GÜVENLİK BAĞLAMINDA RİSK VE RİSK YÖNETİMİ

Yazarlar: Ahmet KÜÇÜKŞAHİN[*]
İskender Cahit ŞAFAK[**]
Çağdaş DEDEOĞLU[***]

Öz

Güvenlik, 'risk ve tehdit' kavramları üzerinden düşünüldüğünde risk, tehdit ve güvenlik arasında, sarmal bir ilişki mevcuttur ve bu iki kavram söylemde ve yazında, kalıp şeklinde ve sıklıkla kullanılmaktadır. Bu çalışmada, birbirinin ardılı olarak kabul edilen 'risk ve tehdit' kavramlarından, 'risk' ve buna bağlı olarak 'risk yönetimi'nin farklılığı irdelenmiştir.

Risk ve risk yönetimine ilişkin yapılan çalışmaların incelenmesi sonucunda, risk kavramın, 'olasılık' anlamı yerine, 'hedeflerin gerçekleştirilmesinde sorun yaratan olay ve olguların henüz tehdide dönüşmemiş ve yönetilebilir hali' olarak anlaşılması ve kullanılması daha yerinde olacaktır. Bir diğer ifadeyle, bu çalışma, risk kavramını, güvenlik alanında kullanırken, anlam farklılığını vurgulayabilmek için kavramın 'güvenlik riski' olarak ifade edilmesini önermektedir. Türkçede var olan 'sıkıntı' kelimesinin de güvenlik riskiyle karşı karşıya olan karar alıcıların duygu durumuna benzer bir hali çağrıştırdığı görülmektedir.

Güvenlik riskinin yönetimi konusundaki çalışmaların, ilave hukuksal tedbirlere başvurulmadan normal hukuk düzeni içerisinde yapılmasının yeterli olması, güvenlik alanındaki risklerin tehditlerden ayrı değerlendirilmesinin önemini artırmaktadır.

Anahtar Kelimeler: *Güvenlik, risk ve tehdit, güvenlik riski, risk yönetimi, güvenlik risk yönetimi, sıkıntı.*

Risk and Risk Management in the Context of Security

Abstract

When security is associated with "risk and threat", there is a complex relationship among risk, threat and security. These two concepts are frequently used as common phrases in

[*]Harp Akademileri Komutanlığı, Stratejik Araştırmalar Enstitüsü Müdürü, Dr. P. Kur. Alb. E-posta: ahkucuksahin@gmail.com
[**]Harp Akademileri Komutanlığı, Stratejik Araştırmalar Enstitüsü, Uluslararası İlişkiler Yüksek Lisans Öğrencisi, Dz. Ütğm. E-posta: İskendersafak@hotmail.com
[***]Harp Akademileri Komutanlığı, Stratejik Araştırmalar Enstitüsü, Ulusal ve Uluslararası Güvenlik Stratejileri Yüksek Lisans Öğrencisi. E-posta : Ataydede@gmail.com

discourse and literature. In this study, of the notions of 'risk and threat' taken as corollaries, 'risk' and its projection on 'risk management' are analyzed distinctively.

As a result of examining studies on risk and risk management, the concept of "risk" has to be understood and used as "the state of events and phenomena, not yet threats but manageable, that constitute problems in reaching the goals", instead of conceiving of the concept in terms of "probability". In other words, while using the concept of risk within the field of security, this study suggests that term be used to reflect security risk in order to emphasize the distinction in meaning. It is also observed that the word "trouble" can also be associated with something similar to the emotional states of the decision-makers who are faced with security risk.

That the implementation of studies on security risk management through standard legal procedures, without recourse to additional legal precautions, are sufficient adds to the significance of assessing risks apart from threats in the field of security.

Key Words: *Security, risk and threat, security risk, risk management, security risk management, trouble.*

Giriş

Kişi, kurum, sistem veya devlet olsun bireysel ya da kurumsal bilince sahip herhangi bir unsur güvenliğe ihtiyaç duyar. Bu ihtiyaç, var oluşla yani yaşamın devamı ile ilişkilendirilebileceği gibi kazanılan değerlerin korunması veya arttırılması ile de ilişkilendirilebilir. Güvenliğin var oluşa ilişkin olan yönü hiçbir şekilde esneme kabul etmez, buna karşın kazanılan değerlerin korunmasına veya artırılmasına yönelik olan boyutu daha esnek olabilir. Ancak her iki boyutun ortak özelliği uzun vadeli bir tasarım gerektirmesidir. Bu yaklaşımın bir sonucu olarak, varlığa ve değerlere ilişkin olası olumsuz davranışları önceden tespit etme zorunluluğu ortaya çıkmaktadır. Bunun için ileriye yönelik beklentiler, düşünceler ve hedefler büyük önem arz etmektedir. Çünkü bunların gerçekleştirilmesine veya korunmasına yönelik engellerin tespiti ve ikinci aşamada bunların bir vesile ile yönetilmesi veya etkisiz hale getirilmesi önemlidir.

Güvenliği 'risk ve tehdit' kavramları üzerinden yorumladığımızda; risk, tehdit ve güvenlik arasında, sarmal bir ilişkinin olduğu, 'risk ve tehdit' kavramlarının söylemde ve literatürde kalıp şeklinde ve sıklıkla birlikte kullanıldığı (Özkök, 2004; UK Cabinet Office, 2008) görülecektir. Her ikisi de, güvenlik alanı içerisindeki kullanılan

kavramlardır ve aralarında merdivenin basamakları gibi yükselen bir hiyerarşi mevcuttur. Bu hiyerarşik yapı, yönetim bağlamında alınacak olan tedbirlerle doğrudan ilintilidir. İkisi arasındaki fark ortaya konulamadığı takdirde, zaman, para ve nihayetinde refah kaybı olacaktır. Bununla birlikte sorunlara yanlış teşhis ve bunun sonucu olarak yanlış tedavi uygulanacaktır. Çünkü risk ve tehdit bir hastalığa konulan teşhisin adlarıdır. Bu nedenle nelere risk, nelere tehdit denildiğinin ayırımı kritik bir mahiyet kazanmaktadır. Bu çalışmada, birbirinin ardılı olarak kabul edilen 'risk ve tehdit' kavramlarından, 'risk' ve buna bağlı olarak 'risk yönetimi'nin farklılığı irdelenecektir.

Risk ve Risk Yönetimi: Kavramsal İnceleme

Konuya dair şimdiye kadar yapılmış çalışmalar incelendiğinde birbirinden çok farklı alanlarda risk kavramına ve bir yönetim çeşidi olarak risk yönetimine rastlanmasının mümkün olduğu görülecektir. Dolayısıyla; risk ve risk yönetimine dair bir çalışmada, her şeyden önce riskin, birbirinden farklı alanlarda hangi anlamı karşılayacak şekilde kullanıldığının ortaya konulmasının faydalı olacağı değerlendirilmektedir. Bu açıdan, riskle ilişkili çalışmalar, iki şekilde gruplandırılabilir; finans, bankacılık, sigortacılık, istatistik ve doğal afetle mücadele gibi alanlarda yapılmış matematiksel çözümlemelere dayalı çalışmalar ilk grupta sayılabilir (Knight, 1921; Athearn, 1969; Keeley, 1990; Erb, Harvey, ve Viskanta, 1996; Borge, 2001; Mechler, 2004). Toplumsal gelişmeler ışığında, sosyo-kültürel ve psikolojik temelli yaklaşımlara yer veren çalışmalar ile güvenlik çalışmalarını ise ikinci gruba yerleştirmek mümkündür (Giddens, 1991a; Beck & Ritter, 1992; Douglas, 1994; Lupton, 1999). Riski böylesine geniş bir bağlamda görebilmek için incelemeye öncelikle tarihsel açıdan bakmakta fayda görülmektedir.

İnsanoğlu, başına gelen kötü olayların; talih, kader ya da hasımları tarafından yapılan kara büyülerin sonucu olduğu fikrine uzun zaman sadık kalmış, fakat olayların gelişmesinde ve sonuçlanmasında farklı etkenlerin de rol oynadığını gördükçe yeni kavramlar arayışına girmiştir. Bu bilinçlenme hali, olayların derinlemesine analiziyle birlikte, risk kavramıyla tanışma sürecinin doğmasına neden olmuştur (Giddens, 2003). Modernizmin, getirdiği rasyonel düşünme yetisi sonucunda, doğal ve toplumsal olayların belirli bir düzen içinde işlediği ve bu

düzenin, ölçülebilen, hesaplanabilen ya da önceden tahmin edilebilen kurallar çerçevesinde sürdüğü fikri gelişmiştir. (Lupton, 1999) 20'nci yüzyılın ortalarında, bilgisayar teknolojilerindeki gelişmeler sonucu, istatistiksel ve olasılık temelli hesaplamaların da popülerlik kazanmasıyla birlikte, risk çalışmaları finans, sigorta ve bankacılık alanları başta olmak üzere birçok sektörde ön plana çıkmıştır (Inhaber ve Norman, 2006). Küreselleşmenin hızlanmasıyla birlikte, iletişim ve etkileşimdeki sınır aşan hareketlilik, riskin tanımlanması noktasında da kendisini göstermiştir. Risk bu dönemden sonra daha az tanımlanabilen, öte yandan da daha ciddi sonuçlara yol açan ve daha zor yönetilen bir kavram haline gelmiş (Beck, 1992), hatta zamanla tehlike ve tehdit kavramlarının yerine de kullanılır olmuştur (Lupton, 1999, s.12).

Tarihsel süreçte riske dair farklı bakış açılarına rastlanılmasına rağmen, kavramın kullanılışında önemli ortak noktalar dikkat çekmektedir. Riskin, "insanların sahip oldukları değerlerin, insan faaliyetleri veya olayların sonuçları nedeniyle zarar görmesi olasılığı" şeklinde yaygın bir tanımı mevcuttur (Klinke ve Renn, 2002, s.1071). Yine başka bir tanıma göre, belirli bir zaman aralığında belirli bir hedefe ulaşamama ve dolayısıyla zarara uğrama olasılığı olarak tanımlanan riskin en belirgin özellikleri; 'tam ve net olarak bilinememesi, zamanla değişkenlik göstermesi, olumsuz sonuçlar doğurma olasılığına sahip olması ve yönetilebilir olması' şeklinde sıralanabilmektedir (Babuşçu, 2005). Dolayısıyla kişilerin, kurumların, sistemlerin ve devletlerin var oluş nedenlerini ve stratejilerini başarıyla yönetmelerini etkileyecek herhangi bir olayı risk olarak tanımlamak mümkün olacaktır. Bu açıdan bir organizasyon için çeşitli risklerin mevcut olabileceği ve bunların küresel, çevresel, sosyal, kültürel, finansal, uzun ve kısa vadeli, paydaşlardan kaynaklı ya da teknik riskler olarak sınıflandırılabileceği ileri sürülmüştür (Aras ve Crowther, 2009, s.45). Öte yandan doğal afetler üzerine yapılan çalışmalarda da risk bir olasılık olarak kabul edilmekle beraber, doğal afet riskinde olayın kendisinden ziyade gerçekleşmesi sonrası oluşan durum ile ilgilenilmektedir (Ergünay, 1996). Bu türden çalışmalarda farkı yaratan, riskin kaçınılamazlığına yapılan vurgudur.

Risk teriminin kullanımının en yaygın olduğu alan olarak finans sektörü ön plana çıkmaktadır. 2005 yılında, ABD'nin Pennsylvania

eyaletinde düzenlenen finansal risk yönetimi sempozyumunda konuşan IMF eski Baş Ekonomisti Micheal Mussa, finans kurumlarının amacının riskin yönetilebilir kılınması olduğunu ortaya koyarken riskin belirsizlikle olan yakın ilişkisine dikkat çekmiştir (Mussa, 2005). Bu bakış açısında riskin, belirsizliği de kapsayan bir nitelikte olduğu vurgulanmaktadır. Öte yandan, risk ve bilgi ilişkisine tam ters noktadan yaklaşarak karar vericinin matematiksel oranlarla bir olayın gerçekleşme ihtimalinden bahsedebildiği durumların risk, bahsedemediği durumların belirsizlik olarak tanımlandığı çalışmalar da önem arz etmektedir (Knight, 1921). Bu şekilde bir yaklaşımda risk, belirsizlik ile zıt yönlere giden iki ayrı vagon gibidir. Ancak bu iki farklı yaklaşımın da temelinde, bilgi seviyesi bakımından sürecin tamamına hâkim olup olmamak yatmaktadır. Çünkü finansal risk ve bilgi arasında; *bilinen*, *bilinmeyen* ve *bilinmesi imkânsız* hallerden oluşan bir denklem vardır (Mussa, 2005). Her ne kadar bilgi edinme sayesinde belirsizlik seviyesi düşürülebilse de bilinemeyen rastgele durumların olması kaçınılmazdır. Böyle bir durumda belirsizlikler bilgi edinme yoluyla azaltılabilirken, rastgelelikler üzerinde herhangi bir kontrol sağlanması mümkün değildir. (Vose, 2008, s.8) Dolayısıyla finansal sürece ilişkin olarak bilinmesi imkânsız hususlar her zaman mevcut olacağından, riskin sıfırlanmasının mümkün olamayacağı ve hatta bazı durumlarda riski azaltmak üzere bilgiye sahip olmanın maliyetinin riskin neden olacağı zararın maliyetinden daha yüksek olabileceği öne sürülmektedir (Crockett, 2005). Bu kapsamda sürece ilişkin bilinmeyenlerin ya da bilinmesi imkânsızların varlığına rağmen tüm hususlar biliniyormuşçasına hareket etmenin de ayrı bir sorun olduğu görülmektedir.

Finans alanında risk yönetimine bakıldığında ise dikkati çeken önemli bir durum, riskin fırsatla ilişkilendirilmesidir (Kindler, 1998, s.36; Bodine, Pugliese ve Walker, 2001, s.65). Öte yandan, ilgili olduğu alandan bağımsız olarak herhangi bir olayın karakteristiğini belirleyen üç unsur: Olayın gerçekleştiği bir senaryonun varlığı, bu senaryonun gerçekleşme ihtimali ve senaryonun gerçekleştikten sonra mevcut duruma olan etkisidir (Vose, 2008, s.3). Bu üç etmen, risk ve fırsat kavramlarının sahip oldukları ortak özellikler olarak öne çıkar. Bu kullanım, içinde, mevcut durum sonrası ortaya çıkabilecek zarar veya

kazançları barındırması sebebiyle, riskin hem olumsuz hem de olumlu şekilde tanımlandığı bir çerçeve sunar. Bu kapsamda risk ve fırsat arasındaki farkı, sonucun olumlu ya da olumsuz olmasının belirlediği söylenebilir. Dolayısıyla bu bakış açısına göre iyi yönetilen bir risk, fırsata dönüşebilecektir. Riskin olasılık boyutunu öne çıkaran bu tür yaklaşımlara göre bilgi ve maliyet dengesinin kurulması önemli olmakla birlikte belirli bir kayıp da makul karşılanmaktadır. Riskle beraber fırsatın/fırsatların da mevcut olduğundan hareketle, risk – fayda analizi önem arz etmektedir. Ayrıca organizasyonların risk toleransı açısından birbirinden oldukça farklı olabilecekleri göz önünde tutularak her organizasyonun risk analizinin, içeriden bakan bir gözle yapıldığı takdirde daha verimli kılınabileceği düşünülmektedir. Risk – fayda analizinde şartlar ortaya konulduktan sonra süreç; *riskten sakınma, risk transferi, riski hafifletme veya kabullenme* yolu ile yönetilmeye çalışılır (Bodine, Pugliese ve Walker, 2001, s.67). Bu türden bir analiz, riskin alınıp alınmaması üzerine kurulu olması açısından dikkat çekicidir. Dolayısıyla bu tür bir tercih söz konusu olduğunda bazı kişi, kurum ya da örgütler günlük yaşamlarında risk alırken bazıları da riskten kaçınmayı tercih edecektir. Buradan hareketle, bu yöntemle yapılan bir risk - fayda analizinde riskin edilgen bir yapıya büründüğü söylenebilir.

Riski olasılık ile ilişkilendirerek edilgen bir unsur olarak inceleyen anlayışların aksine; riski, harekete geçmiş ya da geçmek üzere olan bir tetikleyici unsur olarak inceleyen bir anlayışın hâkim olduğu doğal afet veya bilgi sistemleri çalışmalarında riskin etken bir yapıda olduğunu söylemek mümkündür. Özellikle bilgi sistemleri çalışmalarında riskin, etken yapısından ötürü, güvenlik riski olarak anıldığı görülmektedir (Adams & Sasse, 1999; Şengonca, Teke, & Karaaslan, 2002; Başbakanlık, 2003) Deprem gibi bir doğal afet söz konusu olduğunda ise riskin gerçekleşmesi engellenememekle birlikte, bir yönetim stratejisi dâhilinde depremden hasar görme olasılığı azaltılarak depremin zarar riskleri yönetilmiş olmaktadır. Böyle bir durumda depremin olma olasılığı konusunda bir değişiklik yoktur (Barka ve Er, 2002). Doğal afetlerle ilgili çalışmalarda ve bilgi sistemleri yönetiminde kabul gören türden risklerin yönetilmesindeki farklılaşmanın bir benzeri proje risklerinin yönetilmesinde de göze çarpar. Bir risk unsuru projeye zarar vermeden önce potansiyel

problemlerin tanımlanması, ortaya çıkabilecekleri alanların belirlenmesi ve bahse konu sorunların yok edilmesine dayalı risk yönetim modeli (Wiegers, 2007), olma olasılığı değiştirilemeyen ya da artık gerçekleşmeye başladığından dolayı geriye doğru işletilemeyen süreçlerin sonuçları açısından yönetilebilmesine dayanmaktadır.

Risk ve risk yönetimine ilişkin yapılan çalışmaların incelenmesi sonucunda, risk kavramına yaklaşımda bir bütünlük bulunmadığı değerlendirmesi yapılabilir. Bu durumun güvenlik çalışmaları alanında yarattığı karmaşa ve buna yönelik çözüm önerisi bir sonraki bölümde ele alınacaktır.

Risk ve Güvenlik Riski

Literatürde yapılan incelemeler göstermiştir ki zararın gerçekleşme sıklığı ve yarattığı sıkıntı farklı boyutlarda olmakla birlikte kullanıldığı tüm alanlarda risk, bir şekilde olasılık ile ilişkilendirilmektedir. Bu olasılığın yönetilmesine gelindiğinde; finans ve bankacılık gibi alanlarda, olasılığın kabul edilebileceği limitlere göre bir analiz yöntemi belirlenmekte; doğal afet yönetimi gibi olasılığa müdahale edilemeyen alanlarda ise riskin gerçekleşmesi durumunda oluşacak zararların önüne geçilmesi şeklinde tedbirler alınmaktadır. Bilişim teknolojisinde kullanılan risk kavramı ise, 'olasılık' anlamı yerine, 'olay ve olguların henüz tehdide dönüşmemiş ve yönetilebilir haline' daha yakın bir anlamda kullanılmaktadır. Bu yüzden, finansal risk modellerinden farklı olarak, olası bir kötü durumdan çok yönetilmediğinde tehdide dönüşecek bir olgu olarak karşımıza çıkmaktadır.

Finansal analizlerde, riskler açıkça ortaya konulabilirken, uluslararası ilişkilerde hâkim olan belirsizlik yüzünden lineer bir yöntem belirlenmesi imkansız olmaktadır. Çünkü ekonometride kullanılan zaman cetvellerinin aksine, güvenlik riskinde herhangi bir olay dizisi arasında standart zaman aralıkları mevcut değildir. Ortaya çıkan iki olay arasında çok uzun süreler olabilirken, aynı günde birden fazla olay da meydana gelebilmektedir (Schrodt, 1997). Ekonomide, fiyatlardaki ufak bir oynamanın arz-talep dengesindeki etkisi rahatlıkla anlaşılabilirken, siyasi olaylarda bir önceki durumun müteakip haller üzerinde çok daha büyük etkisi olabilmektedir (Schrodt, 1997).

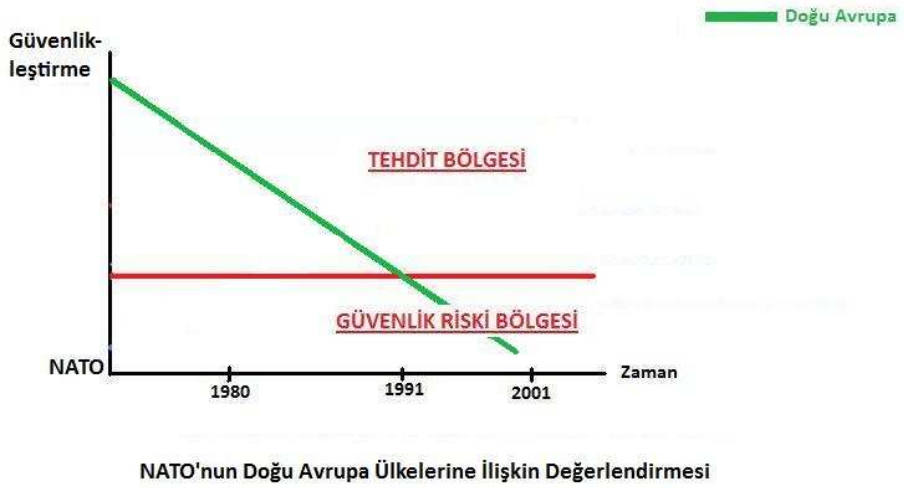
Literatürdeki risk yönetimi değerlendirmeleri; riski almak, ondan kaçınmak ya da zararını telafi etmek üzerinden yapılırken, güvenlik riski, alınan ya da kendisinden kaçınılan bir olgu olmadığı gibi önlem alınamadığı takdirde vereceği zararın telafisi de mümkün olmayabilir. Dolayısıyla olasılık hesabının kabul edilemez olduğu hayati konularda ve toplumsal sonuçlar doğuracak olaylar noktasında, riskin yönetilmesi farklı bir boyutta değerlendirilmelidir. Bir olayın risk ya da tehdit olarak değerlendirilmesi esnasında, güvenlik bağlamında kast edilen risk; olasılıklı bir zarara uğrama hali midir, yoksa tehditle özdeş bir başka anlama mı vurgu yapılmaktadır? Olasılık bağlamındaki riske ilişkin yaklaşım, güvenliğin varlığa yönelik olan kısmına uyarlandığında, varlığın risk taşıması, yaşamın olasılıklar üzerine kurulması anlamına gelecektir. Yani hayat; belirsizlik, şüphe, korku, gerilim, güvensizlik ve kısaca kumar demek olacaktır. Riskin tanımı böyle kabul edildiğinde ise hayatın, güvenlik mantığı üzerine oturtulması gerekecektir. Dolayısıyla yönetimsel açıdan risk ile tehdit arasında var olması gereken hiyerarşik durum ortadan kalkacak ve riskin koşulları, tehdidin koşullarından daha ağır hale gelecektir. Çünkü tehdit bilinenler üzerinden bir yönetimi gerekli kılarken risk bilinmeyenleri de içereceğinden daha sıkı önlemlere gereksinim duyulacaktır.

Bir başka yaklaşımla, güvenliğin, varlığa ve değerlere yönelik olmak üzere iki boyutu dikkate alındığında riske yüklenen anlam farklılaşmaktadır. Güvenliğin değerlere yönelik olan boyutunda, risk 'zarara uğrama tehlikesi' olarak kabul edilebilir. Bu tehlike gerçekleştiği takdirde söz konusu değer zarar görmüş olur. Belki de tamamen yok olabilir. Aynı yaklaşım varlığa yönelik olarak düşünüldüğünde riskin gerçekleşmesi durumunda varlık ya zarar görecek veya tamamen yok olacaktır. Risk, riski kabul eden kişi, olgu veya olayın varlığını tamamen ortadan kaldırma boyutuna ulaşmışsa onun yönetilebilirliğinden söz etmek mümkün görülmemektedir. O, artık tehdit olmuş demektir. Bu durumda, yönetimden ziyade mücadeleden söz etmek gerekecektir.

Yukarıda değinilen hususlar ışığında herhangi bir unsurun varlığı ve sahip olduğu değerlerin korunmasına yönelik bir güvenlik ilişkisinde riskin olasılık olma halinden çıkarılıp güvenlikleştirilmesinde bilginin önemli bir faktör olduğu değerlendirilmektedir. İstihbarat olarak da nitelendirilebilecek bu bilgi, kendisine ulaşan kişinin algısında

değişikliklere yol açacak ve konu üzerindeki ilgiyi artıracaktır. Dolayısıyla bilgi, algı ve güvenlik arasında doğrudan bir ilişki olduğu söylenebilir. Bu noktada belirtilmesi gereken husus, bilginin içeriğinin ne olduğudur. Edinilen fazla bilginin ve bu bilginin yanlış değerlendirilmesinin, mevcut ortamda aşırı güvenlikleştirme yaratarak ortamı daha da yaşanmaz hale getireceği açıktır. Bu yüzden zaman içinde işlenerek, işlevsel hale getirilmiş bir bilginin, algıyı doğru yönlendirebilecek bilgi türü olduğu değerlendirilmektedir.

Bu kapsamda, istihbaratın önemi ortaya çıkmaktadır. Günümüz çok boyutlu risk ve tehdit ortamında (Büyükanıt, 2003) ülkeler bir yandan doğru risk ve tehdit tanımlarını yapmak bir yandan da halkı risklerin yönetimi noktasında ikna etmek durumundadırlar. Karar alıcı mekanizmalardan birisi olan hükümetlerin, halk desteğiyle göreve geldikleri düşünüldüğünde, kamuoyu desteğinin izlenen politikalarda ne kadar önemli bir unsur olduğu görülecektir. Tehdidin belirlenmesine yönelik "6 soru" prensibi günümüz çok boyutlu risk ve tehdit ortamında işletilemediğinden karar vericilerin işi zorlaşmakta ve istihbaratın önemi ortaya çıkmaktadır. Bu kapsamda, yetersiz istihbaratın, güvenlik riskinin yönetilememesine ve tehdide dönüşmesine neden olabileceği söylenebilir. 2001 yılında ABD'de gerçekleştirilen saldırıların ardından yapılan araştırmalar (Zegart, 2005, s.78; Betts, 2007, s.587), bu tür bir saldırı riskinin bilindiğini fakat bu riskin iyi yönetilmediği için bir tehdide ve sonrasında da gerçek bir saldırıya dönüştüğünü ortaya çıkarmıştır. Böylelikle zamanında yönetilmeyen güvenlik riski yüzünden hem tehdide maruz kalınmış hem de sonrasında aşırı güvenlikleştirme kapsamında alınan tedbirler ve uygulanan risk yönetimi usulleriyle halkın refahı düşmüş, insanlar güvenlik kontrollerine boğulmuşlardır (Beck, 2002).



Şekil 1. NATO'nun Doğu Avrupa Ülkelerine İlişkin Değerlendirmesi

Şekil-1'de de görüldüğü gibi Soğuk Savaş boyunca NATO tarafından bir tehdit unsuru olarak görülen Doğu Avrupa, Sovyetler Birliği'nin dağılması ve sonrasında gelen Avrupa Birliği genişleme süreciyle birlikte artık güvenlik riski seviyesine indirgenmiştir (Ağır, 2004). Bu indirgemenin işlevsel bilginin yardımıyla gerçekleştirilmiş olması oldukça önemlidir. Öte yandan, öncesinde risk olarak dahi kabul edilmeyen bazı durumların, gerçekleşen birtakım olaylar sonucunda tehdit halini alabileceği de göz önünde bulundurulmalıdır. Örneğin; 2001 yılı olayları, mevzu odaklı bir yaklaşımla incelendiğinde ortaya çıkan risk, bir terör saldırısıyla karşı karşıya kalma riskidir. Denilebilir ki, bu türden bir risk, edinilen istihbaratlar sonucunda güvenlik riski vasfını kazanmış, yani bir olasılıktan etken bir duruma geçmiştir. Yeterli güvenlik algısının oluşmaması sonucunda bahse konu terör riskinin olasılık boyutunda kabul görmeye devam etmesi, bir ara yönetim söz konusu olmadığından, saldırılar sonucu aniden tehdide dönüşmüştür.

Risk ve Algı

Risk, gerçeklerle algıların kesiştiği yerde kabul gören bir kavram olarak tanımlandığında, bilgi kavramının yanında anılması gereken bir diğer kavramın da algı olduğu ortaya çıkmaktadır. Gerçek, tek ve değiştirilemez olmasına rağmen, gerçeğin algısı, sahip olunan bilgiyle orantılı olarak kişiden kişiye değişebilmektedir. Bu yüzden risk algısı,

kavramın incelenmeye başlandığı zamanlardan bu yana öznel bir unsur olarak kabul edilmiştir. Bu öznellik, güvenliğe ihtiyaç duyan birimlerin münhasır durumlarından kaynaklanmakta ve algıda seçicilik olarak ifade edilebilmektedir. Örneğin; suyun kirlenmesi çevreciler için risk unsuru iken ekonomik kalkınmacılar için aynı durum söz konusu olmayabilmektedir. Buradan hareketle algıda seçicilik yaklaşımını bilgi, kişilik, ekonomi gibi farklı göstergelere dayanarak analiz eden yaklaşımlar mevcuttur (Wildavsky ve Dave, 1990). Fakat mevcut bir riskin bilinmemesi, meydana gelebilecek olası zarar ve hasarları engelleyemeyeceği gibi ortadan da kaldıramayacaktır (Gebizlioğlu, ty, s.2).

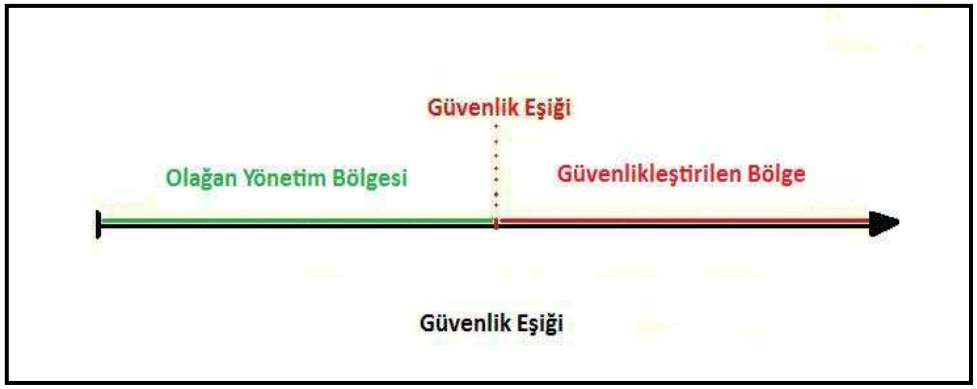
Risk, modern bir kavram olmasının yanında (Beck, 2002), kapsamının ne olacağı konusu, etkilemesi muhtemel toplumun ve devletin risk algısıyla alakalıdır. Yani hiçbir şey kendi kendine risk değildir. Tehlikenin nasıl analiz edildiği, olayın nasıl algılandığı riskin çerçevesini belirleyen temel unsurdur (Campbell, 1992, s.1-2). Ortada herhangi bir risk yokken dahi, söylem ve algı bazında böyle bir riskin olduğuna inanılması, o riskin var olduğu kanısını toplumda yerleştirebilir (Cebeci, 2007). Örneğin ülkelerin risk portföylerinin; siyasi ve toplumsal bağlamda yapılan değer analizleri, ilgi alanı seçimleri gibi kamuoyunu ilgilendiren siyasi söylemler doğrultusunda oluşturulmasının (Ericson, 2006, s.345) bir örneği olarak, ABD askeri politikasının belirlenmesi noktasında uygulanan yöntem dikkat çekicidir. Buna göre, ABD Genelkurmay Başkanı tarafından kongreye sunulan önceden oluşturulmuş risk tanımlamaları, ABD askeri politikasını belirlemekte, fakat bu risk belirlemeleri sayısal verilere göre değil, kamuoyunda ve siyasi karar mekanizmalarında oluşan genel fikirler doğrultusunda gerçekleştirilmektedir (Johnson, ty, s.1). Bu değerlendirmeler ışığında risk algısının oluşum sürecinin analizi güvenlik riskinin yönetilmesi noktasında önemlidir.

Bu noktada akla gelen soru, algının nasıl oluşturulması gerektiğidir. Zira güvenlikleştirme aşamalarında yaşanan sıkıntıların çoğu, çeşitli düzeydeki kullanıcı ve yöneticilerin risk algılarını gerekenden düşük seviyede tutmalarından kaynaklanmaktadır (Straub ve Welke, 1998, s.442). Dolayısıyla güvenlik riskinin algılanması sürecinde, bilginin edinilmesi kadar, bu bilginin doğru aktarılması da

önem kazanmaktadır. Bilginin doğru aktarılması mevcut durumun berraklaşmasını sağlayacağından algıyı doğru yöne kaydırmanın yanı sıra olaylar arasında ilişkilendirmeye de olanak sağlayacaktır. Bu kapsamda algısal ilişkilendirmeyi yapması gereken, güvenlikten doğrudan etkilenen birim olurken; bilgi aktarımını yapması gereken ise güvenliği sağlayacak olan aktör olmalıdır. Bilgi aktarımında bir diğer önemli nokta ise, taraflar arasındaki iletişimin duygusal olarak da yeterli düzeyde olması gerekliliğidir. Zira, güvenlik, güvende olma olarak tanımlandığında, bir kişi ya da sistemin güvenilirliğine itimatla doğru orantılı bir hal almaktadır (Giddens, 1991b, s.39). Bu itimat sağlandığı sürece, kişi varoluşsal endişesini ya da korkusunu yenecek ve kendini güvende hissedecektir. Böylece kural koyucu ve uygulayıcı arasında itimada dayalı modern bir yönetim modelinin işletilmesi sağlanacaktır (Giddens, 1991b, s.94). Fakat özellikle iletişim olanaklarının azami seviyeye ulaştığı günümüz dünyasında, kitleler, medya ve internet vasıtasıyla ciddi propagandalara maruz kaldıklarından, güvenlik risklerinin belirlenmesinde kamuoyu algısının tek kıstas olarak kabul edilmesinin de hatalı sonuçlara yol açabileceği göz önünde bulundurulmalıdır.

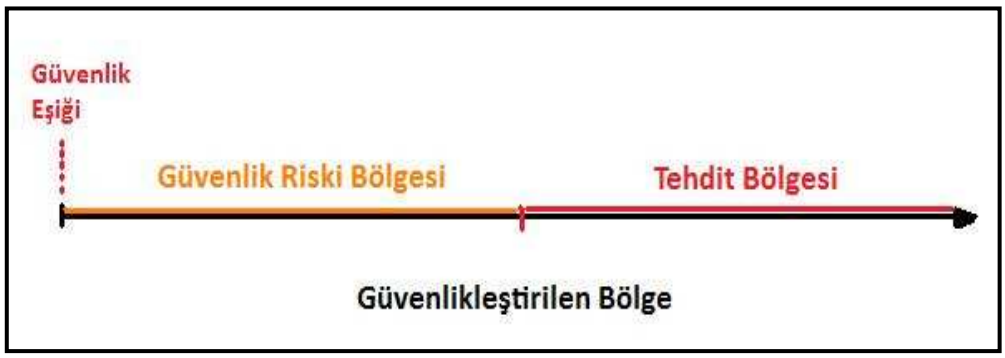
Güvende olma veya güvenlik içinde olma, enerjinin boşa harcanmamasını ve refaha daha fazla vakit ayrılmasını gerektirir. Ancak, bu ideal dileğin gerçekleşmesi sıfır olasılıklıdır. Daha işin başlangıcında yani hangi konuların güvenlik konusu olacağı noktasında ayrım başlamaktadır. Farklılığın sebepleri arasında, yaşanan ortamın hafızalarda bıraktığı izler, geçmişteki hatıralar, kişilik özellikleri vb. birer etkendir. Belki de başlangıçtaki anlaşmazlık, bir olayın hangi tahammül sınırından sonra bir güvenlik sorunu olarak kabul edileceği noktasındadır. Bu tahammül sınırı değişkendir ve güvenlik eşiği olarak kabul edilebilir. Sırf bu yüzden dahi güvenlik konuları için bir standart oluşturmak mümkün değildir.

Güvenlik Eşiği, Güvenlik Riski ve Tehdit İlişkisi



Şekil 2. Güvenlik eşiği

Güvenlik eşiği, beliren olumsuz bir olay veya olgu için tahammül gösterilebilecek son seviyedir (Şekil 2). Bu seviye geçildikten sonra olay güvenlikleştirilerek alınan önlemler sayesinde güvenlik eşiğinin altına yani katlanabilir seviyenin altına düşürülmesine çalışılır. Bir başka ifade ile bir olayın güvenlikleştirilmesinden kasıt, tahammül edilemeyecek seviyeye gelen olay veya olgunun tekrardan tahammül edilebilir bir seviyeye getirilmesini sağlamaktır. Güvenlikleştirilen konular, bünyenin gücü oranında iki kategoriye ayrılır. Bunlardan birincisi güvenlik riski ikincisi tehdittir (Şekil 3). Söz konusu olay veya olgu, tarafımızdan yönlendirilebilir durumda ise güvenlik riski; yönlendirilemez durumda ise ve tedbir alınmayı gerektiriyorsa tehdit aşamasında olduğu kabul edilir.



Şekil 3. Güvenlik riski ve tehdit.

Güvenlik riski aşamasının, tehdit aşamasına göre daha hafif koşulları içermesi gerekir. Her şeyden önce, güvenlik riski aşaması, normal hukuk kuralları içerisinde yürütülürken, tehdit aşaması, ilave hukuksal kararların ve tedbirlerin alınmasını gerektirir. Örneğin, