İÇ İŞLERİNE KARIŞMAMA İLKESİ BAĞLAMINDA ENFORMASYON TEKELİ VE DEZENFORMASYON: ŞANGAY İŞBİRLİĞİ ÖRGÜTÜ UYGULAMALARI AÇISINDAN BİR DEĞERLENDİRME

Information Monopoly and Disinformation in the Context of Non-Interference in Internal Affairs: An Evolution in Terms of the Practices of the Shangai Cooperation Orgonisation

Tabriz JAFAROV*

ÖZ

Makale internetin hızlı biçimde gelişmesi sonucunda daha da güncellik kazanan dezenformasyon kavramını iç işlerine karışmama ilkesi ve Şangay İşbirliği Örgütü (ŞİÖ) uygulamaları kapsamında ele almaktadır. Dezenformasyonun yanı sıra enformasyon tekeli üzerinden kurulan hegemonyanın oluşturduğu eşitsiz siberalan ve mevzubahis eşitsizlik sebebiyle devletlerin egemen eşitliğine yönelen pratik tehditler de makalenin inceleme alanı içerisindedir. Araştırma çerçevesinde bir taraftan da ŞİÖ uygulamaları kapsamında ele alınan sözü geçen kavramların saldırı olarak değerlendirilmesine dair koşullar açısından tespitlere yer verilmiştir. Nihayetinde her dezenformasyonun bir iç işlerine karışma şeklinde değerlendirilemeyeceği fakat koşullara dayalı olarak bahsi geçen ilkenin ihlalinin oluşabileceği sonucuna varılmıştır. Öte yandan ortak yönetilmesi gerektiği kanısına varılmış siberalanın enformasyon tekeline tekabül edecek biçimde kullanılmasının ise egemen eşitlik ilkesi ile bağdaşmadığı görüşü hasıl olmuştur.

Anahtar Kelimeler: Dezenformasyon, İç İşlerine Karışmama, Uluslararası Hukuk, Şangay İşbirliği Örgütü, Enformasyon Tekeli

---

Makalenin Geliş Tarihi: 31.07.2022, **Makalenin Kabul Tarihi:** 23.11.2022.

* Dr. Ankara Üniversitesi Sosyal Bilimler Enstitüsü Kamu Hukuku Bölümü, Milletlerarası Hukuk Anabilim Dalı, e-posta: tebriz.rauf@gmail.com, ORCID: 0000-0002-7087-6919.

ABSTRACT

The article deals with the concept of disinformation, which has become more current as a result of the rapid development of the internet, within the scope of the principle of non-interference in internal affairs and Shanghai Cooperation Organization (SCO) practices. In addition to disinformation, the unequal cyber space created by the hegemony established through the information monopoly and the practical threats to the principle of sovereign equality of states due to the inequality in question are also within the scope of the article. Within the framework of the research determinations are included in terms of the conditions regarding the evaluation of the aforementioned concepts as an attack within the scope of SCO practices. In the end, it was concluded that every information can not be considered as an interference in internal affairs, but a violation of the aforementioned principle may occur depending on the circumstances. On the other hand, it has been concluded that the use of cyberspace in a way that corresponds to the information monopoly is incompatible with the sovereign equality principle.

Keywords: Disinformation, Non-interference in Internal Affairs, International Law, Shanghai Cooperation Organization, Information Monopoly.

I. GİRİŞ

İç işlerine karışmama ilkesi Birleşmiş Milletler Antlaşması tarafından hükme bağlanan ve uluslararası hukukun egemen eşitlik prensibinden yola çıkarak oluşturduğu devletlerin beraberliği tezinin olmazsa olmazlarındandır. Bu prensipten yola çıkılarak devletlerin siyasi bağımsızlıklarını da kapsayacak bir şekilde iç işlerine müdahale mevcut uluslararası hukuk tarafından yasaklanmaktadır. Prensibin içeriği çok geniş olduğu için olayların duruma göre değerlendirilmesi ve müdahalenin gerçekleşip gerçekleşmediğine karar verilmesi elzemdir. Son dönemler internetin getirdiği realite hasebi ile enformasyon kavramı daha da yaygınlaşmış, dünya ahalisinin son istatistiklere göre yüzde 60'ından fazlasının çevrimiçi olması ile birlikte daha da güncelleşen enformasyon kavramı iç işlerine müdahale edilmemesi prensibi bağlamında da önem arz etmeye başlamıştır. Zira Birleşmiş Milletler (BM) üyesi olan ülkelerin bazıları enformasyon savaşı, enformasyon terörü, enformasyon saldırıları gibi yeni tanım ve terimleri kullanmaktadır. İlgili devletler kendi iç hukuklarının yanı sıra uluslararası

platformlarda konuya nazaran teamül oluşturabilecek nitelikteki davranışlarını mevzubahis temeller üzerine inşa etmektedirler.

Bahsettiğimiz tanımlar üzerinden güvenlik doktrini oluşturmaya çalışan devletler çoğunlukla Şangay İşbirliği Örgütü (ŞİÖ) şemsiyesinde birleşmiş bulunmaktadırlar. Nitekim çalışmamızda iç işlerine karışmama temelinde ŞİÖ tarafından inşa edilen güvenlik kapsamlı enformasyon kavramları incelenecek ve bahsi geçen tanımlara dayalı olarak gerçekleştirilen ne tür siber eylemlerin uluslararası hukuk çerçevesinde iç işlerine karışmama yasağının ihlali olduğuna dair tespitler yapılacaktır.

II. ŞANGAY İŞBIRLIĞI ÖRGÜTÜ

Şangay İşbirliği Örgütü (ŞİÖ) Rusya ve Çin'in başını çektiği doğu grubu ülkelerinin oluşturduğu bir uluslararası örgüttür[1]. 15 Haziran 2001'de Şanghay'da (Çin) kurulduğu ilan edilen örgüt dünya nüfusunun 40% ve gayri safi yurt içi hasılasının (GSYİH) 20% teşkil etmesi sebebiyle evrensel siyasette son derece etkin konuma sahiptir.[2] Rusya ve Çin'in de içinde yer alması hasebi ile batılı ülkelerden farklı olarak demokrasi noktasında daha muhafazakar ve geleneğe dayalı bir siyaset izleyen örgüt internet konusunda da benzer tavır sergilemektedeir. Özellikle yıllar uzunu Rusya'nın siyasi ve askeri işbirliği içerisinde olduğu Orta Asya devletleri ile beraber Çin'in etkili olduğu örgüt bir yandan da Hindistan ve Pakistan gibi devletleri içine almakla jeopolitik alanını daha da genişletmiştir[3]. Asil üyelerin yanı sıra Afganistan, İran, Beyaz Rusya ve Moğolistan ise gözlemci statüsü ile ŞİÖ bünyesinde yer almaktadır[4]. ŞİÖ bir grup devletlerle de "Diyalog Ortağı" düzeyinde işbirliği

---

1 http://eng.sectsco.org/about_sco/ (e.t. 31. 03. 2022); Şanghay İşbirliği Örgütü (SCO), Kazakistan Cumhuriyeti, Çin Halk Cumhuriyeti, Kırgız Cumhuriyeti, Tacikistan Cumhuriyeti, Özbekistan Cumhuriyeti ve Rusya Federasyonu tarafından 15 Haziran 2001'de Şanghay'da (Çin) kurulduğu ilan edilen kalıcı bir hükümetler arası uluslararası örgüttür.[2] Bruna Toso de Alcântara, "SCO and Cybersecurity: Eastern Security Vision for Cyberspace", International Relations and Diplomacy, Cilt: 6, Sayı. 10 (2018): 549

2 Bruna Toso de Alcântara, "SCO and Cybersecurity: Eastern Security Vision for Cyberspace", International Relations and Diplomacy, Cilt: 6, Sayı. 10 (2018): 549

3 İbid.

