SİBER UZAY VE ULUSLAR ARASI İLİŞKİLER / TEORİSİ

Müberra ALTINER[*]

Fatma ÇAKIR[**]

Siber Uzay ve Uluslararası İlişkiler/ Teorisi Çalıştayı, Cyber Politik Journal, Orta Doğu Teknik Üniversitesi ve Selçuk Üniversitesi ortaklığı ile 11 Aralık 2017 tarihinde gerçekleştirilmiştir. Çalıştay iki oturumdan oluşmuş, ilk oturumda açılış konuşmasını Prof. Dr. Hüseyin Bağcı yapmıştır. Moderatör, Prof. Dr. Özlem Tür olurken, konuşmacılar ise, Dr. M. Emin Erendor (Çukurova Üniversitesi, Cyber Politik Journal) ve Doç. Dr. Nezir Akyeşilmen (Selçuk Üniversitesi, Cyber Politik Journal)'dir. Konuşmacıların sunum başlıkları ise, sırasıyla, 'Siber Uzayın Temel Kavramları' ve 'Siber Uzay ve Uluslararası İlişkiler/ Politika' dır.

Çalıştayın ikinci oturumunun moderatörlüğü ise Prof. Dr. Bilal Sambur (Yıldırım Beyazıt Üniversitesi, Cyber Politik Journal) tarafından yapılmıştır. Konuşmacılar sırasıyla, 'Siber Uzayın Felsefesi' konulu sunumu ile Prof. Dr. Mustafa Çevik (Ankara Sosyal Bilimler Üniversitesi) ve 'Teknoloji ve Uluslararası İlişkiler Teorisi' adlı sunumu ile Prof. Dr. Davut Ateş (Selçuk Üniversitesi) olmuştur.

'Siber Uzayın Temel Kavramları' adlı sunumunda Dr. M. Emin Erendor'a göre (Çukurova Üniversitesi, Cyber Politik Journal) siber kavramının tek başına bir anlam ifade etmemekte, literatürde yeni olan bu kavram, yanına aldığı eklerle anlamlı hale gelmektedir. Bunun yanında, antik Yunan kökenli bu kelime rehberlik etmek, kontrol etmek anlamları taşımaktadır. Siber kelimesi ilk kez 1958 yılında Louis Couffignal tarafından kullanılmış olmakla beraber, 1984 yılında William Gibson'ın Neuromancer adlı romanında siber uzay kavramını kullanımı ile kavramın kullanımı yaygınlık kazanmıştır. Siber Uzay kavramını tanımlayan Erendor; bilginin elektromanyetik formda oluşturulması ile başlayıp dünyanın dört bir yanını kuşatan çeşitli sistemler vasıtasıyla bilgiye erişimin sağlandığı sanal ortamın bütünü olarak tanımlamaktadır. Ancak bu tanımdan farklı olarak ABD Hava Kuvvetlerinin siber uzayı tanımlarken; ağ sistemleri ve fiziksel yapılar üzerinde veri depolamak, değiştirmek ve geliştirmek amacıyla

[*] Yüksek Lisans Öğrencisi, Selçuk Üniversitesi, İİBF Uluslar arası İlişkiler Bölümü.

[**] Arş. Gör., Selçuk Üniversitesi, İİBF Uluslar arası İlişkiler Bölümü.

elektronik ve elektromanyetik spektrumun kullanılması olarak tanımlama yoluna gittiğini de belirtmiştir.

Erendor, siber suçları siber uzayın bileşeni olan bilişim sistemleri ile bu bileşenlere karşı işlenmiş suçların bütünü olarak tanımlar. İnternete bağlı herhangi bir bilgisayar sisteminin ya da ağının diğer bilgisayar sistem/ağlarına karşı kötü maksatlı eylemler gerçekleştirmek amacıyla kullanılması, klasik suçların yeni teknolojik imkanlar kullanılarak işlenmesi de bu kapsamda değerlendirilmektedir.

Erendor, siber saldırıları; bir web sitesine, bilgisayar sistemine, bilgisayarların gizliliğini, bütünlüğünü, erişilebilirliğini veya içinde depolanan bilgiyi tehlikeye düşüren tek bir bilgisayara (toplu olarak bir bilgisayar) karşı yapılan saldırılar olarak tanımlamıştır. Siber saldırı çeşitlerini sıralayan Erendor; bir bilgisayar sistemine yetkisiz erişim kazanmaya çalışma, hizmetin bozulması veya reddi saldırıları (DDoS), bir web sitesini kesmek, virüs veya kötü amaçlı yazılım yüklemesi, verilerin işlenmesi için bir bilgisayarın yetkisiz kullanımı, bir şirketin çalışanları tarafından bilgisayarların/uygulamaların şirkete zarar verecek biçimde uygunsuz kullanılması örneklerini verir.

Siber terörizm konusunda Erendor; siber uzay ve terörizmin birleşimi şeklinde bir tanımlama yapar, siyasi/sosyal mercilere, kişilere gözdağı verip baskı oluşturmak maksadıyla, resmi birimlerin bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasa dışı tehdit veya zarar verici saldırılar olarak belirtmiştir. Siber terör; ölümcül olan ya da fiziksel hasara yol açan, şiddetli ekonomik kayba neden olan saldırılar olarak örneklendirilebilir.

Siber savaş ise Erendor'a göre, bir devlet tarafından başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yapmak üzere gerçekleştirilen sızma faaliyetleridir. Ayrıca ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar olarak tanımlanabilir.
Siber casusluk; kullanıcısının bilgisi dahilinde olmadan, bireysel kullanıcıların, firmaların, kurum ve kuruluşların bilgilerinin, internet veya internet üzerinden siber taarruz yöntemleri kullanılarak kişisel, askeri ve ekonomik amaçlar için elde edilmesidir.

Siber istihbarat; bir yandan bilgileri toplayıp analiz yaparak, karar vericilerin önünü aydınlatmak şeklinde tanımlanırken bir yandan da karar vericilerin belirlediği politikalar

doğrultusunda, psikolojik harekat, propaganda gibi yöntemler kullanarak toplumların algılarını yönetmek olarak ifade edilebilir.

Siber güvenlik; siber ortamda, devlet, kurum, kuruluş ve bireysel kullanıcılar tarafından güvenlik amaçlı kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik talimatları, klavuzlar, risk yönetim yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi-işlem donanımları, personeli, altyapı ve uygulamaları, hizmetleri, telekomünikasyon sistemleri ve siber ortamda iletilen veya saklanan bilgilerinin tümünü kapsamaktadır.

İlk oturumun ikinci sunumu 'Siber Uzay ve Uluslararası ilişkiler/Politika' konulu sunumu ile Doç. Dr. Nezir Akyeşilmen (Selçuk Üniversitesi, Cyber Politik Journal) tarafından yapılmıştır. Akyeşilmen'in verdiği bilgilere göre, günümüzde; internet kullanıcısı: 3.794 milyarken, ilk web-sitesi-1991 yılında oluşturulmuştur. İlk e-mail: 1971 yılında atılırken bugün günlük olarak 250 milyar e-mail atılmaktadır. Dünyanın en ünlü arama motoru Google'da günlük 5 milyar arama yapılmaktadır. Dünya üzerinde günlük blog yazısı: 5 milyonken, günümüzde toplam facebook kullanıcısı: 2,055 milyara ulaşmış durumdadır. Günlük olarak hacklenen web-sitesi sayısı 90 bini bulurken, dünya üzerinde günlük olarak satılan akıllı telefon sayısı 4 milyonu bulmaktadır. (Kaynakça; http://www.internetlivestats.com/)

Akyeşilmen sunumuna bir soruyla başladı: Siber uzay hayatımızın ne kadarını kapsıyor?
Siber küreselleşme kavramının tanımını yapan Akyeşilmen, küreselleşmenin dünyayı bir köy haline getirdiğini ancak bunun ötesinde siberin dünyayı bir apartman haline getirdiğini ifade etmiştir. Buna göre, artık herkes herkesle komşu, mesafe ve sınırlar ortadan kalkmış durumda. Siber uzay ve politika ilişkisini ifade eden Akyeşilmen, siber güven(siz)lik sorunu ya da siber başarısızlık teknik bir başarısızlık değildir. Politik başarısızlığın sonucudur. Yani fonksiyonel ve stratejik politikaların zayıflığıdır.(Lewis, 2013). Nedeni ise, siyasi ve bürokratik elitin ve karar alıcıların siber uzay konusunda az bilgi sahibi olmalarındandır. Siber güvenlikte en zayıf halka kullanıcıdır, yani bireydir ve bireylerin siber güvenlik konusundaki bilinç ve bilgi düzeyleri düşüktür.

Akyeşilmen, siber uzay ve uluslararası ilişkileri, literatür, çalışmalar ve konular üzerinden ele almıştır. Uluslararası İlişkilerde siber literatür; 2001-2010 tarihleri arasında 26, Uluslararası İlişkiler dergisinde Siber ile ilgili yayımlanan makale sayısı 49'a ulaşmıştır. (Reardon ve

Choucri, 2013). Bugün; Siber Çalışmalar, Oxford Uİ Siber Çalışmalar Programı, Charles Sturt University – Siber Çalışmalar ve Araştırmalar Master Programı, International Hellenic University – İletişim ve Siber Güvenlik YL programı, ABD Deniz Akademisi – Siber Güvenlik Çalışmaları Programı, The Centre for Strategic and International Studies(CSIS) – Güvenlik programı altında -Advanced Cyber Studies bulunurken Avrupa ve Amerika'da birçok üniversitede siber politika dersleri verilmektedir.

Siber Uzay ve Uluslararası İlişkiler/Politikalar noktasında ise Akyeşilmen, siber uzay çalışmalarının inter-disipliner olmakla birlikte sosyal bilimlerde daha çok Uluslararası İlişkiler'in alanına girdiğini ifade etmiştir. Uluslararası ilişkilerin belli başlı kavramları ve siber uzaya bakıldığında, siber uzayın anarşik doğası dikkat çekmekte ve siberin merkezi neresidir? sorusu gündeme gelmektedir. *Yine bu noktada belli başlı konu başlıkları ve bunlara yönelik bir takım soruların cevaplarının verilmesi gerektirmektedir. Bunlar genel manada şu şekilde sıralanabilir: Internet sistemi: Katman modeli: OSI-TCP/IP Modeli – Uİ'de Analiz düzeyi (Chouci ve Clark): Açıklayıcı bir model mi?Anonimlik siber uzayı daha bilinmez, belirsiz ve güvenliksiz kılmaktadır. Siberde kimlik ve güvenlik; Siber Yönetişim Sorunu (2014 Küresel Siber Yönetişim Programı – J. Nye)- Siber Uzayı kim yönetecek? Sorularının yanında Siber Güç - Siber Caydırıcılık var mıdır? Siber Güvenli derken Kimin güvenliğinden bahsediyoruz? Açık Diploması konusunda – diplomatik sızıntılar- Wikileaks ve Snowden olayları örnek teşkil etmektedir. Siber istihbarat: Kimin işidir? Nesnelerin Interneti (IoTs?nedir?; 1,2 milyar araç, 2020'de 40 milyar araç internete bağlanacaktır da bunlar ne kadar güvenlidir? Büyük Veri (Big Data)'den Uluslararası İlişkilerde teori ve analiz nasıl etkilenir? E-ticaret: 10 trilyon $: Küresel bölüşüm ve güç transferine etkisi?*

Aktörler (paydaşlar sistemi), Uluslararası Sınırlar, Egemenlik, Ulusal-Uluslararası Güvenlik, Küresel yönetişim, Dış Politika, Siber Çatışmalar, İnsan Hakları başlıkları da siber alanla birlikte tekrar gündeme gelmektedir. Siber uzayın Westfalyan Uluslararası İlişkiler düzenine etkileri; Yeni uluslararası aktörlerin ortaya çıkması, geleneksel güç ilişkileri değiştirmesi; güç transferini kolaylaştırması bağlamında, yeni tehdit türleri ve yeni ulusal güvenlik boyutu (siber güvenlik) oluşturması, siber çatışmalar; (güvenlikleştirme, kritik altyapılar ve siber istihbarat), siber uzay yönetişiminde özel sektörün gücü, geleneksel uluslararası yönetişim kurumlarının etkisinin siber uzayda az olması, Siber yönetişim için artan işbirliği ihtiyacı ve çabaları – küresel siber normlar sorusunu beraberinde getirmiştir.

Küresel Siber Saldırılar ve Uluslararası İlişkiler bağlamında; Estonya'ya DDoSsaldırları (2007) İsrail-Suriye radar kontrolü (2007), Stuxnet (2010), Wikileaks ve Snowden saldırıları ele alınmıştır.

İkinci oturumun birinci sunumu "Siber Uzayın Felsefesi" başlığıyla Prof.Dr. Mustafa Çevik (Ankara Sosyal Bilimler Üniversitesi) tarafından yapıldı. Siber uzaya felsefi bir yaklaşımla bakan Çevik, sanallık ve gerçeklik kavramlarını tartıştı. Var olma ve koşullarına değinilen tartışmada var olmak için fiziksel dünyada olmak ve üç boyutlu olmanın bir zorunluluk olup olmadığı tartışıldı. Siber uzayın farklı bilim dallarıyla ilişkisi ve gelecekte insan üzerindeki etkileri tartışıldı. Aynı sunumda yapay zeka ve insanlık kavramları da detaylı bir şekilde tartıldı.

İkinci oturumun ikinci sunumu, 'Teknoloji ve Uluslararası İlişkiler Teorisi' başlığı ile Prof. Dr. Davut Ateş (Selçuk Üniversitesi) tarafından yapılmıştır. Konvansiyonel teknoloji ile başlayan Ateş, modern uluslararası ilişkilerin ortaya çıkışında ve evriminde teknolojik gelişmelerin başat rol oynadığını ifade etmiştir. Sanayi devrimi-1 (buharlı makineler ve gemiler)... Denizaşırı taşımacılık ve ticaret...Sanayi devrimi-2 (içten yanmalı motorlar ve elektrik)... Fosil yakıtların ve doğal kaynakların önemi... Daha küçük ve hareketli makineler...Sanayi devrimi-3 (elektronik)... İşlevsel mini makinelerin yaygınlaşması... Uydular…

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Pratik Örnekleri; Savunma sanayi (yeni silahların gelişmesi) Ulusal güvenlik (istihbarat yöntemleri dahil) Uluslararası ticaret ve yatırımlar, Enerji kaynaklarının kontrolü, Ekonomik kalkınma politikaları, İletişim ve haberleşme, Nakliye araçları (deniz, hava, kara, demir), Diplomatik ilişkiler, Uluslararası örgütlenmeler, Yasal düzenlemeler (uluslararası hukuk) olarak belirtilmiştir.
Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Teori Örnekleri; Teknolojik rekabet ve güvenlik (realist yorumlar), Karşılıklı bağımlılık, örgütler (liberal açılımlar), Hegemonya ve yeni sömürgecilik (neo-Marksist yaklaşımlar), Teknoloji / iktidar birliktelikliği, özgürlük özlemi (eleştirel yaklaşımlar), Alternatifleri keşfetme girişimleri (post-yapısal yaklaşımlar), Sosyal değişim ve evrim (konstrüktivistler)oolarak ifade edilmiştir.

Siber teknoloji 4. Sanayi Devriminin unsurlarından biri olarak görülmektedir. 4. Sanayi Devriminin başlıca unsurları: Akıllı makineler (yapay zeka), Üretimde robotların hakim konuma gelmesi, Mikro-çipleşme, İnternet ve siber dünya, İletişim ve nakliyede artan hız, Bilginin birincil sermaye haline gelmesi, İnsan-akıllı makine özdeşliği olarak ifade edilmiştir.

Siber teknoloji, reel hayatın siber ortama aktarılması ve sürdürülmesine yarayan araçlar bütünü olarak tanımlanabilir. Başlıca unsurları: İnternet, Sosyal medya, Bilgi ve iletişim teknolojileri, E-Ticaret, E-Finans, E-Suç olarak belirtilmiştir.

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Pratik Örnekleri; Günümüzde uluslararası alandaki bir kısım pratikler siber alana aktarılmaktadır. Bazı örnekler: Ülkeselliğin dönüşümü (post-territoriality), Siyasal alanın sibere kayması, Siber istihbarat ve siber saldırı, Siber güvenlik (ulusal, kurumsal ve kişisel), Siber savaşlar ve çatışmalar, terörizm, Yeni örgütlenmeler ve sosyal hareketler, E-devlet ve e-vatandaş (sanal devlet-vatandaş), Küresel toplum ve kamuoyu (mahşer), Uluslararası hukukun dönüşümü (siber hukuk) ele alınmıştır.

Konvansiyonel Teknoloji ve Uluslararası İlişkilerde Teori Örnekleri;Siber teknolojiler uluslararası ilişkilere yaklaşımları etkileyecektir sorusunu teoriler üzerinden ele alınmıştır. Realizm; Siber ilişkilerdeki gelişmeler ‘‘realizm’’i realist olarak bırakacak mı yoksa yeni bir tür realizme geçiş mi olacak? Savaş, güvenlik, ulusal çıkar ve güç gibi realist kavramlar siber dünyada nasıl incelenecek?Siber dünya gerçeklikten bir kopuş gibi algılanabileceği için realist perspektif bu konuya yabancı mı kalacak?Soruları cevaplanmıştır.

Liberalizm; Siber dünya bir ‘‘açık pazar ortamı’’ olarak kavramlaştırılabilecek mi? Kompleks karşılıklı bağımlılığın unsurları ve dinamikleri nasıl açığa çıkarılacak? Siber dünyada devlet dışı aktörlerin çoğalması ve etkinliklerinin artması mümkün olacak mı?Önceki dönemde bir seçenek gibi kavramlaştırılan uluslararası örgütlenmeler meselesi siber ilişkiler ağında artık geri döndürülemez bir zorunluluk olur mu?Siber dünya Kantçı idealin gerçeğe dönüşmesine imkan tanıyabilir mi? Soruları yanıtlanmıştır.

Yeni Marksist Yaklaşımlar; Siber dünyada sermaye, emek, artı değer, sömürü, emperyalizm, bağımlılık, dünya sistemi gibi olguların özünde bir kısım değişimler var mı, yoksa yalnızca şekil mi dönüşüyor?Yeni dönemde akıllı makineler insan için çalışacaksa, siber dünya Marksist ideal olan evrensel komünist toplum için bir altyapı teşkil edebilir mi?Sınıflar ve ülkeler arasındaki eşitsizlikler var olmaya devam edecek mi, yoksa siber dünya bunların giderilmesi konusunda bazı fırsatlar sunuyor mu? Uluslararası politik ekonomi? Olarak yanıtlanmıştır.

Konstrüktivizm; Siber dünya kimlik, çıkar ve normların şekillenmesi ve dönüşümü üzerinde nasıl bir etkiye sahip olacak? Uzay çalışmaları önümüzdeki dönemde olası yeni yerleşimler

konvansiyonel uluslararası ilişkileri nasıl etkiyecek?Kimliğin önemli bir unsuru olan dil farklılığının ortadan kalkması kimlik tanımları ve sınırları üzerinde nasıl bir etkide bulunacak? (otomatik simültane tercüme makinelerinin gelişimi)Siber dünya ve teknolojiler yeni değer oluşumlarını hangi yollarla destekleyecek? Olarak ifade edilmiştir.

Yeni Teorik Tartışma Başlıkları; Evrensel veya kozmopolitan toplum olgusu siber teknolojiler sayesinde zorunlu olarak ortaya çıkan yeni bir gerçeklik mi? Siber dünyada sınırlar olacak mı? Yoksa ülkeler arasındaki fiziki sınırlar zaman içerisinde anlamsızlaşacak mı?Savaş ve çatışmalar dahil pek çok iş, üretim ve faaliyet akıllı makineler tarafından yapılacağına göre siber dünyada insan faktörünün yeni rolleri nasıl olacak?Akıllı makineler güvenliğe katkı sağladığı kadar ne tür handikaplar taşımaktadır?Karşılıklı bağımlılığın ve entegrasyonun yoğun olacağı siber alanda devletlerin egemenliği ne ölçüde mutlaklığını koruyabilecek? Yoksa mutlak anarşiden tedrici biçimde bir hiyerarşiye dönüşüm olacak mı, olacaksa hangi yollarla gerçekleşecek? Siber teknolojiler küreselleşme olgusunu yeni bir evreye mi taşıyacak? Teknolojinin gelişimine bağlı olarak savaşlar meydan muharebesi, cephe savaşları, topyekunsavaş şekline dönüşmüştü. Yeni dönemde ne tür savaşlarla karşılaşacağız ve bunların icrasına ilişkin ortak kurallar nasıl belirlenecek? Olarak ifade edilmiştir.

Ontoloji Boyutunda; Bütün bu tartışma başlıkları özelde uluslararası ilişkilerle alakalıymış gibi görünse de, esasında sosyal teoriye ilişkindir. Siyaset, sosyoloji, iktisat, tarih, hukuk, felsefe gibi pek çok sosyal bilim dalı teknolojideki gelişmelere paralel biçimde dönüşen sosyal olguyu anlama, açıklama ve anlamlandırma konusunda yeni yaklaşımlar geliştirme yükümlülüğü altındadır.Bunlar arasında en fazla inter-disipliner özelliğe sahip uluslararası ilişkiler teorisi bu çerçevede kendisini güncelleyebilmek için öteki sosyal bilim dallarına daha fazla dayanmak zorunda kalacaktır. Aynı zamanda sosyal bilim dallarının her biri yeni sosyal gerçekliği açıklama uğraşı içerisinde siber ilişkiler ağı, küresel alan ve kozmopolitan toplum gibi olgulara daha fazla angajeolmak zorunda kalacaktır. Önceki dönemlerde daha özel bir alanmış gibi kavramlaştırılan uluslararası ilişkiler diğer sosyal bilim dallarının bir kesişim noktası haline gelecek, halka açılıp daha fazla şeffaflaşabileceği ifade edilmiştir.

Çalıştay boyunca sunum yapanlar ve katılımcılar siber uzay ve uluslararası ilişkiler disiplini arasındaki ilişkiyi irdelemek, anlamak ve anlamlandırmak için yoğun bir tartışma ve müzakere sürecine girdiler. Disiplinde yeni bir alan olması hasebiyle bağlantılar ve etkileşimleri tartışıldı.