In chapter eleven, the authors explain the importance of setting up a response team to practice different possibility tactics and make efforts to tackle both past and new problems as a preparatory ground work to self-defense. Hackers are said to be fast lesson learners which demand equal measure of response to avoid repeating past mistakes. To be able to complete this task easily more experience needed to be shared among groups of different organizations, states and communities. However, security experts find it problematic in sharing experiences with each other since there is no trust among them. Chapter twelve briefly highlights encryptions as hidden weapon despite the fact that there still "computing power, computing parallel and new computing paradigm" (p, 67) which still threatens them in the virtual world. The competition to encrypt is parallel to arms race where parties employ to outwit the system. No matter the complexity of encryption it cannot be said to be hundred percent safe.

Thus, the final chapters 13 and 14 advocated for two things. First, the need to realize the importance of personal responsibility, by changing out attitude toward the use of the internet. Second, making cyber security the central theme in various organizations and the international community. These fundamental two issues are sure way to staying ahead away from hack risk in an attempt to win the cyber security crisis looming in the foreseeable future.

From the above discussion, it is patent that the book despite its brevity still provides a great insight into future of cyber world. Although much of the discussion was centered on business organization not much of cyber security and state role in the international system is discussed. In fact sates issues which mentioned were specific, general sketches and scattered international incident. However, the nature of conflict among organizations, lack of regulations governing the administration of the internet virtual world if extended into the domain of international politics will produce more chaotic hostility if not the same. As a result, it is palpable to conclude the book is more of handbook to understanding cybersecurity.

'GÜVENLİŞLEŞTİRME'Yİ YENİDEN GÖZDEN GEÇİRMEK: TEORİ VE VAKALAR

Cihan DABAN[*]

[*] Arş. Gör., Selçuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, ,E-mail: dabancihan@gmail.com

Thierry Balzac, Sarah Leonard and Jan Rujicka.(2015). 'Securitization' Revisited: Theory and Cases, Sage Journal, 30(4), pp.494-531.

Makale üç yazar tarafından ele alınmıştır. Bu yazarlar, Thierry Balzacq, Sarah Leonard ve Jan Ruzicka'dır. Balzacq, doktorasını Cambridge Üniversitesi'nden almıştır. Doktora sonrası Harvard'da görev yapan Balzacq, ardından Edinburgh Üniversitesi'nde Onursal Profesörlük görevinde bulunmuştur. Ayrıca Beşeri Bilimler Enstitüsünde Yüksek Öğrenim Çalışmalarında "seçkin araştırma" konusunda görev de yapmıştır. 2015 yılında Diplomasi ve Uluslararası Güvenlikte Seviye 1, Kanada Araştırma Başkanı (yılda 200.000 ABD Doları değerinde) ödülüne layık görülmüştür. Balzacq, güvenlik, güvenlikleştirme teorisi, Uluslararası İlişkiler Teorisi ve Avrupa Birliği politikası üzerine 100'den fazla bildiri yayınlamıştır. 150'den fazla da sunum yapmıştır. Güvenlik üzerine çalışan Balzacq, 2015 yılında yayımlanan "Gözden Geçirilmiş Güvenlikleştirme: Teori ve Vakalar" konulu makalede diğer iki yazarla beraber siber güvenlik konusuna değinmiştir. Diğer yazarlardan Leonard, Birleşik Krallığa bağlı İskoçya Dundee Üniversitesi'nde çalışmaktadır. Yazarın çalışma alanları; dış politika ve güvenlik konularıdır. 2015 yılında Balzacq ile birlikte ele aldığı bu makalede, güvenlik konusunu siberle bağlantılı olarak ele almıştır. Üçüncü yazar olan Ruzicka, 2010 yılında güvenlikleştirme teorisine ilişkin teorik bir eleştiri ile Fransız ve Rus devrimlerinin tarihsel vaka incelemelerini konu alan teziyle doktorasını almıştır. Güvenlik üzerine çalışmalar yapan Ruzicka, öte yandan uluslararası ilişkiler teorisi ve Orta Avrupa bölgesi üzerine de çalışmalar yapmaktadır.

Gözden Geçirilmiş Güvenlikleştirme: Teori ve Vakalar başlıklı makalede en dikkat çekici durum güvenlik algısının siberle bağlantılı olduğu kısımdır. Bu kısım ikinci ana başlıkta ayrıntılı olarak değinilmiştir. Bu kapsamda makale, üç ana başlıktan oluşmaktadır. Birinci ana başlık *Güvenlikleştirmenin Kavramsal Boyutlarıdır*. Bu kısımda, güvenlikle ilgili olarak güç ilişkileri, uygulamalar ve araçlar ele alınmıştır. İkinci ana başlık, *Güvenlikleştirmenin Ampirik ve Teorik Etkileri'*dir. Bu kısımda kimlik ve göç, enerji ve çevre, küresel sağlık, din ve en önemli konulardan biri olan siber güvenlik alanlarına değinilmiştir. Üçüncü ana başlık ise; *Geleceğe Yönelik Kalkınma için Karşılaşılan Zorluklar ve Olası Yöntemler'dir*. Burada ele alınan konular ise, teori ve metodolojidir.

Üç ana başlıkta incelenen makalede ilgi çeken konu, siberden daha eski olan güvenlik konusunun siberle bağlantılı olarak ele alınmış olmasıdır. Güvenlikleştirme üzerine yapılan çalışmalarda, başlangıçta siber denilen bir alan olmadığı için siber alanın öneminden

bahsedilmemiştir. 196'lardan sonra yaygınlaşan internet, beraberinde siber alanı da ortaya çıkarmıştır. O günden bu yana, daha geniş teorik gelişmelere yol açan siber güvenlik ve güvenlikleştirme konusunda önemli çalışmalar yapılmaya başlanmıştır. Bu alanın önemi birbiriyle ilişkili iki eğilimden kaynaklanmaktadır. Birincisi, devletler, toplumlar, işletmeler ve bireyler giderek siber uzayda bulunan veri, sistem ve teknolojilere güvenmiş ve bu, bir dizi aktörün çeşitli tehditleri tanımlayan yeni güvenlikleştirme hareketlerini geliştirmesi için verimli bir zemin sunmuştur. İkincisi, siber güvenlik açıklarıyla meşgul olmaktır. Bu durum Soğuk Savaşın sona ermesinden bu yana güvenlik uzmanları ve bürokrasiler arasında sürmekte olan yeni tehditler ve risklerin araştırılmasına çok uygun bir dönem olmuştur.

Makale, bilgi teknolojilerinin (BT) yalnızca bilgisayarların güvenlik açığı başlangıçlarından beri bilindiği 1990'ların sonlarında güvenlikleştirmeyi incelemiştir. BT'nin güvenlik gündeminin bir parçası haline geldiğini anlamak için, "çerçeveleme" kavramını kullanmıştır. Bu kavramla başarılı bir güvenlikleştirme için kriterleri sunmuştur. Bunu ise yalnızca bir konunun siyasi gündeme yerleştirilmesi ile eşleştirmiştir. Buna ek olarak, BT'nin bir güvenlik sorunu olarak tanımlanmasının, geleneksel güvenlik uzmanlarının ötesine geçen, ayrı politika alanlarından aynı anda ortaya çıktığını da savunmuştur. Eriksson'un çalışması İsveç davasıyla sınırlı kalmıştır. Ancak uluslararası politika yayılımı konusunda daha geniş bir tartışmaya da yer verilmiştir.

Siber uzayın güvenlikleştirilmesi ile ilgili daha yeni çalışmalar Amerika Birleşik Devletleri'nde ortaya çıkmıştır. Bu anlamda makale, üç argüman üzerinde durmuştur. Bunlar; çerçeveleme özellikleri, bağlamsal koşullar ve çerçeveleyici aktörler olarak ileri sürülmüştür. Bu argümanları analizlerine dahil ederek gevenlikleştirme teorisinin ötesine geçmeye çalışmışlardır. 1990'lı yıllarda birçok güvenlikleştirme eylemine rağmen, Bush yönetimi, 2001 yılına kadar "güvenlikleştirme" üzerine çok az sayıda olağanüstü önlem çağrısı yapmıştır. Fakat bu dönemde siber güvenlik ve kritik altyapılar arasında kurulan bağlantı sayesinde, özellikle siber güvenlik alanına daha çok önem vermeye başlandığı görülmüştür. 11 Eylül saldırıları, daha sonra, devletlerarası siber çatışma açısından değil, siber terörizm açısından, siber tehditlerin çerçevesini güçlendiren bir "odaklanma olayı" olarak algılanmıştır. Bu döneme kadar siber tehditlere karşı (alınan istisnai önlemler dışında) çok az önlem alındığı görülmüştür. Bu durum güvenlikleştirme teorisine daha da çok odaklanmasına ve "tehdit politikası yaklaşımının" daha da çok geliştirilmesine olanak vermiştir.

Özetlemek gerekirse makale, ana hatlarıyla güvenlikleştirme teorisini siber güvenlikle bağdaştırmada önemli bir yol izlemiştir. Bu yönüyle literatüre önemli katkılar sunmuştur. Siber güvenlik açısından nasıl bir yol izlenmesi gerektiğini çok ayrıntılara girmeden ve karmaşık bir yöntem izlemeden, ana hatlarıyla ileri sürmüştür. Bu nedenle hem sade bir dil kullanılmış hem de teorik çerçeve iyi analiz edilmiştir. Bu durum okuyucunun makaleyi daha kolay anlamasını sağlamıştır. Öte yandan, güvenlikleştirme teorisi ile siber uzay arasındaki bağlantının incelenmesi, sadece siberle ilgili altyapıların incelenmesiyle değil, aynı zamanda sağlık, çevre, enerji, din, teori, kimlik ve göç gibi diğer alanlarda yapılan araştırmalar üzerinde de durmuştur. Bu yönüyle makale, okuyucuya önemli bilgiler kazandırmaya çalışmıştır/çalışmaktadır.

Notes For Authors / Yazarlar İçin Notlar

We would like to thank you for choosing to submit your paper to *Cyberpolitik*. In order to fasten the process of reviewing and publishing please take try to read and follow these notes in depth, as doing so will ensure your work matches the journal's requirements.