4 Gözlemci devletler için bkz. https://dppa.un.org/en/shanghai-cooperation organization#:~:text=The%20SCO%20currently%20comprises%20eight,Cambodia%2C%20Nepal%2C%20Sri%20Lanka%20and (e.t. 26.08.2022); İran İslam

yapmaktadır. Nitekim Ermenistan, Azerbaycan, Kamboçya, Nepal, Sri Lanka ve Türkiye'nin dahil olduğu "Diyalog Ortağı" statülü işbirliği platformuna 2021 Duşanbe Zirvesi'nde Suudi Arabistan, Mısır ve Katar da eklenmiştir.[5]

Örgüt bilişim ve teknoloji alanına münasebette gerekli hukuki işlemleri yaparak politikalarını resmiyete dökmüştür. Keza 2009 tarihli Yekaterinburg Sözleşmesi ve 2011'de BM Genel Kurulu'na sunulan "Code of Conduct for Information Security" isimli taslağı ŞİÖ'nün siber alana yönelik temel hukuki kaynakları olarak değerlendirilebilir.[6]

III. İÇ İŞLERİNE KARIŞMAMA İLKESİ

İç işlerine karışmama ilkesi BM Antlaşması'nda kendi içeriğini bulan[7] bir uluslararası hukuk prensibi olmakla özü itibariyle devlet egemenliği kavramından doğmaktadır.[8] Bilindiği üzere BM Antlaşması bütün üye devletlere egemen eşitlik hakkını tanımaktadır ve kendi siyasi bağımsızlığı ve diğer hususlarda özgür karar alabilme yetkisi ile donatmaktadır. Hakeza bu

---

Cumhuriyeti'nin üyeliği onaylanarak örgüte katılması için resmi prosedürler başlatılsa henüz nihai işlemler tamamlanmamıştır.
Bu konuda bkz. https://www.mfa.gov.tr/shanghai-cooperation-organization.en.mfa (e.t. 16.08.2022)

5 İbid.

6 Yekaterinburg Sözleşmesi için bkz. http://eng.sectsco.org/documents/ (e.t. 19.08.2022); "Code of Conduct for Information Security" taslak metni ve metnin sunulduğu Genel Kurul oturumu için bkz. UN doc. A/66/359, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N11/496/56/PDF/N1149656.pdf?OpenElement (e.t. 19.08.2022)

7 BM Antlaşması 2.1'e göre "Örgüt, tüm üyelerinin egemen eşitliği ilkesi üzerine kurulmuştur."; BM Antlaşması 2.4'e göre "Tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığa karşı, gerek Birleşmiş Milletleríin Amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar."; BM Antlaşması 2.7'e göre ise "İşbu Antlaşmaínın hiçbir hükmü, Birleşmiş Milletlere herhangi bir devletin kendi iç yetki alanına giren konulara müdahale yetkisi vermediği gibi üyeleri de bu türden konuları işbu Antlaşma uyarınca bir çözüme bağlamaya zorlayamaz.", BM Antlaşmasının Resmi Gazete'de yayınlanmış metni için bkz. RG, 24 Ağustos 1945, Sayı: 6092, https://www.resmigazete.gov.tr/arsiv/6092.pdf (e.t. 19. 07. 2022).

8 Fatih Tosun, "Uluslararası Hukuk'ta "Kuvvet Kullanma Ve Karışma" Kavramlarının Değişen Anlamı", Güvenlik Stratejileri Dergisi, Cilt: 5, Sayı. 9 (2009): 108-109.

ilkeden yola çıkılarak iç işlerine karışılmaması gerektiği normunu uluslararası hukukun en önemli kaynaklarından olan BM Antlaşması'na dayatmak mümkündür. İlke gereğince devletler birbirlerinin iç işlerine karışmamalı ve egemen eşitliğine saygı göstermelidir.

Fakat uluslararası hukuk doktrininde iç işlerine karışılmaması konusu dar ve geniş çerçevede yorumlanabilmektedir[9]. Bazı devletler dar çerçeveden bakarak yalnız etkin ve somut müdahalelere iç işlerine karışılması penceresinden bakmakta ise bir grup başka devletler ise her türlü faaliyeti kendi ülkelerine yönelik birer iç işleri müdahalesi olarak görmektedir. Başka bir cümle ile ikinci grup devletler hattâ bazı eleştirisel nitelikteki açıklama ve yorumları dahi iç işlerine müdahale olarak değerlendirebilmektedir. Nitekim enformasyon konusunu da bu çerçevede ele alarak bilgi ve iletişim teknolojilerinin meydana getirdiği yeni durumda ayrı ayrı teknoloji şirketleri vasıtası ile yapılan eylemlerin iç işlerine karışılmaması prensibine dayanılarak nasıl ele alınmasının açıklığa kavuşturulması önem arz etmektedir. Örneğin ŞİÖ 2011 tarihli taslak maddelerinde ve 2009'da kabul ettiği Yekaterinburg Sözleşmesi'nde enformasyon saldırıları ve enformasyon silahları gibi kavramlara değinmektedir[10]. Aynı zamanda örgüt devletlerin siyasi bağımsızlığını hedef alan enformasyon müdahalelerini de bu çerçevede algılamaktadır. Zira örgüte üye olan Rusya kendisinin kültürel altyapısını ve ideolojik varlığını hedef alan, aynı zamanda bu çerçevede yürütülen her türlü bilgi paylaşımı ve propaganda faaliyetlerini iç işlerine karışma olarak kabul etmektedir.[11]

---

[9] Abu Saleh Md Mahmudul Hasan, "Uluslararası Hukukta Devletlerin İçişlerine Karışmama İlkesinin İncelenmesi: Bangladeş Örneği", Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, Doktora Tezi (Yayınlanmamış) (2021): 84-85.

[10] "Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization", Madde 2. Sözleşme metni için bkz. http://eng.sectsco.org/load/207508/ (e.t. 31. 07. 2022)

[11] Russian Federation, Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space, Information Security Doctrine of the Russian Federation approved by the President of the Russian Federation on 9 September 2000, NATO Cooperative Cyber Defence Center of Excellence, 2000, http://www.ccdcoe.org/strategies /Russian_Federation_unofficial_translation.pdf (e.t. 01. 09. 2022)

IV. SALDIRI VE SALDIRI OLARAK DEZENFORMASYON

BM Genel Kurulu'nun 1974 tarihli Saldırının Tanımı kararına göre, *"Saldırı, bir Devletin diğer bir Devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya işbu Tanımda belirtildiği üzere, Birleşmiş Milletler Andlaşması ile bağdaşmayan diğer herhangi bir tarzda silahlı kuvvet kullanılmasıdır"*.[12] İlgili kararın 3. Maddesinde ise saldırı olarak değerlendirilecek fiillere yönelik bir sıralama yapılmıştır. Yapılan sıralama silahlı kuvvet kullanımıyla gerçekleştirilecek eylemleri kapsamı dahiline almaktadır. Fakat mevzubahis kararın 4. Maddesi ile karar çerçevesinde belirlenen fiilerin tüketici nitelikte olmadığının altı çizilmiştir.[13] Dolayısıyla ilgili düzenlemede yalnız silahlı kuvvet kullanımıyla yapılan eylemlerin değil, klasik anlamda silahlı kuvvetle desteklenmeyen eylemelerin de bir saldırı olabileceğine olanak tanımıştır.

Her enformasyon saldırısı aslında birer saldırı olarak da nitelendirilebilir. Fakat her saldırı bir enformasyon saldırısı değildir. Saldırı kavramı daha çok BM Antlaşması'nın 51. Maddesi çerçevesinde belirlenmiş olan meşru müdafaa hakkının doğması için gerçekleşmesi gereken silahlı saldırı fiili ile birlikte ele alınmaktadır.[14] Zira BM Antlaşması'nın 2.4 Maddesi ile yasaklanan kuvvet kullanımı var olan silahlı saldırı eylemini önlemek için başvurulan meşru müdafaa hakkı ile istisnailik arzetmektedir.[15]

Bilgi ve İletişim teknolojilerinin gelişimi ile ortaya çıkan yenilikler ennformasyon kavramının daha da güncelleşmesine ve öneminin artmasına sebebiyet vermiştir. Özellikle internetle birlikte bu alanda yaşanan devrim niteliğindeki kalkınma ve büyüme yalnız fertler arasındaki ilişkileri etkilemekle kalmaksızın devletlerarası ilişkilere de etkisini göstermiştir.[16]

---

[12] Undoc A/RES/3314(XXIX), https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/NR0/739/16/IMG/NR073916.pdf?OpenElement (e.t. 31. 08. 2022)

[13] Muharrem Uğur BOZKURT, "Siber Saldırıların BM Şartı'nda Yer Alan Silahlı Saldırı Kavramı Kapsamında Değerlendirilmesi", Çanakkale Araştırmaları Türk Yıllığı, Sayı. 32 (2022): 29.

[14] Malcolm N. Shaw, International Law, Eighth Edition, (Cambridge University Press 2017), 861-862.

[15] Esat Mahmut Yılmaz, "Uluslararası Hukukta Saldırı Suçu", Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü (2011): 61.

[16] Henry H. Perritt Jr, "The Internet Is Changing the Public International Legal System", 88 Ky. L.J. 885 (2000): 886.

Nitekim enformasyon savaşı ve enformasyon silahları kavramlarının kullanılmasıyla ise enformasyon saldırı türlerinden olarak tartışılmaya başlamıştır.

Enformasyon saldırısı ABD Hava Kuvvetleri tarafından *"içinde bulunduğu fiziksel varlığı gözle görülür bir şekilde değiştirmeden düşman bilgilerini doğrudan bozmak"* veya *"bir rakibin bilgilerini, içinde bulunduğu fiziksel varlığı gözle görülür bir şekilde değiştirmeden manipüle etmek veya yok etmek için gerçekleştirilen faaliyetler"* olarak tanımlanmaktadır. [17] Dolayısı ile enformasyon saldırıları fiziksel bir içerik barındırmış olmasa dahi hedef aldığı kitleyi, toplumu veya devleti saldırıyı gerçekleştiren aktörlerin çıkarları doğrultusunda değiştirmeyi, etkilemeyi amaçlamakta ve bazı durumlarda gerçekleştirilen saldırının düzeyine de bağlı olmakla silahlı saıldırı seviyesinde zararlara yol açabilmektedir.

V. ŞİÖ'NÜN SİBER ALANIN YÖNETİMİ BAĞLAMINDA YAKLAŞIMI VE BATI GRUBU ÜLKELERİ İLE FARKLILIKLARI

ŞİÖ internete yaklaşım konusunda Avrupa Birliği (AB) ve Avrupa Konseyi (AK) üye ülkeleri ve Amerika Birleşik Devletleri'nden (ABD) farklı bir yaklaşım ortaya koymakta ve bu yaklaşım kendisini daha çok Rusya ve Çin'in siber politikaları ile göstermektedir.[18]

Detayları ile incelendiğinde AB ülkeleri, daha genel bir ifade ile batı görüşünü savunan ülkelerden farklı olarak ŞİÖ siber ilişkilere yönelik daha katı ülkesel egemenlik tezini savunmakta olup kontrol mekanizması üzerinde kurulan bir internet tezini desteklemektedir.[19] Aynı zamanda internetin açıklığı ve insan hakları ve temel özgürlükler konusunda da ŞİÖ ve bahsi geçen batılı ülkeler arasında fikir ayrılığı devam etmektedir. Zaten 2017 tarihinde BM Genel Kurulutarafından kurulan hükümet uzmanlarından oluşan grubun raporunu sonuçlandıramaması ŞİÖ üye ülkeleri, özellikle Rusya ve Çin ile batılı ülkeler arasında oluşan ideolojik farklardan

[17] George J. Stein, "Information Attack: Information Warfare In 2025", A Research Paper Presented To Air Force (1996): 2.
[18] Zine Homburger, "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace", Global Society, 33:2 (2019): 233.
[19] Homburger, 233

kaynaklanmaktaydı.[20] Bu ideolojik çatışmaya bir diğer örnek ise 2012 yılında Dünya Telekomünikasyon Teşkilatı (DTB)'nin ileri sürdüğü sözleşmenin batılı devletler tarafından imzalanmaması gösterilebilir. Bu kapsamda AK tarafından hazırlanan ve imzaya sunulan Budapeşte Sözleşmesi'nin Rusya ve Çin tarafından reddedilmesi de ŞİÖ teşkilatının enformasyon konusu başta olmak üzre siber uzaya yönelik görüşlerinin farklılık arz ettiğini gösteren önemli etkenlerdendir.[21]

Dolayısıyla görüldüğü üzere ŞİÖ'nün internetin yönetilmesi konusunda görüşleri batılı devletlerin görüşleri ile bağdaşmamaktadır.

ŞİÖ'nün siber alana yönelik politikalarını açıklayan temel belgelerden biri 2011 yılında BM Genel Kurulu'nun onayına sunulan "International Code of Conduct"[22] (ICC) taslağıdır. Taslak özellikle batılı devletler tarafından reddedilmiştir. Taslak incelendiğinde örgütün internet ortamındaki ilişkilerin devletlerin egemenliği ilkesine dayandırılması gerektiğine dair görüş ortaya koyduğu görülmektedir.[23] Diğer yandan ciddi kontrol mekanizmalarını kendisinde barındırmaktadır. Tabii ki bütün bu yaklaşımlar aslında örgütün önemli 2 üyesi olan Çin ve Rusya'nın demokrasi noktasındaki yaklaşımları ile de örtüşmektedir. Keza ŞİÖ'nün esas yönetici ülkeleri olarak görülen Rusya ve Çin siber alana egemenlik ve milli güvenlik prensipleri çerçevesinde bakmakta ve bu anlamda Bilgi ve İletişim Teknolojileri (BİT), onların her türlü hizmet ve ürünleri üzerinde devletlerin bağımsız kontrol haklarının olduğunu öngörmektedir.[24] Nitekim Budapeşte Sözleşmesinin 32. maddesinde ifadesini bulan bir devletin belli şartlarda diğer devletin de ülkesini kullanarak bilgi toplama yetkisinin olabileceğine dair yaklaşım ŞİÖ tarafından reddedilmektedir. Bunun tersine ICC'de ŞİÖ egemenlik ve milli

---

[20] Theresa Hitchens & Nancy W. Gallagher, "Building confidence in the cybersphere: a path to multilateral progress", Journal of Cyber Policy (2019): 5-6. DOI: 10.1080/23738871.2019.1599032

[21] See Council of Europe, "Chart of signatures and ratifications of Treaty 185", status as of 18/04/2018, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (E.t. 08 Aralık 2021)

[22] Uluslararası Davranış Yönetmeliği olarak bilinen taslak bilgi ve iletişim alanında uluslararası işbirliği imkanlarını ele almakta ve devletlerin davranışlarına dair normlar içermekteydi.

[23] BM GK A/66/359.

[24] Üye devletlerin, gözlemci devletlerin ve diyalog ortaklarının listesi için Şanghay İşbirliği Örgütü'nün web sitesine bkz. http://eng.sectsco.org/about_sco/ (e.t. 08 Aralık 2021)

güvenlik hususuna yoğunlaşarak bahsi geçen kavramları kırmızı çizgi olarak görmektedir.[25]

Aslında bir anlamı ile ŞİÖ'nün ileri sürdüğü düzenlemeler devletlerin internetle ilgili bütün toplumsal konuları düzenlemelerine meşruiyet kazandırmakta ve bahsi geçen hususları egemenlik hakları çerçevesinde değerlendirmektedir. Nitekim devletin bilgi ve iletişim teknolojileri ürün ve hizmetlerine yönelik bağımsız kontrol etme hakkının bulunduğuna dair benimsenen görüş söylenilenlerin birer kanıtıdır.[26]

Diğer yandan taslakta bilgi ve iletişim teknolojilerinin kriminal ve terörist amaçlarla kullanımına dair de ibarelere yer verilmiştir. Şöyle ki örgüt üyelerince ayrılıkçılık, terörizm ve ekstremizm içeren bilgi içeriklerinin milli güvenliği tehdit ettiği karara bağlanmış ve önüne geçilmesi için gerekli işbirliği çağrıları yapılmıştır. Bu yaklaşım Rusya'nın bilgi güvenliği stratejisinde de kendi içeriğini bulmakta olup iç ve dış bilgi tehditlerine karşı devlet korumasına yönelik yaklaşımlar benimsenmiştir.[27]

ŞİÖ ve AB ülkeleri arasında siber boyutta rekabete dayalı genişleme savaşı da görülmektedir. Örneğin AB'nin AK ile işbirliği çerçevesinde başlattığı siber suçların önlenmesi için evrensel faaliyet (GLACY) projesinin ASEAN ülkeleri arasında da teşvik edilmesi sonucunda Budapeşte Sözleşmesi Filipinler tarafından onaylanmıştır.[28] Buna karşılık Çin'in önderliğinde başlatılan siber güvenlik alanında ASEAN bölgesel formu ise Pekin'in evrensel çerçevede genişleme politikalarını yansıtmaktadır.[29]

Siber alanda düzenleme konularının ideolojik temellere dayandığını ve bu temeller kapsamında propaganda sürecinin yürütüldüğünü bir örnekte daha görmekteyiz. Örneğin bazı ülkeler hem Çin ve Rusyan'ın başını çektiği ŞİÖ

---

[25] Budapeşte Sözleşmesi'nin resmi metni için bkz. RG 9 Ağustos 2014, Sayı: 29083, https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5.htm (e.t. 19. 08. 2022); Homburger, 234.

[26] İbid.

[27] Doctrine of Information Security of the Russian Federation, approved by Decree of the President of the Russian Federation No. 646 of 5 December 2016, Para. 2(c).

[28] Chat Le Nguyena, Wilfred Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action' ", Computer law & security Review 40 (2021): 5.

[29] Cai Cuihong, "Cybersecurity in the Chinese Context", China Quarterly of International Strategic Studies, Vol. 1, No. 3 (2015): 491.

politikalarına yeşil ışık tutmakta hem de AK üyeliğinden dolayı Budapeşte Sözleşmesi'ni kabul etmektedir. Örneğin Sırbistan ve Ermenistan bu kabilden olan devletlerdendir.[30]

Nihayetinde Çin ve Rusya bilginin içeriğini dahi kendilerinin milli güvenliğine tehdit oluşturduğunu söylerken ABD ve batılı devletler bu konuda ifade özgürlüğü ve diğer temel haklardan yola çıkarak kontrolsüzlük temelli bir yaklaşım sergilemektedir. Bu konuda en son ABD'de ve Fransa'da gerçekleşen seçimler noktasında meydana gelen etkiler sonucunda batılı devletlerin de görüşlerinde bir kısım değişiklikler istisnai olarak değerlendirilmelidir.[31]

ŞİÖ üyelerinden Çin, Rusya, Özbekistan ve Tacikistan resmi temsilcileri tarafından BM Genel Kurulu'na sunulan Düzenleme Taslağında internet ve diğer telekuminaksyon vasıtalarının hem sivil, hem de askeri amaçlar için istifade edilebileceği belirtilmekle beraber bu sistemlerin sivil amaçlara hizmet edecek şekilde kullanılması gerektiğinin altı çizilmiştir. Taslağın amacı aşağidaki şekilde belirtilmiştir:

"Bu taslağın amacı siberuzayda devletlerin hak ve sorumluluklarəını belirlemek, onların sorumlu ve kurucu davranışlarını teşvik etmek ve siberuzayda ortak sorun ve tehditlere karşı işbirliğini artırmak, böylelikle ağlar da dahil olmak üzere enformasyon ve komünikasyon teknolojileri uluslararası istikrar ve güvenliği sürdürmekle yalnız insanların iyiliği, sosyal ve ekonomik kalkınma amacıyla kullanılır ve kullanılabilir."

ŞİÖnün ileri sürdüğü taslak *"Tüm Devletlerin egemenliğine, toprak bütünlüğüne ve siyasi bağımsızlığına saygıyı, insan haklarına ve temel özgürlüklere saygıyı ve tüm ülkelerin tarih, kültür ve sosyal sistemlerinin çeşitliliğine saygıdan doğan uluslararası ilişkileri yöneten evrensel normları tanımak ve Birleşmiş Milletler Şartına uymak"*; *"Ağlar da dahil olmak üzere enformasyon ve komünikasyon teknolojilerini düşmanca faaliyetler veya saldırganlık eylemleri gerçekleştirmek, uluslararası barış ve güvenliğe tehdit oluşturmak amacıyla kullanmamak ve enformasyon silahları ve ona bağlı teknolojiler üretmemek."*; *"Ağlar da dahil olmakla enformasyon ve komünikasyon teknolojilerini kullanan terörist ve suç teşkil eden eylemelere*

[30] Homburger, 236-237.

[31] Anders Henriksen, "The end of the road for the UN GGE process: The future regulation of cyberspace", Journal of Cybersecurity, Cilt 5, Sayı 1 (2019): 5, https://doi.org/10.1093/cybsec/tyy009

karşı birlikte mücadelede ve terörizmi, ayrılıkçılığı veya aşırılığı kışkırtan veya diğer ülkelerin siyasi, ekonomik ve sosyal istikrarının yanı sıra manevi ve kültürel çevrelerini baltalayan bilgilerin yayılmasını engellemede işbirliği yapmak." gibi son derece önemli konularda normlar içermekteydi ve devletlerin gönüllü olarak taahhüdünü öngörmekteydi[32]

A. Çin

Çin Komunist Partisi Birinci Sekreteri Ji Xinping 2015'de yapılan Dünya İnternet Konferansın'daki konuşmasında konumuz açısından önemli noktalara değinerek katı egemenlik tezini desteklediklerini şöyle ifade etmiştir:

"Küresel siber uzay yönetiminde reformları teşvik etmek için, aşağıdaki ilkelerde ısrar etmeliyiz: ilk olarak, İnternet egemenliğine saygı gösterin. Birleşmiş Milletler Şartı'nda yer alan egemen eşitlik ilkesi, çağdaş uluslararası ilişkilerin temel normlarından biridir. Siber uzay da dahil olmak üzere devletler arası ilişkilerin tüm yönlerini kapsar. Tek tek ülkelerin kendi siber gelişim yollarını ve siber düzenleme modellerini bağımsız olarak seçme ve uluslararası siber uzay yönetiminnde eşit temelli iştirakına saygı duymalıyız."[33]

Görüldüğü üzere Çin Halk Cumhuriyeti Cumhurbaşkanı Dünya İnternet Konferansı'nda Çin'in internet yönetimine yönelik yaklaşımının klasik yönetim prensipleri ile bağdaştığını dile getirmiştir. Ona göre uluslararası ilişkilerin diğer alanlarına münasebette benimsenen ilkelerin siber uzay için de geçerli olduğu tezi doğrudur.[34] Xinping'in konuşması değerlendirilirken Çin'in dünyanın en çok internet kullanıcısına sahip devleti olduğu unutulmamalıdır. 2016 tarihli istatistiğe göre Çin ahalisinin yaklaşık 688 milyonu çevirimiçidir.[35]

---

[32] Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359). https://undocs.org/A/66/359

[33] Xi Jinping, excerpt from his keynote address to the World Internet Conference in 2015, https://www.chinadaily.com.cn/world/2015wic/2015-12/16/content_22724841.htm (e.t. 01. 09. 2022)

[34] Jinghan Zeng, Tim Stevens, Yaru Chen, "China s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" ", Politics & Policy, Cilt 45, Sayı 3 (2017): 432-464. 10.1111/polp.12202, s. 434.

[35] Zeng, Stevens, Chen, 437.

Çin'in internet politikalarına bakıldığı zaman özellikle Arap baharı sürecinden sonra ülkenin son derece kapalı tutum sergilediği ve batı demokrasisinin ürünlerinden sayılabilecek liberal yaklaşımların ülkeye sokulmasının önüne geçilmesi eğilimleri görülmektedir. Bu kapsamda özellikle Çin tarafından internetin ulusötesi özelliğinin önüne geçilmesi için birçok teknik ve diğer tipli önlemler alınmıştır. Çünkü internetin getirdiği yeni imkanların Çin'in merkezi hükümetinin merkezi çerçevede yürüttüğü bilgi ve iletişim politikalarına engel oluşturduğu aşikardır.[36]

2011 ve 2012 senesinden itibaren daha da yaygınlaşan ve geliştirilen siber politikalar Çin'in sosyal istikrar, kamusal güvenlik ve Komünist Partisi'nin (KP) liderliğinin dayanıklılığı hususunda taviz vermeyeceğini göstermektedir.[37]

Çin tarafından yapılan pratik önleyici önlemlere birer örnek olarak kendileri tarafından yaratılan "Sina Weibo"[38] uygulaması gösterilebilir. Sistemin işletim tarzına bakıldığında devlet tarafından denetleme ve kontrol mekanizması olarak kullanıldığı görülmektedir. Hakeza bazı meşhur fikir insanlarının ahlaksız davranış ithamı ile mahkum edilmesinde mevzubahis uygulamanın kullanılması tesadüf değildir.[39] Nitekim bahsi geçen sistem ve diğer bu tipli davranışlardan yola çıkarak söylenilebilir ki Çin tarafı internet ve internet teknolojilerinden meydana gelen her türlü bilginin kendi kontrolünden geçerek topluma yansıtılmasından yanadır ve bu çerçevede topyekün egemenlik prensibini savunmakta, kontrolü devletin egemenlik hakları çerçevesinde değerlendirmektedir. Her ne kadar bu tipli yaklaşımlar bazı yazarlar tarafından KP'nin otoriter siyasetine hizmet şeklinde yorumlansa da uluslararası hukuki yönleri ile devletin egemenlik yetkisi dahilinde değerlendirilecek yanları da yok değildir.[40]

Dolayısıyla Çin'in savunduğu siber yönetim egemenlik ilkelerine dayanmakta ve devletin kontrol mekanizmalarını meşru kılmaktadır. Fakat Çin'in bu yaklaşımının meydana gelmesinde ABD merkezli bir siber alanın

---

[36] Shanthi Kalathil, Taylor C. Boas, Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule (Washington: Brookings İnstitution Press 2003), 3.

[37] Zeng, Stevens, Chen, 438.

[38] https://www.bbc.com/news/technology-39947442 (e.t. 31. 03. 2022.)

[39] Zeng, Stevens, Chen, 439.

[40] Juha Antero Vuori, Lauri Paltemaa, "The Lexicon of Fear: Chinese Internet Control Practice in Sina Weibo Microblog Censorship", Surveillance & Society 13(3/4) (2017): 400-421.

mevcutluğu unutulmamalıdır.[41] Nitekim ABD milli güvenlik ajansına bağlı PRİSM[42] isimli gizli istihbarat programı ve bu program vasıtasıyla ABD'nin denetiminde bulunan siber sahada kendi çıkarları doğrultusunda faaliyetler yapabilme özgürlüğü içerisinde olduğu iddiaları resmi Pekin'in kontrol politikalarının hiç de tamamen siyasi mühaliflerine yönelmediğini tespit etmektedir. Keza PRİSM uygulamasının ABD internet şirketlerinin elinde bulunan şahsi ve ticari bilgilerin devletin eline geçmesine kolayca zemin oluşturmakta olduğu yönünde ciddi iddialar seslendirilirken Google, Facebook, Yahoo, Apple, Microsoft gibi şirketlerin ismi geçmektedir.[43] Zira ABD kendi siber kontrolünde bulunan şirketler vasıtasıyla Çin ve Rusya dahil olmak üzere hatta kendi müttefiklerinden olan AB ülkelerinde de çıkarlarını korumaktadır. Dolayısıyla yukarıda belirttiğimiz örnek olaydan da görülmektedir ki ABD mevcut internet yönetiminin büyük bir kısmında hakimiyetini kurmakla bir taraftan da kendi çıkarlarını korumakta ve bu doğrultuda hareket etmektedir.[44] Haliye mevcut durum diğer devletlerin siber alandaki egemenliklerini kısıtlamakla birlikte iç işlerine karışır nitelikte enformasyon veya dezenformasyon akışlarına müsait zemin oluşturmaktadır. Keza Çin'in aldığı tedbirler hukuken enformasyon sahasını savunma önlemleri şeklinde yorumlanabilir.

Bir defa ABD internetin ve siber alanın evrensel alan olduğunu ve devletlerin egemenlikleri dışında bir evrensellik içerdiği tezini ileri sürse de realitede kendi hâkimiyetinin bulunduğu siber alanda evrenin diğer aktörlerinden daha fazla etki sahibi olmakta ve bunu milli çıkarları doğrultusunda kullanmaktadır.[45] Nitekim Çin'in milli egemenlik tezini ileri sürmesinin önemli etkenlerinden birini de Amerikan merkezci siber alanın mevcutluğu ve bu imkanın hakim devlet tarafından kendi çıkarlarının lehinde, diğer devletlerin ise milli güvenlik ve çıkarlarının aleyhinde olabilecek şekilde kullanılmasıdır. Çin ile beraber Rusya, Brezilya, Güney Afrika ve İran gibi

[41] İbid, s. 440.

[42] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (e.t. 31. 03. 2022)

[43] Greenwald Glenn, And Ewan Macaskıll. 2013. "NSA PRISM Program Taps in to User Data of Apple, Google and Others." The Guardian. June 7. Accessed on December 15, 2021. Available online at https://www. theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

[44] Robert B. Cohen, "Communications Of The Acm", Cilt. 42, Sayı.6 (1999): 37.

[45] Zeng, Stevens, Chen, 440.

devletler devlet merkezli ve egemenlik oryantasyonlu rejim görüşlerini desteklemektedir.[46]

Bütün bu söylenilenler nihai sonuca bağlanmış olursa Çin ve onun görüşlerini destekleyen devletler ABD ve batı destekli özel sektörün egemen (burada özel sektör temsilcilerine veya internet devlerine liberal bir serbestliğin verilmesi söz konusudur.) olduğu şekli ile internetin yönetilmesine karşı çıkmakta ve devlet kontrollü bir internet görüşünü desteklemektedir.

Bu vesile ile Çin ŞİÖ'nün diğer üyeleri ile birlikte 2011 senesinde BM Genel Kuruluna sunulmak üzere siber uzay ile ilgili konuları düzenleyen normlar taslağı geliştirmiştir. Taslak BM Silahsızlandırma Enstitüsü'nün verilerine göre aşırı sert milli egemenlik modeli içerdiği ve bu sebeple baskıcı rejimleri kollayan bir mahiyete haiz olması hasebi ile reddedilmiştir.[47] Yazarlar tarafından taslağın Genel Kurul düzeyinde reddedildiği belirtilmiş olsa da bizce yapılan araştırma sonucunda ilgili taslağın BM Genel Sekreteri'ne gönderildiği tarihi izleyen Genel Kurul oturumu çerçevesinde mevzubahis isimde her hangi bir taslağın müzakereye çıkartılarak reddine rastlanılmamıştır.[48] Nitekim kanaatimizce yazarlar reddedilmiştir derken genel olarak taslakta yer alan fikir ve düşüncelerin mahiyet itibarıyla kabuledilmediğini kastemişlerdir. Daha sonra 2015 tarihinde ŞİÖ tarafından ilgili düzenleme taslağı yenilenmiş fakat yine temel norm olarak internet egemenliği prensibi kendi yerini korumuştur. Çin'in internet egemenliği ile ilgili politikalarına göz atıldığında 2015 tarihinde Xi Jinping'in Wuzhen Konferansı'nda konuşma yaparken buna benzer tespiti ortaya koyduğu görülmekte ve siberalan üzerinde devletin herhangi bir şekilde devlet egemenliğinden yola çıkarak kontrol mekanizması oluşturması gerektiğini savunduğu bilinmektedir.[49]

İnternet politikaları kapsamında milli egemenlik tezini savunmasına rağmen ve bu tezin pratik anlamda uygulamaya konulmasını sağlamak için Büyük Çin Güvenlik Duvarı ismi verilen teknolojik savunma sistemleri kuran resmi Pekin 2012'ye kadar mevzubahis tezinin uluslararası anlamda yaygınlaşması için pek de gayret sarf etmemiş, yalnız son Cumhurbaşkanı

[46] İbid
[47] Ibid.
[48] İlgili Genel Kurul oturumunun resmi stenogramı için bkz. UN doc. A/66/PV.71.
[49] Zeng, Stevens, Chen, 441.

iktidara geldikten sonra ABD'nin çokpaydaşlı yaklaşım (multi-stakeholderizm) ilkelerine dayalı tüm aktörlerin katılımı ile yönetilmesi gereken internet siyasetinin tam tersi olan milli egemenlik tezi ile desteklenen politikaları uluslararası camiada yaygınlaştırmaya başlamıştır[50].

B. Rusya

ŞİÖ'nün üyesi olan Rusya'nın internetteki yönetim ve yetki konularında benimsediği yaklaşım Çin'in yaklaşımlarından pek farklılık göstermemektedir. Bir defa Rusya da bilginin serbest akışı konusunda internetin getirdiği yenilikleri birer tehdit olarak görmekte ve bu bağlamda milli sınırların yetersiz kaldığı, dolayısıyla durumun toplum veya devlete yönelik zarar oluşturabileceği kaygılarını paylaşarak internet egemenliği tezini savunmaktadır.[51]

Rusya'nın siber uzaya yönelik yaklaşımlarını incelerken üç önemli strateji belgesinin göz önünde tutulmasının faydalı olduğu kanaatindeyiz. Bunlardan biri "Uluslararası Bilgi Güvenliği Taslak Sözleşmesi" (Draft Convention on International Information Security), bir diğeri Rusyan'ın askeri siber doktrini olarak da nitelendirilen Rusya Federasyonu Silahlı Kuvvetlerinin Enformasyon Sahasında Faliyerlerine dair Konseptüal Görüşler" (Conceptual Views on the Activity of Russian Federation Armed Forces in Information Space), sonuncusu ise "Bilgi Güvenliği Doktrini" isimli dökümanlardır.

Rusya'nın siber politikalarının gelişmesinde rol oynayan 2010 senesinin 1 Aralık tarihinde Duma seçimlerinden derhal sonra iddia ettiklerine göre onlara karşı başlatılan enformasyon savaşı kampanyası vurgulanmadan da geçilmemelidir.[52]

Nitekim Rusyan'ın siber uzaya yönelik politikalarını değerlendirerek nihai pozisyonu anlamak adına her üç belgenin tek tek değerlendirilmesi faydalı olur.

---

[50] İbid, 442-443.

[51] Keir Giles, "Russia's Public Stance on Cyberspace Issues", in C. Czosseck, R. Ottis, K. Ziolkowski (eds), 4th International Conference on Cyber Conflict, Tallinn: NATO CCD COE (2012): 63.

[52] İbid.

1. Uluslararası Bilgi Güvenliği Taslak Sözleşmesi

Moskova Devlet Üniversitesi'ne (MDÜ) bağlı bilgi güvenliği konularından sorumlu enstitünün önderliği ile hazırlanan Taslak Sözleşme 2011 tarihinde Yekaterinburg'da gerçekleştirilen ve siber konulardan sorumlu üst düzey resmi katılımcıların iştiraki ettiği konferans sırasında ilan edilmiştir. Aynı zamanda unutulmaması gerekiyor ki ilan edilen strateji belgesi az öncesinde Birleşmiş Milletler'e sunulan ve Rusya'nın da dahil olduğu ŞİÖ üye ülkelerinin mevkisini ortaya koyan düzenleme taslağını takip etmekteydi.[53]

Hak ve özgürlüklerin ihlalinden geri durulması, bilgi ve iletişim teknolojilerinin hukuk-dışı amaçlarla kullanılmaması gibi ortak maddeleri içerse de bahsi geçen belgede batı görüşünü desteklemeyen hususlar bulunmakta ve kendini daha açık bir şekilde bilgi içeriklerine yönelik Rusya'nın tehdit algısı ile göstermektedir.[54] Bir diğer ifade ile Rusya tarafı toplumu etkilemek için bilgi içeriklerinin kullanılmasını tehdit olarak görmekte ve bu konuda titiz yaklaşım sergilemektedir. Dolayısıyla Rusya bilgi içeriklerinin de devlet kontrolünden arındırılmış bir şekilde serbest dolaşımından rahatsızlığını dile getirmektedir. Örneğin Londra Konferansı sırasında Birleşmiş Krallık (BK) Dışişleri Bakanı William Hague'nin *"siber alan inovasyona açıklığı, düşünce, bilgi ve ifadelerin serbest dolaşımını korumaktadır"* vurgusuna karşın Rusiyalı Bakan Schegolev *"bilgi akışı milli yasalara ve anti terör değerlendirmelerine tabii olmalıdır"* yaklaşımını ortaya koyarken milli güvenlik sebebiyle hak ve özgürlüklerin kısıtlanabilirliğini savunmuştur.[55] Nihayetinde yaşanan polemikten anlaşılmaktadır ki Rusya internette bilgi dolaşımı hususunda daha katı ve merkeziyetçi yönetim sistemi öngörmektedir.

Taslak sözleşmede yer alan çok önemli iki kriterden biri bilgi ve iletişim teknolojilerini diğer devletlerin iç işlerine karışır nitelikte kullanmaktan geri durmaya ve siber alanda üstün pozisyonda bulunmanın tehdit olarak kullanımına dair yapılan vurgulardır.[56] Aslında baktığımızda özellikle üstün

---

[53] Oleg Demidov, "Internatıonal Regulation Of Informatıon Security And Russia's National Interests", Security Index: A Russian Journal on International Security, 18:4, (2012): 18, DOI: 10.1080/19934270.2012.714597; Giles, 64.

[54] Roger Hurwitz, "The Play of States: Norms and Security in Cyberspace, American Foreign Policy Interests", The Journal of the National Committee on American Foreign Policy, 36:5 (2014) : 323-324.

[55] Demidov, 22; Giles, 65.

[56] Giles, 65.

mevkide bulunmak hususunda taslak sözleşmede yer alan düzenleme ABD yönetimine karşı belirlenen politikanın ürünüdür. Çünkü halihazırda ABD eksenli bir enformasyon alanı var olmakta ve bu anlamda ABD'nin siber uzayı manipüle etme yetki ve imkanlarının bulunduğu da aşikârdır.[57]

Bir başka cümle ile ifade edilmiş olursa Rusya'nın ileri sürdüğü argüman bilgi ve iletişim teknolojilerinin oluşturduğu, internetin ise ana kaynağı olarak görüldüğü siber alanda kapasitesi en fazla olan ve bu kapasite fazlalığının verdiği hakimiyetin ABD'nin elinde olduğunu dillendirmekte ve bu imkanların, yani dominant pozisyonda bulunma imkanının tehdit olarak kullanımı ihtimalini istisna etmemektedir. Zira uluslararası hukuki yönleri ile baktığımızda da ortak bir alan olarak görülen siber uzayın yalnız bir devletin kontrolünde olması ve bu kontrolün tehdit olarak kullanılması elbette ki meşru dayanaklardan yoksundur. Keza "Devletlerin Ay'da ve Diğer Gök Cisimlerindeki Faaliyetlerini Düzenleyen Anlaşma", "Antarktika Antlaşması" gibi uluslararası sözleşmeler mahiyetleri itibarıyla siber alanla benzerlik içeren alanları düzenlerken tüm devletlerin ortak iradelerini esas alan yaklaşım benimsemişlerdir.[58] Eğer benzer tutum siber alana münasebette de sergilenmez ise kapasite yarışının meydana gelebileceği ve bu yarışın uluslararası barış ve güvenliği tehdit altında koyacağı gün gibi aydındır.

Taslakta yer alan ve Rusya tarafının diğer grupla anlaşamadığı hususlardan biri de internet egemenliği ile ilgili ortaya koyduğu yaklaşımdır. Bu anlamda Rusya'nın sergilediği mevki kendisi gibi düşünen ŞİÖ, Bağımsız Devletler Birliği (BDT), Kollektif Güvenlik Sözleşmesi Örgütü (KGSÖ) gibi kuruluşlara üye olan ülkelerin yaklaşımı ile örtüşmekte ve tam olarak bütün internet kaynakları üzerinde milli kontrolün varlığı düşüncesini desteklemektedir.[59] Eklememiz gerekiyor ki az önceki cümlede bahsedilen kontrol devletin fiziki sınırları içerisinde bulunan her türlü internet kaynağını kapsamakta ve bu yönüyle klasik devlet egemenliği ve ulus devlet teorisini ana kaynak olarak görmektedir. Belirttiğimiz koşullar taslağın 5.5. maddesinde aşağıdaki gibi ifade edilmektedir:

---

[57] Milton L. Mueller, Ruling the Root Internet Governance and the Taming of Cyberspace (Cambridge, Massachusetts: The MIT Press 2002), 67-98.

[58] Bkz. Agreement governing the Activities of States on the Moon and Other Celestial Bodies, New York, 5 December 1979, United Nations, Treaty Series , vol. 1363; The Antarctic Treaty, United Nations, Treaty Series No. 5778.

[59] Giles, 65.

"Her üye devlet, egemen normlar belirleme ve bilgi alanını kendi ulusal yasalarına göre yönetme hakkına sahiptir"

ABD'nin Dışişleri Bakanı Hillary Clinton vasıtası ile Aralık 2011'de dile getirdiği gibi Rusya'nın bu yaklaşımı aynı zamanda devletlerin üzerine kendi yetki alanında bulunan ülkeden gerçekleştirilebilecek zarar verici enformasyon aktivitelerinin önüne geçme yükümlülüğü de koymaktadır. Bir başka ifade ile taslağın 6.2. maddesi ile ileri sürülen görüş devletlerden kendi ülkelerinde bulunan bilgi ve iletişim altyapılarından düşmanca amaçlar için kullanılmamasına dair garanti istemekte ve bu tipli faaliyetlerin kaynağının belirlenmesi yönünde işbirliği yükümlülüğünü getirmektedir.[60] Giles'in cümleleri ile ifade etmiş olursak, *"Yalnızca kendi yetki alanlarındaki içeriğin yasallığını denetlemekle kalmamalı, aynı zamanda diğer tüm imzacıların yargı alanlarında zararsız ve düşmanca kabul edilmemesini sağlamalıdır - aksi takdirde, derhal Sözleşme'yi ihlal eden düşmanca faaliyetlere izin vermekle suçlanabilirler."*[61]

Taslağın ortak bir noktada buluşmaya engel olan ibarelerinden biri de sözleşmenin 9.5 maddesinde yer alan aşağıdaki yaklaşımdır:

"Bilgi alanında terör eylemlerinin yürütülmesi için istihdam edilmekle yasal olarak ilişkili olan Taraf Devletin topraklarındaki bilgi ve iletişim altyapısının belirli bölümlerine yasal erişimi garanti edecek yasal veya diğer nitelikteki gerekli adımları atmak."

Giles'e göre bu maddeden yola çıkarak meydana gelen uyuşmazlığın iki temel unsuru bulunmaktadır.[62] Biri terörizm, bir diğeri ise yabancı devletin enformasyon alanına giriş kavramlardır. Terörizm konusunda söylenilebilir ki Rusya ve diğer devletlerin uyuşmaz yaklaşımları öteden beri var olmaktadır ve bu uyuşmazlık siber alana özel değildir.[63] Çünkü "terörizm" kavramının uluslararası hukukta genel kabul gören bir tanımı bulunmamaktadır. Dolayısıyla siber terörizm anlamında meydana gelen uyuşmazlık aslında Rusya ve diğer devletlerin terörizm derken neyi kastettikleri çerçevesinde meydana gelen farklılıklardan doğan uyuşmazlıkla ayniyet teşkil etmektedir.

---

[60] International code of conduct for information security, Annex to the letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359), 2011.

[61] Giles, 65.

[62] İbid, 66.

[63] Anna-Maria Talihärm, "Cyberterrorism: in Theory or in Practice?", Defence Against Terrorism Review, Cilt. 3, Sayı. 2 (2010): 59-60.

Nihayetinde taslak sözleşmeyi incelediğimiz sırada ileri çıkan temel ayrım Batı görüşünün özgür, kısıtlanmamış ve kontrol edilmeyen bilgi akışı tezini savunduğu, Rusya ve onun gibi düşünen ülkeler bloğunun ise bilgi akışı noktasında belli kontrol mekanizmaları düşünmesi ve özellikle siber alan üzerinde milli egemenlik ilkeleri görüşünü desteklemesidir.[64] Dolayısıyla taslaktan da yola çıkarak söylenilebilir ki Rusya'nın siber alana yönelik görüşleri milli egemenlik ve bilgi dolaşımı üzerinde devletin topyekün kontrolü şartlarına dayanmaktadır ve her türlü siber altyapı, siber içerik üzerinde denetlenebilir bir sistem hedeflemektedir.

2. Rusya Federasyonu Silahlı Kuvvetlerinin Bilgi Alanındaki Faaliyetlerine İlişkin Kavramsal Görüşler

Bahsi geçen strateji belgesi 14 Aralık 2011 tarihinde Berlin Konferansı sırasında ilan edilmiş ve 22 Aralık 2011'de yayınlanmıştır.[65]

Askeri strateji ortaya koyan bu belgede çalışmamız açısından ilgimizi çeken unsurlardan özellikle enformasyon savaşı kavramı üzerinden devam etmemiz gerekmektedir. Bir defa belge enformasyon çatışmaları ve enformasyon savaşı kavramlarını kullanarak bu yönde Rusya Savunma Bakanlığı'na bağlı oluşabilecek herhangi bir siber saldırıyı önlemek, belirlemek ve gerekli tedbirleri almak için hedef imha mekanizmalarının oluşturulduğunu beyan etmektedir.[66]

Zira belgede bilgi veya enformasyon savaşı kavramı çok geniş bir şekilde ele alınmış ve özellikle psikolojik etki veya toplumun istikrarını ortadan kaldıracak şekli ile toplum üzerinde psikolojik destabilize faaliyetlerinin yürütülmesini de kavram içerisinde ele almakta ve bu faaliyetlerin hükümet üzerinde yabancı güçlerin çıkarları doğrultusunda karar alma baskısı olarak yorumlamaktadır.[67] Belgede enformasyon savaşı aynen şöyle tanımlanmaktadır:

---

[64] Giles, 67.

[65] Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?", The Journal of Slavic Military Studies, 27:1 (2014): 109. 101-130, DOI: 10.1080/13518046.2014.874845; Belgenin Rusça tam metni için bak. http://www.pircenter.org/media/content/files/9/13480921870.pdf (e.t. 04.03.2022)

[66] Thomas, 109-110; Giles, 67.

[67] Media Ajir and Bethany Vailliant, "Russian Information Warfare: Implications for Deterrence Theory", Strategic Studies Quarterly, Cilt. 12, Sayı. 3 (2018): 72.

""Bilgi sistemlerine, süreçlere ve kaynaklara, kritik öneme sahip yapılara ve diğer yapılara zarar vermek, siyasi, ekonomik ve sosyal sistemleri yıkmak amacıyla bilgi alanında iki veya daha fazla devlet arasındaki çatışma, toplumu ve devleti istikrarsızlaştırmak için nüfus üzerinde kitlesel psikolojik çalışma ve hükümeti karşı tarafın çıkarları doğrultusunda kararlar almaya zorlamak."

Strateji senedinde Rusya Silahlı Kuvvetleri'nin siber anlamda da kullanılabileceğinin gerekliliğine dair fikirler yer almakta ve bu anlamda gerekli kuvvetlerin ve kaynakların başka devletlerin ülkesine gönderilmesi ile de enformasyon güvenliğinin sağlanması söz konusu olmaktadır.[68] Yaklaşım Rusya'nın siber alanda güvenlik konularını ne kadar önemli bir şekilde değerlendirdiğini ortaya koymakta ve aslında onların siber alanda meydana gelebilecek saldırılarla klasik saldırı kavramları arasında pek bir fark ortaya koymadığını da göstermektedir. Kanımızca bu söylediklerimizi Rusya tarafından önemli kılan sebep ise, yani siber alanda gerçekleştirilen bütün faaliyetlerin hatta askeri düzeyde denetlenebilmesine yönelik Rusya tarafından ileri sürülen görüşleri önemli kılan son dönemler internet de dahil olmak üzere teknolojik gelişmelerin 100 milyonlarca insanı bir araya getirmesi ve evrensel çerçevede bir enformasyon alanının oluşturulmasıdır.[69]

3. Rusya'nın Enfarmasyon Güvenliği Doktrini

Doktrin 2000 tarihinde yayınlanmak olmuş ve Rusya'nın politikalarının ana unsurlarını kendi içeriğinde bulundurmakta ve bir anlamda milli politika şeklinde de değerlendirilebilmektedir.[70] İlk bakışta bahsedilen doktrin incelendiğinde aslında serbest enformasyon akışı, şahısların anayasal hak ve özgürlüklerinin temini yönünde vurgular söz konusu olsa da sonraki maddelerde devletin medya vasıtası ile toplumsal görüşü yönetebilme yetkisinin bulunduğu hususu karara bağlanmıştır.

Doktrinde yeralan bütün ifadelere yer vermeksizin özetle söylenilebilir ki Rusya tarafı bilgi ve iletişim teknolojileri vasıtası ile iç politikasının dış güçler tarafından şekillendirilmesinde zarar görmekte ve bu tipli faaliyetlerinin önüne geçmeyi milli güvenlik meselesi haline getirmektedir.

---

[68] Giles, 68.

[69] İbid, s. 68-69.

[70] Tam metin için bkz. https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (e.t. 04.03.2022.)

Dolayısıyla Rusya'nın bu fikirlerden de yola çıkarak her türlü medya ve ifade özgürlüğünün sağlanması gerektiğine vurgu yapmakla birlikte bütün sürecin devletin üstün kontrolü içerisinde yürütülmesini doğru görmektedir.[71]

Rusya'nın özellikle 2010-11 tarihlerinden itibaren Arap dünyasında yaşanan Arap baharı isimli ve özellikle de bilgi ve iletişim teknolojileri vasıtası ile gerçekleştirilen siyasi protesto eylemleri ve devrimler çerçevesinde de rahatsızlık hissettiği görülmekte ve bu rahatsızlığın birer örnek olarak o dönemin Cumhurbaşkanı Dimitri Medvedev tarafından 2011 tarihli bir konferansta şöyle dile getirildiğini aşağıda ifade edebiliriz[72]:

"Ortadoğu'da ve Arap dünyasında ortaya çıkan duruma bakın. Son derece kötü. Önümüzde büyük zorluklar var... Gerçeğin gözlerinin içine bakmamız gerekiyor. Bu bizim için hazırladıkları türden bir senaryo ve şimdi onu gerçekleştirmek için daha da çok çalışacaklar."

Nitekim Rusya interneti ve bilgi ve iletişim teknolojilerinin getirdiği yenilikleri Batı görüşlü veya batının desteklediği grupların kendilerine haiz görüşleri ve çıkarlarını sağlamak adına diğer devletlerin iç işlerine karışır bir şekilde kullandığını ileri sürmektedir. Dolayısıyla enformasyon savaşı ve bunun etkilerinin önüne geçmek için hazırladığı mekanizmaların doğrultusunda ortaya koyduğu kendi siber alanını koruma teşebbüslerini bahsedilen gerçeklikler ile ilişkilendirmektedir. Zira Rusya hatta kendi enformasyon alanına dahil olmakla toplumun sosyo-psikolojik yapısının istemediği bir şekle dönüştürülmesini de milli güvenlik meselesi olarak görmekte ve bütün bunları hesaba katarak geniş bir internet egemenliği kavramını müttefiki Çin gibi savunmaktadır.

VI. SONUÇ

Son istatistik verilere göre dünya ahalisinin yarısından fazlası "online" hayat yaşamaktadır. Özellikle internet devrimi ile birlikte insanlar hayatlarının büyük bir kısımını çevrimiçi geçirmekte, sosyal yaşamlarını siberalana taşımış bulunmaktadırlar. "Metaverse" girişimi ile birlikte daha da heyecan kazanmaya başlayan bu süreç görüş ve pozisyonları incelediğimiz makalemizden anlaşıldığı üzere ŞİÖ ve üye ülkeleri tarafından pek olumlu

[71] İbid, s. 70-71.

[72] Dmitri Medvedev, "Dmitriy Medvedev provel vo Vladikavkaze zasedaniye Natsionalnogo antiterroristichesko go komiteta," 22 February 2011. http://www.kremlin.ru/transcripts/10408. (E.t. 16.12.2021)

karşılanmamaktadır. Özellikle enformasyonun serbest dolaşımı konusunda örgüt muhafazakar yaklaşım benimsemekte ve devlet egemenliği tezini savunmaktadır. Nitekim Rusya ve Çin başta olmak üzere Örgüt üyeleri kendi enformasyon alanlarının tamamen kendi kontrollerinde bulunduğu bir sistem arzu etmektedir. Dışarıdan rızalarının aleyhinde ülkelerine yönelik dezenformasyon olarak gördükleri enformasyon müdahalelerini ise iç işlerine karışılmaması yasağının ihlali olarak görmektedirler.

ŞİÖ tarafından BM'ye 2011 ve yenilerek 2015 tarijinde sunulan taslak maddelerden ve 2009 tarihli Yekaterinburg Sözleşmesinden anlaşılmaktadır ki örgüt "enformasyon silahları", "enformasyon savaşı" gibi kavramları da benimsemiş bulunmaktadır. Hakeza birer dezenformasyon olarak da nitelendirebileceğimiz bahsi geçen müdahaleler yalnız içişlerine karışmak olarak değil, siber saldırı veya siber savaş olarak da değerlendirilebilmektedir. Nihayetinde makalemiz boyunca incelediğimiz belge ve görüşlerden yola çıkılarak dezenformasyon niteliğindeki bilgi saldırıları ŞİÖ tarafından iç işlerine müdahale olarak değerlendirilmekte ve uluslararası hukukun ihlali sayılmaktadır.

Diğer yandan mevzubahis dezenformasyon ortamının oluşmasında Amerikan merkezli internet altyapısının rolü es geçilmemelidir. Nitekim bilgi ve iletişim teknolojileri alanında dominant pozisyona sahip ABD'nin enformasyon tekeline sahip olması diğer devletlere karşı dezenformasyon olasılılığını artırmaktadır. Keza mevcut durumda her ne kadar Çin ve Rusya gibi devletlerin kısıtlamalarla zengin internet düzenlemeleri insan hak ve özgürlüklerine negatif etkide bulunmuş olsa da milli çıkarlar ve güvenlik noktasında tamamen ihtiyaçtan yoksun değildir. Dolayısıyla bahsi geçen düzenlemeler insan hak ve özgürlüklerini kısıtlamayacak biçimde kullanıldığı takdirde milli güvenliğini koruma önlemleri olarak değerlendirilebilir.

KAYNAKÇA

Ajir, Media and Vailliant, Bethany. "Russian Information Warfare: Implications for Deterrence Theory". Strategic Studies Quarterly, Cilt. 12, Sayı. 3 (2018): 72.

Bozkurt, Muharrem Uğur, "Siber Saldırıların BM Şartı'nda Yer Alan Silahlı Saldırı Kavramı Kapsamında Değerlendirilmesi", Çanakkale Araştırmaları Türk Yıllığı, Sayı. 32 (2022): 29.

Cohen, Robert B. "Communications Of The Acm". Cilt. 42, Sayı.6 (1999): 37.

Cuihong, Cai. "Cybersecurity in the Chinese Context". China Quarterly of International Strategic Studies, Vol. 1, No. 3 (2015): 491.

Demidov, Oleg. "Internatıonal Regulation Of Informatıon Security And Russia's National Interests". Security Index: A Russian Journal on International Security, 18:4, (2012) 15-32, DOI: 10.1080/19934270.2012.714597

Doctrine of Information Security of the Russian Federation, approved by Decree of the President of the Russian Federation No. 646 of 5 December 2016

Giles, Keir, "Russia's Public Stance on Cyberspace Issues". in C. Czosseck, R. Ottis, K. Ziolkowski (eds), 4th International Conference on Cyber Conflict, (Tallinn: NATO CCD COE, 2012)

Glenn, Greenwald and Macaskill, Ewan. 2013. "NSA PRISM Program Taps in to User Data of Apple, Google and Others." The Guardian. June 7. Accessed on December 15, 2021.

Hasan, Abu Saleh Md Mahmudul. "Uluslararası Hukukta Devletlerin İçişlerine Karışmama İlkesinin İncelenmesi: Bangladeş Örneği", Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü, Hukuk Anabilim Dalı, Kamu Hukuku Bilim Dalı, Doktora Tezi (Yayınlanmamış), Bursa 2021

Henriksen, Anders. "The end of the road for the UN GGE process: The future regulation of cyberspace". Journal of Cybersecurity, Cilt 5, Sayı 1 (2019): 5, https://doi.org/10.1093/cybsec/tyy009

Hitchens, Theresa and Gallagher, Nancy W. "Building confidence in the cybersphere: a path to multilateral progress". Journal of Cyber Policy (2019): 5-6. DOI: 10.1080/23738871.2019.1599032

Homburger, Zine. "The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace". Global Society, 33:2 (2019).

Hurwitz, Roger. "The Play of States: Norms and Security in Cyberspace, American Foreign Policy Interests". The Journal of the National Committee on American Foreign Policy, 36:5 (2014) : 323-324.

Jinping, Xi. excerpt from his keynote address to the World Internet Conference in 2015 (Xinhua News 2015)

Kalathil, Shanthi and Boas, Taylor C. Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule. Washington: Brookings İnstitution Press 2003.

Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General (A/66/359).

Mueller, Milton L. Ruling the Root Internet Governance and the Taming of Cyberspace. Cambridge, Massachusetts: The MIT Press 2002.

Nguyena, Chat Le and Golman, Wilfred. "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action' ". Computer law & security Review 40 (2021): 5.

Perritt Jr, Henry H. "The Internet Is Changing the Public International Legal System". 88 Ky. L.J. 885 (2000): 886.

Shaw, Malcolm N., International Law, Eighth Edition. Cambridge University Press 2017.

Stein, George J. "Information Attack: Information Warfare In 2025", A Research Paper Presented To Air Force, August 1996.

Talihärm, Anna-Maria. "Cyberterrorism: in Theory or in Practice?". Defence Against Terrorism Review, Vol. 3, No. 2, pp. 59-74.

Thomas, Timothy. "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?". The Journal of Slavic Military Studies, 27:1 (2014): 109. 101-130, DOI: 10.1080/13518046.2014.874845

Tosun, Fatih. "Uluslararası Hukuk'ta "Kuvvet Kullanma Ve Karışma" Kavramlarının Değişen Anlamı". Güvenlik Stratejileri Dergisi, Cilt: 5, Sayı. 9, Ankara 2009

USAF, Cornerstones of Information Warfare.

Vuori, Juha Antero, Paltemaa, Lauri. "The Lexicon of Fear: Chinese Internet Control Practice in Sina Weibo Microblog Censorship". Surveillance & Society 13(3/4) (2017): 400-421.

Yılmaz, Esat Mahmut, "Uluslararası Hukukta Saldırı Suçu", Doktora Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara 2011

Zeng, Jinghan, Stevens, Tim and Chen, Yaru. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty" ". Politics & Policy, Volume 45, No. 3 (2017)

http://eng.sectsco.org/about_sco/ (e.t. 31. 03. 2022)

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures (E.t. 08 Aralık 2021)

http://eng.sectsco.org/about_sco/ (e.t. 08 Aralık 2021)

https://undocs.org/A/66/359 (e.t. 31. 03. 2022)

https://www.bbc.com/news/technology-39947442 (e.t. 31. 03. 2022.)

https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (e.t. 31. 03. 2022)

http://www.pircenter.org/media/content/files/9/13480921870.pdf (e.t. 04.03.2022)

https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/Russia_2000.pdf (e.t. 04.03.2022.)