 2018 en adelante y en lugar de titulización, hay una desecuritización de los ataques cibernéticos que se llevaron a cabo principalmente a nivel de unidad. En ambas oleadas, la desecuritización y la titulización se construyen dentro del discurso de seguridad nacional. Sin embargo, en la primera ola, se construye y se hipersecuritiza una amenaza a la seguridad nacional, particularmente en relación con los desarrollos a nivel social. En la segunda ola, el énfasis se pone en la fuerza de la seguridad nacional, por lo que se minimizan las amenazas y ataques cibernéticos a nivel de unidad que se originan en otros estados para construir un orgullo y una fuerza nacional. Por lo tanto, el objetivo principal de este artículo es llenar el vacío en la escuela de Copenhague relacionado con el sector de la seguridad cibernética. El segundo objetivo es llenar el vacío específicamente en la

respuesta de Turquía a los eventos en el ciberespacio y la construcción de un discurso y una cultura de ciberseguridad.

**Palabras clave:** Copenhagen School, titulización, ciberespacio, Turquía, cibersecuritización, estudios críticos de seguridad

## Introduction

with a particular rise since the turn of the millennium, cyber-security become one of the most important security sector in contemporary security politics. despite this, the convergence of cyberspace and security has mostly been analyzed within the context of technical areas and had been neglected in the political realm and international relations academia.

in the political realm the securitization of cyberspace has gained impetus following the cyber-attacks against the usa by china in 2006, against estonia in 2007 by russia , against syria by israel in 2007, against afghanistan by germany in 2008, against china by iran in 2010, and against iran by israel and the usa in 2010 (stuxnet). these incidents along with many more has led the countries to establish more clear-cut responses against cyber threats and cyber-attacks. in military-strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space (deibert & rohozinski, risking security: policies and paradoxes of cyberspace security., 2010, s. 16).

with these developments there is an increasing literature regarding the relevance of cyber security within the framework of international relations (dunn cavelty & wenger, 2020; akdağ, 2019; gill, 2019; stevens, 2018; collier, 2018; buchanan, 2016; valeriano & manessa, 2015; bıçakcı, 2014; tikk, 2011; dunn cavelty, 2013; kremer & müller, 2013; choucri, 2012; nye, 2011; hansen & nissenbaum, 2009; eriksson & giacomello, 2007; nissenbaum, 2005; nissenbaum, 2004; der derian, 2003; deibert, 2003; rosenau & singh, 2002; saco, 1999), among those most of them focus on cyber security within the traditional framework of national security blocks such as the usa, china, the eu and russia (rehrl, 2017; sharp, 2017; geers, 2014; cavelty dunn, kristensen, & soby, 2008; wilner, 2020; weber, 2018; deibert, rohozinski, & crete-nishihata, 2012; lobato & kenkel, 2015) and international norm-settings (lin, 2012; polański, 2017; mačák, 2017; porcedda, 2018; georgieva, 2020). there is a limited literature on critical security studies that focus on cyber security (saco, 1999) and the conceptualization of copenhagen school (hansen & nissenbaum, 2009; geelen, 2016; fouad, 2019; lacy & prince, 2018) within them main focus is on discourses of government officials (lobato & kenkel, 2015; lee & macdonald, 2016). cyber securitization literature remains very limited in research related to turkey and their main focus is on international relations in general (bıçakcı, ergun, & çelikpala, 2015). the remaining research taking turkey as case study either focus on the technical/ sectoral analysis (yesil, sözeri, & khazraee, 2017; sari, 2019), legislation (taşçı & can, 2015), or social media analysis (bulut & yörük, 2017).

as seen in the existing literature the concept of cybersecurity is still a novelty in many policy actors and academics. the main goal of this article therefore is to fill the gap in the copenhagen school related to cyber security sector. the second aim is to fill the gap specifically in turkey's response to events in cyberspace and construction of a cybersecurity discourse and culture. the choice of copenhagen school for analyzing the state and cyberspace relationship is because it allows analyzing the interplay between different levels of analysis and different sectors. secondly securitization theory which blends well with the constructivist stand allows individual agents to be more active in constructing cyberspace as a national security concept (aydindag & ısiksal, (de) securitization of ıslam in turkey, 2018). however, there are certain gaps in copenhagen school with respect to individual level of analysis and the cybersecurity sector which is mainly

out of the five main sectors of securitization. hence the article will try to overcome these gaps, through a case study of turkey.

the article analyzes these aspects through primary and secondary resources including but not limited to legislations and official statements, reports of international and national organizations, newspapers, reports by think-tanks and security firms. the article argues that in line with developments in the domestic and international arena, the akp government shifted towards the securitization of cyberspace. secondly the article argues that there seems to be two waves of securitization and desecuritization within the case. the first wave starts from 2006 through the end of 2017 whereby cyber securitization took place within the subunit level and very much connected to political and societal sectors. this first wave particularly heightened after the 2016 attempted coup and the eventual collapse of the peace process with the pkk. the second wave came in the 2018 onwards and instead of securitization, there is a desecuritizationn of cyberattacks took place mostly at the unit level. in both waves, the desecuritization and securitization is constructed within the national security discourse. however in the first wave, a threat to national security is constructed and hypersecuritized particularly in relation to developments at the societal level. in the second wave, the emphasis is put on the strength of national security therefore the threats and cyber-attacks at the unit level that are originated from other states is downplayed in order to construct a national pride and strength.

the first part of the article will give a brief discussion of the copenhagen school and how cyberspace fits into the critical security studies in general. the later sections analyze specifically how turkey responds to cybersecurity issue; what is constructed as a threat and what is not and how the government responds to these threats or threat perceptions.

## copenhagen school of security and cyberspace

the copenhagen school conceptualized securitization as the discursive and political process through which an inter-subjective understanding is constructed within a political community to treat something like an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with the threat (buzan, waever, & de wilde, 1998: 30). in that respect, the 'referent object' is the object that is claimed to be threatened and holds a general claim on 'having to survive.' additionally, there are 'securitizing actors' who make the claim through speech acts and audience. speech acts point to an existential threat to this referent object and thereby legitimize extraordinary measures (buzan, waever, & de wilde, 1998: 32).

mostly known through barry buzan, ole wæver and jaap dewilde, the importance of copenhagen school is that it has a social viewpoint to security studies. copenhagen school more elaborately systematized the deepening and widening of the security studies firstly through sectors and levels of analysis and secondly through the securitization theory.

buzan sets out five security sectors and five levels of analysis in security studies. the sectors are political, societal, environmental, military and economic. the levels of analysis are; systemic, sub-systemic, unit, subunit and finally individual (buzan, waever, & de wilde, 1998:7). the upcoming sections builds cyberspace among those 10 dyads of sectors and levels of analysis synthesis and focus on the theory's strengths and weaknesses regarding particularly the individual level and cyber security's relationship with these main five sectors.

copenhagen school argues that security is the action that takes politics and frame the issue as a special kind of politics or above politics. to put in other words, securitization in that respect is a more extreme version of politicization. copenhagen school's main contribution to security studies literature is this concept of securitization. "when an issue is presented as an existential threat, requiring emergency measures and justifying actions outside the normal bounds of political procedure" that issue becomes securitized (buzan, waever, & de wilde, 1998: 24). this brings forth another aspect of securitization as a means of legitimization. according to taureck, three steps are

needed for successful securitization: the "identification of existential threats", "emergency action", and the "legitimization of exceptional measures" (taureck, 2006). thus, securitization is applied to legitimize a political action that might not otherwise considered as legitimate. to put it in other words, securitization is the "discursive and political process through which an inter-subjective understanding is constructed within a political community to treat something as an existential threat to a valued referent object, and to enable a call for urgent and exceptional measures to deal with that threat" (buzan, waever, & de wilde, 1998: 25). however, the research argues that securitization in addition to being political also sociological process manifest in language, history and culture, in effect of interest, power, process, bureaucratic position, and inter-subjectivity (aydindağ, işiksal, 2018). in different settings, different linguistic rules, and different cultures, securitizing moves have different effects which provide various power dynamics (salter, 2008). securitizing moves use a unique language with a particular heritage, history, and heft - fundamentally different from securitizing moves within elite or technocratic settings (salter, 2011). the sociological view shows that within the configuration of circumstances such as context, cultural background, psychological background, and the power that audience and securitizing actor brings to interaction, the securitization is better understood as a pragmatic process. furthermore, a distinct kind of agency is manifested by the discourse of securitization, which reproduces and transforms, through judgement and habit, these structures, in response to problems posed by various historical context (emirbayer and mische 1998:970).

thirdly, the sociological view emphasizes, the mutual constitution of securitizing actors and audiences. in that respect, the units of security analysis are the 'referent object' which is the "object that is/ claimed to be threatened and holds a general claim on 'having to survive".' in addition to that, there are 'securitizing actors,' through speech act this is the person "who makes the claim of pointing to an existential threat to the referent object and therefore legitimizing extraordinary measures, often but not necessarily to be carried out by the actor itself" (buzan, waever, & de wilde, 1998: 29), 'functional actor(s) "who affect the dynamics of a sector. without being the referent object or the securitizing actor", this is an actor who significantly influences decisions in the field of security, finally 'audience'; "those who have to be convinced in order for the speech act to be successful" (buzan, waever, & de wilde, 1998: 26). hence securitization process by the agency of securitizing actor inherently involves an individual level of analysis dimension due to the fact that the designation of the securitization process relies heavily on the agent's capacity.

since securitization is mainly explained through speech act then desecuritization means the lack of this speech act. thus, not to talk about an issue in terms of security entails the desecuritization of that issue. behnke defines desecuritization as "the lack of any securitizing speech act" (behnke, 2006), since securitizing speech is considered evidence for securitization, lack of such speech must be enough to show desecuritization. in similar vein, oelsner argues one way of an issue transcending security language is that the issue may lose being a threatening image, because the nature of the threat becomes void for agent and the audience altogether. however, this kind of loss of threat perception involve no action on the part of audience or the agent; the threat just loses its capability. despite, this is not the case, in addition to the real changes in the threat itself what changes is that the intersubjective perceptions of the threat, the outcome of this mechanism may well just be indifference (oelsner, 2005). as seen in the next sections of the article desecuritization of cyber space at the unit level is constructed in the 2018 onwards mostly, in order to prove the strength and ability of the state/regime.

ironically though, although cyber security is acknowledged in the original a framework for analysis it was not considered essential, since it was not considered as an existential threat to states due to its lack of "cascading effects on other security issues" (buzan, waever, & de wilde, 1998:25). fast-forward to second half of 2000s cyber security become a national security concern for most of the states and cyber defence became nato's core task of collective defence (nato, 2020). in the move from "computer security" to "cyber security", the technical discourse is linked to securitizing discourse" developed in the specialized arena of national security" (nissenbaum,

2005:65). the main conceptualization of cyber security within the copennhagen school framework came from lena hansen and helen nissenbaum's 2009 article "digital disaster, cyber security, and the copenhagen school", which will be further analyzed in coming sections.

## conceptualization of security sectors

sectors identify specific types of interaction regarding security. copenhagen school rejects the classical security studies limiting security into single – military- sector and construct a more radical view that is towards military as well as non-military threats to security. certain values and units are particular only to that of certain sectors, it is normal since the main purpose of sectors is to differentiate those types of interactions. in that respect, the nature of survival and threat will differ across different sectors and types of unit (buzan, waever, & de wilde, 1998: 27). in security: a new framework for analysis, buzan sets out 5 security sectors as following: military, political, societal, economic and environmental. this conceptualization is based on four non-military security sectors contributing to an understanding of the non-military aspects of security and provide analytical categories in researching those non-military aspects. as such, looking at security studies from a sectoral view can be regarded as 'widening' of the traditional security studies.

societal security concerns the societies. its referent object is largescale collective identities that can function independent of the state such as religion and nation. the threats to societal security can be migration, vertical and horizontal competition or depopulation. military security concerns the "two-level interplay of the armed offensive and defensive capabilities of the state" (buzan, waever, & de wilde, 1998: 8). the sector implies that the state is the main referent object and the ruling elites are the most important securitizing actors. because force is particularly effective as a way of acquiring and controlling a territory, the fundamentally territorial nature of the state underpins the traditional primacy of its concern with the use of force (buzan, waever, & de wilde, 1998:22). the threats to territorial integrity mostly explained through external and military nature. furthermore, military vehicles have an important dominance over the outputs of all other sectors (waever, 1993). due to the fact that the most visible part of state behavior, it is the most prominent sector among the others. environmental security concerns the "maintenance of the local and the planetary biosphere as the essential support system on which all other human enterprises depend" (buzan, waever, & de wilde, 1998:8). in the environmental sector environment itself and the nexus of civilization are referent objects. the economic sector deals with access to resources, finance and markets necessary to sustain acceptable levels of welfare and state power. there are many referent objects within the economic sector, state being one of those, but other referent objects from different levels of analysis may exist such as in the system and subsystem levels; the world bank, the eu, or more abstractly international liberal economic order. finally political security concerns the organizational stability of state, systems of government and the ideologies that give them legitimacy. in the political sector, state sovereignty or its ideology is the referent object. sovereignty can be existentially threatened by anything that questions recognition, legitimacy or governing authority. political sector is the widest sector and also a residual category. in a way all security is political and to securitize is also a political act. thus, in a sense societal, economic, environment, and military security really mean "political-societal security", "political – economic security" and so forth (buzan, waever, & de wilde, 1998:143).

cyber sector is mainly built upon the framework of hansen and nissenbaum's article "digital disaster". similar to environmental sector and to a degree economic sector, the cyberspace sector easily transpass national borders and the threats to cyberspace sector also go beyond the national borders. cavelty argues that "cyber security and national security differ most decisively in scope, in terms of actors involved and in their referent objects" (dunn cavelty, 2012). hansen

and nissenbaum point out that the importance of cyber security in international relations and securitization theory as follows:

cyber securitizations are particularly powerful precisely because they involve a double move out of the political realm: from the politicized to the securitized, from the political to the technified, and it takes an inter-disciplinary effort to assess the implications of the move, and possibly to counter it . . . cyber security stands at the intersection of multiple disciplines and it is important that both analysis and academic communication is brought to bear on it. the technical underpinnings of cyber security require, for instance, that ir scholars acquire some familiarity with the main technical methods and dilemmas, and vice versa that computer scientists become more cognizant of the politicized field in which they design and how their decisions might impact the (discursively constituted) trade-offs between security, access, trust, and privacy.

hansen and nissenbaum identify three discourses with different referent objects and separate forms of securitization grammer and specific speech acts for securitization. these three securitization modes are; hypersecuritization , everyday security practices and technifications.

hypersecuritization which was originally introduced by buzan (buzan, 2004:172) describe an moving securitizaiton beyond the normal levels of threat by defining " a tendency both to exaggerate threats and to resort to excessive countermeasures". ın cyber security realm hypersecuritization imply the manner in which cyber security discourse hinges on multi dimensional cyber disaster scdenerious and neither of these scenerious have so far taken place (hansen & nissenbaum, 2009: 1164). everyday security practice meanwhile relies on paris school of security studies since the audience is only briefly described in a framework for analysis (1998). thierry balzacq developed the concept through explaining the importance of audience since ''the success of securitization is highly contingent upon the securitizing actor's ability to identify with the audience's feelings, needs, and interests,'' and that ''the speaker has to tune his⁄her language to the audience's experience'' (balzacq 2005:184). audiences do not exist ''out there'' but are constituted in discourse, and security discourses draw boundaries around the ''we'' on whose behalf they claim to speak, and the ''you's'' who are simulta- neously addressed by the linking of fears and threats to ''feelings, needs and interests.'' (hansen & nissenbaum, 2009: 1165). importance of everyday securitization in the concept of cyber securitization is that even those who doesn't own internet or computers in general still are subject to consequences of immidiate danger. therefore "experiences of threats are not cases of individual security or crime but are constituted as threats to the network and hence the society (hansen & nissenbaum, 2009: 1165). technification is a result of logic of securitization since it gives a privilaged role to computer and information scientists within the cyger security discourse (hansen & nissenbaum, 2009: 1167). inherently it implies the threat is so big and important that ordinary polğiticians or amateurs can not handle it. it constructs the technical as a domain requiring an expertise that the public and politicians do not have annd therefore these scientistst become securitizing actors all the while in the eyes of the audience having the prerogative of not being accused or questioned if being politicized or having an ulterior motive. as seen in the turkish case most of the securitizing o desecuritizing actors are owners of cyber security firms or academia belonging to technical fields.

## A) interconnectedness of sectors

in reality a security issue is not necessarily sector dependent. there is often a dynamic transition between different sectors. sectors are lenses focusing on the same world, they are not ontologically separate realms. the purpose of desegregating is to put security back to a more transparent form (buzan, waever, & de wilde, 1998: 167). problems on the surface seem to be societal might turn out to be motivated by threats of the other four sections. for example, some actors such as states may appear in all of the sectors whether as a securitizing actor, functional actor or threat. a specific security analysis does not start by separating the world into sectors, it starts as a phenomenon and then the units become legitimate referent object for security action and finally the pattern of mutual references among units. looking sector by sector may risk of

missing intense security dilemmas in cases where a threat in one sector, may be securitized in another sector.

within the cyber security sector, it is often agreed that there are multiple discourses however there are different views regarding the referent objects of this sector. one view argues that there are separate referent objects within the cyber sector (deibert, 2002) the other view argue that multi discursivity arise from "competing articulations of constellations of referent objects" (hansen & nissenbaum, 2009:1163; saco, 1999). as explained in turkey's case below, particularly in line with the gezi park protests and collapse of pkk peace process and the government rhetoric on legitimizing the internet surveillance, censorship and blockings of social media platforms through referencing "national security" and "protection of child and family". the case points out the linkage between the individual unit of analysis to unit annd subunit levels of analysis. at the same time these levels of analysis act collective referent objects, in which the individual of the rhetoric is linked to societal sector and the political sector and become those sectors' referent objects. as argued by saco within the case of september 11, the discourses are not separate with unrelated referent objects but competing articulations of the appropriate individual-state contracts of the state (saco, 1999).

## securitization of cyberspace at the subunit level and linkages between sectors

although legislation against cybercrimes took part early on in turkish penal system, the institutionalization and the scope of crimes were relatively limited. the first criminalization was mainly technical in nature. the first law was introduced in 1991 in the turkish penal code number 765, (tck) law no. 3756. it was included into article 20 of the amendments to "the crimes in the informatics department", through the clause 525 / a, b, c and d (tbmm, 1991). the article penalized the unlawful seizure of programs, data, and other elements from a computer system along with their use, transfer, or copy with the aim of unlawful control of assets. with the turn of the new millennium, the penalization also become more elaborated. turkish penal code no. 5237, implemented in september 2004, acknowledged the notion of cyber-crime within the framework of the penal code both extending its definition, and section 10 of the turkish penal code, titled "information technology (it) crimes" (bıçakcı, ergun, & çelikpala, 2015) included protection against stealing, unlawful give or take or use personal data. furthermore the institutionalization of cyber security began to show up in 2005 through the establishment of office of crimes committed through informatics under the public order branch office and also the directorate of telecommunication and communication (tib) under information and communication technologies authority (btk) although it was shut down in august 2016.

the securitization of cyberspace began in the second term of the akp. with a change made in 2006, cybercrime is included in the anti-terrorism law no. 3713. the amendment includes the following statement: "if the following crimes are committed within the framework of the activity of a terrorist organization established to commit a crime for the purposes stated in article 1, such as unauthorized access to the system, system blocking, data corruption and modification, some other crimes that can be committed through information systems are also included in this article. according to the article 2 of the anti-terrorism law, even if individuals are not members of a terrorist organization, they are considered terrorists and punished like members of an organization if they commit a crime on behalf of a terrorist organization. the reasons for this shift can be found in the era that brought several different dynamics at the societal sector that eventually led to cyber-securitization. the first dynamic was the presidential elections. the existing president was ahmet necdet sezer, a former judge, a hardline secularist and whose term in the office would end in 2007. as the president was elected with a majority vote of the assembly, this meant that the ruling party would have the power to appoint a like-minded 'conservative-democrat' president. the akp's presidential candidate was abdullah gül, who was also one of the founding members of the party. the effect of the possibility of having an akp-based president, in addition to being the ruling party, on societal securitization was twofold. the first one could be defined as political-military sector interrelatedness. as mentioned above, the military has always been a securitizing actor of secularism in the turkish political arena, generally considering themselves as the guardians of the

republic and ataturk's reforms, most importantly secularism. on the eve of the presidential election, the then chief of general staff, yaşar büyükanit published an 'online memorandum' that arguably was considered as an indirect military coup. he stated that 'the problem that emerged in the presidential election process is focused on arguments over secularism. the turkish armed forces are concerned about the recent situation…the turkish armed forces are a party in those arguments, and absolute defender of secularism' (excerpts of turkish army statements, 2007). in line with the online memorandum, president ahmet necdet sezer also became involved in the process, warning that the country's secular system faced its greatest threat since the founding of the republic in 1923 (rainsford, 2007). here, having the bureaucracy and the military acting as securitizing actors implied that having a pro-islamist president created an existential threat to secular identity. the securitization of identity was successful since audience response was the mass 'republic protests' gathered through facebook and twitter and led by several civil society organizations in tandoğan square in the capital city ankara. the slogans included 'turkey is secular and secular it will remain' (*türkiye laiktir, laik kalacak*) (evrensel.net , 2007). in february 2008, the parliament voted to amend turkey's constitution by eliminating the ban on headscarves being worn on university campuses. the headscarf issue, dormant during the first term of the akp government, suddenly became the number one issue of desecuritization in early 2008. erdoğan, in a speech act in madrid, stated that the ban should be lifted even if the headscarf is used as a political symbol. he added that there was no need to wait for the adoption of a new constitution and the problem could be solved by a simple 'one sentence' constitutional amendment. this dichotomy caused a backlash from the secular public and secular elite establishments. they argued that it represents a threat against turkey's secular identity, because it might put pressure on women who choose not to wear a headscarf. the islamists, on the other hand, argued that it is a human right to wear religious symbols in public spaces. this dichotomy resulted in a closure case for the akp. however, the constitutional court did not ban the party and erdoğan was not banned from politics. in fact, akp, under erdoğan's leadership, was extremely careful to function within the limits of secular laws. the 2008 ergenekon and 2010 sledgehammer cases changed the dynamics in the civil-military and islamic-secular relationships. the ergenekon trials involved high ranking military officials, judiciary, and journalists, all alleged to be members of the ergenekon organization. ergenekon was a supposedly secular clandestine organization plotting against the akp. operation 'sledgehammer' was the name of an alleged turkish secularist military coup plan dating back to 2003, in response to the akp's victory.

the state response to these incidents was increased control of the internet which began in 2007 through denying access to websites and/or filtering the contents of those websites by either blocking the ip addresses or domains, servers and keywords. the securitization rhetoric was based on protection of family and children, and in fact turkey's first internet law no. 5651 entitled "regulation of publications on the internet and suppression of crimes committed by means of such publications" was approved in may 2007 with the stated objective of protecting families and minors. however the offer of "child" and "family" filtering options have been criticized as arbitrary and discriminatory, since the child filter obstructs access to facebook, youtube, yasam radyo (life radio), the armenian minority newspaper *agos*, and several websites advocating the theory of evolution (freedom house, 2019). the organization's acronym in turkish "tib" which controlled online content and direct hosting had become synonymous for internet censorship until its closure in the post coup-attempt, also youtube was inaccessible between 2008 and 2010. although youtube was officially banned in turkey, the website was still accessible by modifying connection parameters to use alternative dns servers. responding to criticisms of the courts' bans, in november 2008 the prime minister recep tayyip erdoğan stated ironically "i do access the site. go ahead and do the same." in june 2010, turkey's president abdullah gül used his twitter account to express disapproval of the country's blocking of youtube, which also affected access from turkey to many google services (ntvmsnbc, 2008). the restrictions on internet access had accelerated to such an extent that on march 11, 2010, reporters without borders added turkey to the list of "countries under surveillance." the ankara-based association of internet technologies filed a complaint about website blocking to the european court of human rights (echr), accusing

the turkish authorities of violating freedom of expression the echr (2013) ruled that the turkish internet law was against the european convention on human rights (eldem, 2020).

the second wave came with the spillover effect of arab uprisings in the environmental-political sector through the gezi park protests of 2013. taksim square and gezi park, as symbols of secularism and progress, were planned as urban spaces that would make the republic permeate into the daily lives of the newly secular society along with solving the problems of urban transportation, hygiene/ecology and aesthetics (baykan & hatuka, 2010). the akp's attempt at building a mosque in the square and erdoğan's persistence in demolishing the atatürk cultural center (akm), the secular symbol of westernization through ballet and other performances became the concrete examples of cultural transformation of erdoğan from conservative democracy to islamist identity. the protests in itself was a dual securitization and counter securitization move from both the secular and religious establishments. the protests which started as a peaceful environmental demonstration against the confiscation of a historical park for the building of a shopping mall, faced with denial of the right to peaceful assembly and un-proportional police attacks. from the very beginning the gezi protests were not solely a crisis at the environmental sector (aydindag, 2019:1031). demonstrations were against erdoğan government's perceived religious conservatism. it was the largest mass protest in a decade. as mentioned earlier one of the most problematic area of copenhagen school's securitization theory was the speech act. the non-verbal attempts at securitization such as protests and demonstrations done by actors usually considered as audience is sidelined. in copenhagen school structure securitization presents a linear dynamic of security construction, starting with a securitizing actor who constructs a referent object and a threat. this narrative of existential threat is then either accepted or rejected by an audience, thus determining the outcome of the securitizing move. in practice, however, the process may start at any point, with the component parts of the securitization developing simultaneously and being mutually constitutive (wilkinson, 2011) and done simultaneously by varying actors whether the actors normally in the sphere of audience or functional actors. tayyip erdoğan called protestors looters (the guardian, 2013).

his speech act institutionalized the juxtaposition of national identity and societal identity. cyber securitization took on the form of heavy censorship on media and blockading the internet websites with an overnight bill that allowed the government to block internet trafficking (reuters, 2014) further fueled the rage. most infamous media censorship occurred when the mainstream media did not broadcast any news regarding the demonstrations for three days. the lack of media coverage was symbolized by cnn international covering the protests while cnn turk broadcasting a documentary about penguins at the same time (oktem, 2013). the radio and television supreme council (rtük) controversially issued a fine to pro- opposition news channels such as halktv for their broadcasting of the protests, accusing them of morally, physically and mentally de-stabilizing the children (özgenç, 2013). news, like security, is a social construction. news reflect the construction and inorganic process that reflect the culture in or for which news is produced and how the audience should feel about the constructed data (vultee, 2011: 93). whether it's penguins or issuing of a fine and daily ban on channels produce the same securitization attempt by the secular audience and later securitizing actors. the centrality of media accounts in forming and shaping public opinions point to the relevance of media models in understanding the securitization process. balzacq suggests repurposing securitization as a pragmatic act: "a sustained argumentative practice aimed at convincing a target audience to accept the claim that a specific development is threatening enough to deserve an immediate policy to curb it" (balzacq, 2009: 60). this social-constructivist approach raises several elements to the level of the speech act - the "securitizing move" - itself: not just the actor who "speaks security," but the target audience of the move and the context in which it is made; media frame. gezi protests created a rupture in akp's legitimacy of responding to varying societal demands. instead of answering to those demands

erdoğan's marginalizing rhetoric and coercion created to identify erdoğan with the secular-pious separation in a cultural polarization reflected in political sector. (mis & aslan, 2018:29)

aligned with these it wasn't unexpected that in 2013 national cyber security strategy (ncss) was published. the publication focused on information systems of critical infrastructures such as electronic communication, energy, water management, critical public services, transportation, and banking and finance (eldem, 2020:10). anti-terror law which was already included cyber crimes had been extensively used for individuals, social media applications which were operable for organizing large gatherings such as twitter, youtube, facebook government agencies put on a close surveillance for activities that are deemed against the government. here one can also see the main problem with the copenhagen school's securitization theory: focusing solely on the speech act as securitization tool is misleading because there are practices or physical or visual actions that are excluded which do not follow the securitizing speech act "format", but are part of the process where meanings of security are communicated and constructed (mcdonald, 2008). in cyber securitization issue, the government even without making asformal speech act, through surveillance and censorship creates an everyday security practice. with the gezi protests, particularly twitter but also other social media platforms have been transformed into "a medium of government-led populist polarization, misinformation and lynching" (bulut & yörük, 2017:4108). internet bots – which are software applications running automated tasks over the internet – are also extensively deployed by the government to assist paid individuals (yeşil et al., 2017). with the law no: 6639 the infamous tib was empowered to block online content without court order if there is a complaint from an individual about his/her right to privacy is breached and also enhanced the government control over the internet. the prime minister and other relevant ministers are empowered to immediately request the removal of internet content and/or blocking of a website when a court order for such action has been delayed and a risk to public or national security exists (eldem, 2020).

as a spillover effect of the syrian civil war the government-initiated peace process with kurdish terrorist organization pkk became strained. the truce fully collapsed in july 2015, following the ceylanpinar incidents in which two turkish police officers were killed by pkk terrorists and the government considered this as a casus belli to renewed full-scale warfare in south-eastern turkey. furthermore, on july 15, 2016 turkey eluded a coup attempt by feto terror organization. immediately aftermath turkey revised its ncss (2016-2019) and constructed cyber security as a national security concept. additionally, the telecommunication and communication presidency (tib), which implemented the country's website blocking law, was shut down under an emergency decree, and all of its responsibilities were transferred to the btk. erdoğan described the tib as "among the places that has all the dirt". it was closed due to suspicions that it was used by feto as a "headquarters for illegal wiretapping" (freedom house, 2019). the reflection of these as cyber-securitization started with social media censorship. internet disruptions mostly targeted the southeastern region, where ethnic kurds comprise a majority of the population, and which has seen the implementation of a state of emergency and frequent security operations as part of a crackdown by turkish security forces on the militant kurdistan workers' party (pkk). in september 2016, landline, mobile phone, and internet services were shut down in 10 cities in the region for six hours, affecting some 12 million residents; the shutdown came as 28 kurdish mayors were being removed from their posts. a month later, the government suspended mobile and fixed-line internet service in 11 cities for several days including yüksekova, cizre, sur, silopi, leaving six million citizens offline. key public services, such as banks and payment mechanisms, were reportedly unavailable. that shutdown coincided with mass protests prompted by the detention of local kurdish politicians, including the two co-mayors of diyarbakir. turkey's internet backbone is run by ttnet, a subsidiary of türk telekom that is also the largest internet service provider (isp) in the country. türk telekom is partly state owned (freedom house, 2019). additionally, during the 2016–17 purges, the secure instant messaging app bylock was accused by the turkish government of being used primarily by members of the feto. the government launched investigations of over 23,000 citizens for connections to gülen, based solely on evidence that they had downloaded or used bylock. some of these investigations resulted in arrests and detainment.

however, in december 2017, the government announced that it would investigate 11,480 phone numbers had been falsely accused of ties to bylock and gülen, after finding that the accusations were induced by unrelated apps embedding a web beacon pointing to the bylock website from within. an arrest warrant was also issued against the developer of one of these apps (guardian, 2017). wikipedia was inaccessible from april 29, 2017 up until january 15, 2020. governmental requests for the removal of content both on international social media platforms and on popular turkish websites were also widespread. citing security concerns, the turkish government began utilizing new tools such as bandwidth throttling, which is the intentional slowing of an internet service by an isp (eldem, 2020). this happened during times of security or political crises such as the detention of pro-kurdish people's democratic party (halklarin demokratik partisi, hdp) representatives (bianet, 2016), the military coup attempt in 2016, and terror attacks in istanbul, ankara, and suruç between 2015 and 2016 (yesil et al, 2017). in december 2016, the btk ordered turkish isps to block popular vpn services and the tor anonymity network to enable the full implementation of throttling and banning orders (freedom house, 2017). with law no: 6532 national ıntelligence service (mit) gained more authority by accessing online/offline "information, documents, data, or records from public institutions, financial institutions, and entities with or without a legal character." this would mean that mit would not only be able to get citizens' personal data from any public or private institution (banks, schools, hospitals, isps) but also to intercept and store private data on "external intelligence, national defense, terrorism, international crimes, and cyber-security" passing through telecommunication channels" without a court order (eldem, 2020). in 2018, the turkish parliament passed a law giving the national broadcast media regulator, the high council for broadcasting (rtük), authority to monitor and regulate internet services. the law requires online video and streaming services to apply for a license to broadcast to turkish internet users (reporters without borders, 2018). additionally according to the decision published in the official gazette (resmi gazete) on 1 august 2019, online media service providers such as netflix, blutv and puhutv, which broadcast series on the internet, came under the control of rtük. following this decision, digital broadcasting platforms were obliged to obtain a broadcast license to continue broadcasting. with the decision, the rtük administration specified that the violation of the rules of broadcasting could result in sanctions for the broadcasters (freedom house, 2019).

the situation in turkey is in line with what saco describes as "government violations" of personal security where it is a terrain on which multiple discourses and (in)securities compete (saco, 1999). authoritarian regimes and also to some extend non authoritarian ones securitize information flows -both domestic and international- as threats to national security, here national security is actually regime security, and societal identity in a way that expends threat and referent object constellation considerably (deibert, 2002). indeed, in the case of turkey the collapse of peace process with pkk led the government to construct cyber security as a state and societal security issue. the main societal securitization occurred against the kurdish identity in the southeast region of turkey which included cyber securitization through banning social media platforms and cutting kurdish people's communication with the rest of the country and outside world.

## from sub-unit level to unit level: desecuritization of cyber-attacks in the 2018 onwards.

from 2018 onwards the threat perception of the state mostly shifted from domestic threats to foreign threats. indeed since may 2019 there is no report of disruptions to internet took place freedom house, 2019). turkey is the fifth most cyber attacked country in the world following the united states, russia, china and india and turkey is the most cyber attacked country in europe (yeni çağ, 2019). despite the fact that since 2014 there have been cyber attacks against turkey that are originated from other countries such as 2014-dated attack from dragonfly originating from eastern europe targeting industrial systems that manage electrical, water, oil gas and data systems (bbc news, 2014), 2017-dated wannacry ransomware worm targeting it systems (ablak, 2017), and 2014 and 2019-dated iran originated cyber espionages from chafer group which used spear

pfishing, watering hole attacks against the turkish government and security organizations (siber savaş cephesi, 2019; haberler.com, 2014), 2018-dated north korean attack by groups “hidden cobra” and “lazarus” against turkish firms (haberturk, 2018), 2018-dated state sponsored middle eastern hacking group attack targeting telecommunication firms and government embassies (cyberscoop, 2018), 2019-dated cloud atlas attack targeting international financial and aviation sectors, government agencies and religious organizations (anadolu ajansı, 2019), the turkish government desecuritized these issues mostly. between 2017-2018 the cyber attacks mostly targeted the health sector whereas in 2019 the targets shifted towards financial and telecommunication sectors. in october 2019, one of the most important cyber-attack affecting banks and telecommunications institutions in turkey occurred, resulting in a zdnet news of illegally trading card details of the joker's stash is made in turkey from users of the site appeared to be sold over 455 thousand credit cards. ddos attacks against the public and private sectors comprise the majority of cyber-attacks against turkey. the attack targeted garanti bankasi, türk telekom, radore and sadece hosting and took days to overcome. türk telekom technology deputy general manager yusuf kiraç made a statement regarding the 'cyber attack' on sunday, october 27, 2019 and said "we have had to experience one of the cyber attacks that many institutions and even states in the world may be exposed to for some organizations in our country. attack on turkey's information, communications and technology company, was stopped by the timely intervention by the authority in the field of cyber security experts turk telekom” (ulusal kanal, 2019). as seen here, the speech act at first normalized the attack by saying how it happens in almost every country and focused on how well türk telekom acted on the crisis.

the ransomware threat, which has become widespread in the last few years continued in 2019. despite these the turkish government and the academic personnel close to the government worked to desecuritize the attacks. most of the rhetoric revolve around the dangers of cyber attacks and how elaborate the attacks become with further continuing how turkey is very successful in overcoming these threats and attacks. for example dtu president prof. ahmet acar argued that december 14- dated ddos attack is well taken care of by turkish government. meanwhile, ömer fatih sayan, deputy minister of transport and infrastructure, said in a speech given at the beginning of the "international cyber shield 2019 exercise" held at the information technologies and communication authority (btk), that “cyber attacks are increasing all over the world. we have set out to protect them from these attacks and the damage they have caused. we continue our activities to ensure national cyber security in line with the realities of the industry and life within the national cyber incidents response center (usom)” (vatan, 2019). as seen in the rhetoric of academia and government officials, the government

never holds the sole responsibility of cyber security, contrarily the governments almost always encumber private sector with shared responsibility of cyber security within the national security framework. if one reason for that is ownership of computer networks, another reason perhaps more importantly that the private sector holds the know-how (hansen & nissenbaum, 2009:1162). when looked at the annual reports of cyber-attacks to usom, it appears that from 2018 to 2019 the number is doubled. in 2018 the number was 72 thousand 975 whereas in 2019 this number is 136 thousand 411. zurich insurance group turkey ceo yilmaz yildiz argued that it is getting worse with each passing year of cyber-attacks and turkey is among the countries that suffered the most. turkey came in third in the world and ranked second among the biggest risks in the world of cyber attacks, and in europe it came in first. emphasizing that cyber attacks were initially made to commercial, corporate large companies and public companies, and later, with the increase of digital devices, it went down to smes and individuals (hurriyet, 2019). during the operation peace spring and operation olive branch cyber attacks against turkey increased. defense industry president ismail demir said, "in the peace spring operation, the attempts of the hacker groups belonging to the terrorist organization were organized on social media and cyber attacks and data leaks against public institutions were identified." said. we have seen cyber attacks on institutions and telecom operators, which show that cyber security has become a powerful tool in all political and military conflicts for a variety of purposes, from political propaganda to espionage activities, denial of services, and destruction of critical infrastructure. necessary measures are

being taken with the cyber security ecosystem supported by the ssb through actors such as transformation office, information technologies and communication authority, national cyber incidents response center, and cyber security projects." (trt haber, 2019). in the cyber threat status report of defense technologies engineering and trade inc. (stm), increasing cyber attacks parallel the operation olive branch attracted attention. according to the report, terrorist organizations and sympathizers resorted to black propaganda, the most known method of psychological warfare, especially against the international public opinion, against the operation olive branch, which was carried out by the turkish armed forces (tsk) across the border. with the onset of the operation, the aggressive groups carried out systematic cyberattacks especially in the provincial organizations of public institutions and organizations under the heading "#opturkey". it was stated that the terrorist organizations that suffered a significant loss of power and ground during the operation with these attacks, which decreased with the completion of the operation, aimed to sabotage the superiority of the taf, change the perception and drag the masses into the drive (trt haber, 2019).

## final remarks and conclusion

as a result, integrating cyber security sector to securitization theory and particularly to critical security studies is necessary in order to have a better grasp of societal and human security aspects. on the other hand, from a unit level perspective the ongoing organization of the international system as a sovereign nation-states community means that state security concerns remain a priority; on the other hand, the security problems and their solutions are not only defined in a military sense. this necessitates addressing the sources and solutions of security issues that go beyond state- centered structures and assumptions. in this article widening and deepening processes in the field of security studies have been discussed within the framework of cyber security sector. as seen in the case, cyber sector in the globalized world become much more important security sector in the international relations. it not only differentiates in threats, securitizing actors and audience from other sectors, but also connected to each of them and also each of the levels of analysis almost exclusively similar to environmental sector.

the conceptualization of desecuritization in the copenhagen school is undertheorized, explained very briefly as “moving a process in which a political community downgrades or ceases to treat something as an existential threat to a valued referent object, and reduces or stops calling for exceptional measures to deal with the threat” (buzan & wæver, 2003). the case study of turkey shows that in the cyber desecuritization, the technification concept is more clearly seen since the desecuritization is done not just through the political leaders but through professionals of the field or through academic personnel. this also works in two ways: first, since it is not done by politicians the credibility of the desecuritization move is much more reliable in the eyes of the audience, and therefore the desecuritization act is more successful. secondly, as mentioned in the first part, securitization and desecuritization does not necessarily follow a formal speech act, there are situations where without a speech taking place these constructions can exist. here the silence of politicians also constructs a desecuritization act implying the issue is not worthy of their time and explanation. to put it in other words, the silence of politicians and the technificiation process acts as a dual desecuritization act.

## References

Özgenç, M. (2013, June 12). *RTUK’ten Halk TV ve Ulusal Kanal’a Ceza*. May 2019 tarihinde Hürriyet Gündem: http://www.hurriyet.com.tr/gundem/23486445.asp adresinden alındı

Ablak, E. (2017, May 18). *Hurriyet Daily News*. May 2019 You wannacry, don’t you?: https://www.hurriyetdailynews.com/opinion/ersu-ablak/you-wannacry-dont-you--113230

Akdağ, Y. (2019). The likelihood of cyberwar between the United States and China: A neorealism and power transition theory perspective. *Journal of Chinese Political Science, 24*(2), 225-247.

*Anadolu Ajansı*. (2019, August 15). January 2020 Cloud Atlas"tan Türkiye'deki kurumlara siber saldırı: https://www.aa.com.tr/tr/sirkethaberleri/bilisim/cloud-atlastan-turkiyedeki-kurumlara-siber-saldiri/652688

Aydindag, D. (2019). The Evolution and Intersection of Academic and Popular Islamic Feminism in Turkey. *Religación. Revista de Ciencias Sociales y Humanidades, 4*(19), 1026-1034.

Aydindag, D., & Isiksal, H. (2018). (De) Securitization of Islam in Turkey. *Revista de Cercetare si Interventie Sociala, 62*, 294-306.

Bıçakcı, S. (2014). *NATO's Emerging Threat Perception: Cyber Security in the 21st Century.* Kadir Has University.

Bıçakcı, S., Ergun, D., & Çelikpala, E. (2015). Türkiye'de Siber Güvenlik. *Ekonomi ve Dış Politika Araştırma Merkezi (EDAM) Siber Politika Kağıtları Serisi, 1*, 1-35.

Balzacq, T. (2005). The Three Faces of Securitization: Political Agency, Audience and Context. *European Journal of International Relations, 11*(2), 171-201.

Balzacq, T. (2009). Constructivism and securitization studies. M. Dunn Cavelty, & V. Mauer içinde, *Routledge Handbook of Security Studies* (s. 60). London: Routledge.

Baykan, A., & Hatuka, T. (2010). Politics and Culture in the Making of Public Space. Taksim Square, 1 May 1977, Istanbul. *Planning Perspectives, 25*(1), 49-68.

*BBC News*. (2014, July 1). May 2019. Energy firms hacked by 'cyber-espionage group Dragonfly': https://www.bbc.com/news/technology-28106478

Behnke, A. (2006). No Way Out: Desecuritization, Emancipation and the Eternal Return of the Political – A reply to Aradau. *Journal of International Relations and Development,, 9*(1), 65.

*Bianet*. (2016, October 26). Internet outage in eastern and southeastern Turkey,: https://bianet.org/english/media/ 180001-internet-outage-in-eastern-and-southeasternturkey

Buchanan, B. (2016). *The cybersecurity dilemma: Hacking, trust, and fear between nations.* Oxford: Oxford University Press.

Bulut, E., & Yörük, E. (2017). Mediatized populisms, Digital populism: Trolls and political polarization of Twitter in Turkey. *International Journal of Communication, 11*, 4093-4117.

Buzan, B. (2004). *The United States and the Great Powers: World Politics in the Twenty-First Century.* Cambridge: Polity.

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

Buzan, B., Waever, O., & de Wilde, J. (1998). *Security: A New Framework For Analysis.* London: Lynne Rienner Publishers.

Cavelty Dunn, M., Kristensen, M., & Soby, K. (2008). *Securing 'the Homeland'." Critical Infrastructure, Risk, and (In) Security.* London: Routledge.

Choucri, N. (2012). *Cyberpolitics in international relations.* MIT Press.

Collier, J. (2018). Cyber security assemblages: A framework for understanding the dynamic and contested nature of security provision. *Politics and Governance, 6*(2), 13-21.

*Cyberscoop*. (2018, December 10). January 2020. Middle East group goes on hacking spree against telecoms, embassies and more: https://www.cyberscoop.com/middle-east-group-goes-hacking-spree-telecoms-embassies/

Deibert, R. (2002). Circuits of Power: Security in the Internet Environment. J. Rosenau, & J. Singh (Ed.) in, *Information Technologies and Global Politics: The Changing Scope of Power and Governance.* Albany: State University of New York.

Deibert, R. (2003). Black code: Censorship, surveillance, and the militarisation of cyberspace. *Millenium, 32*(3), 501-530.

Deibert, R., & Rohozinski, R. (2010). Risking Security: Policies and Paradoxes of Cyberspace Security. *International Political Sociology, 4*(1), 15-32.

Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war. *Security Dialogue, 43*(1), 3-24.

Der Derian, J. (2003). The question of information technology in international relations.". *Millenium, 32*(3), 441-456.

Dunn Cavelty, M. (2012). Cyber-Security. A. Collins (Ed.) in, *Contemporary Security Studies* (s. 155). New York: Oxford University Press.

Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review, 15*(1), 105-122.

Dunn Cavelty, M., & Wenger, A. (2020). Dunn Cavelty, Myriam, and Andreas Wenger. "Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, *41*(1), 5-32.

Eldem, T. (2020). The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration, 43*(5), 452-465.

*Erdoğan approves law tightening Turkey's Internet controls*. (2014, September 12). January 2019 Reuters: https://www.reuters.com/article/us-turkey-internet/erdoğan- approves-law-tightening-turkeys-internet-controls- idUSKBN0H70N9

Eriksson, J., & Giacomello, G. (Ed.). (2007). *International relations and security in the digital age.* (Volume 52). Routledge.

*Evrensel.net* . (2007). May 2019. Cumhuriyet Mitingleri: https://www.evrensel.net/haber/245040/cumhuriyet-mitingleri /

*Excerpts of Turkish army statements*. (2007, April 28). May 2019. BBC News: http://news.bbc.co.uk/2/hi/europe/6602775.stm

Financial Tribune. (2017, June 9). Turkey's Massive Dam Building Creating Problems. *Financial Tribune*.

Fouad, N. S. (2019). The peculiarities of securitising cyberspace: a multi-actor analysis of the construction of cyber threats in the US (2003-2016). *Proceedings of the 18th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing International Limited.*

Geelen, M. (2016). *Cyber Securitization and Security Policy." The impact of the Discursive Construction of Computer Security on (National) Security Policymaking in the Netherlands.* openaccess.leidenuniv.nl.

Geers, K. (2014). *Pandemonium: Nation States, National Security, and the Internet.* NATO CCDCOE.

Georgieva, ı. (2020). The unexpected norm-setters: Intelligence agencies in cyberspace. *Contemporary Security Policy, 41*(1), 33-54.

Gill, A. S. (2019). Artificial intelligence and international security: the long view. *Ethics & International Affairs, 33*(2), 169-179.

*Guardian*. (2017, September 11). May 2019. Turks detained for using encrypted app 'had human rights breached': https://www.theguardian.com/world/2017/sep/11/turks-detained-encrypted-bylock-messaging-app-human-rights-breached

*Haberler.com*. (2014, December 4). January 2019. İran'dan Türkiye'ye Siber Saldırı: https://www.haberler.com/iran-dan-turkiye-ye-siber-saldiri-6746927-haberi/

*Haberturk*. (2018, March 9). January 2020. Kuzey Kore, Türk finans kuruluşlarına siber saldırı düzenledi: https://www.haberturk.com/kuzey-kore-turk-finans-kuruluslarina-siber-saldiri-duzenledi-1869381-ekonomi

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

*Hurriyet*. (2019, December 6). January 2020. Siber Tehlike: https://www.hurriyet.com.tr/ekonomi/siber-tehlike-41390759

Kremer, J.-F., & Müller, B. (Ed). (2013). *Cyberspace and international relations: Theory, prospects and challenges.* Springer.

Lacy, M., & Prince, D. (2018). Securitization and the global politics of cybersecurity. *Global Discourse, 8*(1), 100-115.

Law on amending certain clauses of the 765-dated Turkish Penal Code, 3756 (June 6, 1991).

Lee, J., & Macdonald, S. (2016). Analogy and authority in cyberterrorism discourse: an analysis of global news media coverage. *Global Society, 30*(4), 605-623.

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross, 94*(886), 515-531.

Lobato, L. C., & Kenkel, K. M. (2015). Discourses of cyberspace securitization in Brazil and in the United States. *Revista Brasileira de Política Internacional, 58*(2), 23-43.

Mačák, K. (2017). From cyber norms to cyber rules: re-engaging states as law-makers. *Leiden Journal of International Law, 30*(4), 877-899.

McDonald, M. (2008). Securitization and the Construction of Security. *European Journal of International Relations, 14*(4), 563-587.

Mis, N., & Aslan, A. (2018). *AK Parti'nin 15 Yılı: Siyaset.* Ankara: SETA Kitapları.

*NATO*. (2020, March 17). March 2020 Cyber Defence: https://www.nato.int/cps/en/natohq/topics_78170.htm

Nissenbaum, H. (2004). Hackers and the contested ontology of cyberspace. *New Media & Society, 6*(2), 195-217.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*(2), 61-73.

*NTVMSNBC*. (2008, November 21). May 2019 Erdoğan: Ben YouTube'a giriyorum, siz de girin.

Nye, J. (2011). Nuclear Lessons for Cyber Security. *Strategic Studies Quarterly, 5*(4), 18-38.

Oelsner, A. (2005). (De)Securitisation Theory and Regional Peace: Some Theoretical Reflections and a Case Study on the Way to Stable Peace: https://www.researchgate.net/publication/5015291_DeSecuritisation_Theory_and_Regional_Peace_Some_Theoretical_Reflections_and_a_Case_Study_on_the_Way_to_Stable_Peace

Oktem, K. (2013, June 9). *Why Turkey's mainstream media chose to show penguins rather than protests*. January 2019. The Guardian:

https://www.theguardian.com/commentisfree/2013/jun/09/turkey- mainstream-media-penguins-protests

Polański, P. P. (2017). Cyberspace: A new branch of international customary law?. *Computer Law & Security Review, 33*(3), 371-381.

Porcedda, M. G. (2018). Patching the patchwork: appraising the EU regulatory framework on cyber security breaches. *Computer Law & Security Review, 34*(5), 1077-1098.

Rainsford, S. (2007, April 13). May 2019. BBC News: http://news.bbc.co.uk/2/hi/europe/6554099.stm,

*Recep Tayyip Erdoğan dismisses Turkey protesters as vandals*. (2013, June 9). May 2019 The Guardian: https://www.theguardian.com/world/2013/jun/09/recep-tayyip- erdoğan-turkey-protesters-looters-vandals

Rehrl, J. (Ed.). (2017). *Handbook on CSDP: The common security and defence policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence and Sports of the Republic of Austria,.

*Reporters Without Borders*. (2018, March 27). January 2020 New law reinforces Turkish government's control of the Internet: https://rsf.org/en/news/new-law-reinforces-turkish-governments-control-internet

Rosenau, J., & Singh, J. (Ed.). (2002). *Information technologies and global politics: The changing scope of power and governance.* SUNY Press.

Saco, D. (1999). Colonizing Cyberspace: "Nationnal Security" and the Internet. J. Weldes, M. Laffey, H. Gusterson, & R. Duvall (Ed.) in, *Cultures of Insecurity: States, Communities, and the Production of Danger.* Minneapolis: University of Minnesota Press.

Sardarnia, K., & Safizadedh, R. (2019). The internet and its potentials for networking and identity seeking: A study on ISIS. *Terrorism ad Political Violence, 31*(6), 1266-1283.

Sari, A. (2019). Turkish national cyber-firewall to mitigate countrywide cyber-attacks. *Computers & Electrical Engineering, 73*, 128-144.

Sharp, T. (2017). Theorizing cyber coercion: The 2014 north korean operation against sony. *Journal of Strategic Studies, 40*(7), 898-926.

*Siber Savaş Cephesi*. (2019, March 6). january 2019 İran'dan Türkiye'ye Siber Saldırı: https://sibersavascephesi.com/irandan-turkiyeye-siber-saldiri/

Stevens, T. (2018). Global cybersecurity: new directions in theory and methods. *Politics and Governance, 6*(2), 1-4.

Taşçı, U., & Can, A. (2015). Türkiye'de Polisin Siber Suçlarla Mücadele Politikası 1997-2014. *Firat University Journal of Social Sciences/, 25*(2), 229-248.

Taureck, R. (2006). Securitization theory and securitization studies. *Journal of International Relations and Development, 9*(1), 53-61.

Tikk, E. (2011). Ten rules for cyber security. *Survival, 53*(3), 119-132.

*TRT Haber*. (2019, October 31). January 2020. Savunma Sanayi Başkanı Demir: Barış Pınarı Harekatı sırasında siber saldırılar tespit ettik: https://www.trthaber.com/haber/gundem/savunma-sanayi-baskani-demir-baris-pinari-harekati-sirasinda-siber-saldirilar-tespit-ettik-438519.html

*Turkey*. (2017, May 31). May 2019. Freedom House: https://freedomhouse.org/country/turkey/freedom-net/2017

*Turkey*. (2019, May 31). January 2020. Freedom House: https://freedomhouse.org/country/turkey/freedom-net/2019#footnote4_7mf9xbs

*Ulusal Kanal*. (2019, October 28). January 2020 Garanti Bankası, Radore ve Sadece Hosting'ten siber saldırı açıklaması!: https://www.ulusal.com.tr/gundem/son-dakika-siber-saldirilar-haberleri-garanti-bankasi-radore-ve-sadece-hosting-ten-siber-saldiri-aciklamasi-garanti-bankasi-mobil-ve-internet-bankaciligi-coktu-mu-garanti-bankasi-na-h241801.html

Valeriano, B., & Manessa, R. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system.* USA: Oxford University Press.

*Vatan*. (2019, December 19). January 2020. Dikkat çeken siber saldırı uyarısı.

Vultee, F. (. (2011). Securitization as a Media Frame: What Happens When the Media 'Speak Security. T. Balzacq içinde, *Securitization Theory: How Security Problems Emerge and Dissolve* (s. 91-107). London: Routledge.

Waever, O. (1993). *Identity, Migration, and the New Security Agenda in Europe.* Copenhagen: St. Martin's Press.

Weber, V. (2018). Linking cyber strategy with grand strategy: the case of the United States. *Journal of Cyber Policy, 3*(2), 236-257.

Wilkinson, C. (2011). The Limits of Spoken Words: From Meta-Narratives to Experiences of Security. T. Balzacq in, *Securitization Theory: How Security Problems Emerge and Dissolve* (s. 95). London: Routledge.

Wilner, A. (2020). US cyber deterrence: Practice guiding theory. *Journal of Strategic Studies, 43*(2), 245-280.

*Yeni Çağ*. (2019, November 8). January 2020 Siber savaşlar ve hedefindeki Türkiye Kaynak Yeniçağ: Siber savaşlar ve hedefindeki Türkiye: https://www.yenicaggazetesi.com.tr/siber-savaslar-ve-hedefindeki-turkiye-255525h.htm

Yesil, B., Sözeri, K., & Khazraee, E. (2017). *Turkey's Internet policy after the coup attempt: The emergence of a distributed network of online suppression and surveillance.* An Internet Policy Observatory Publication.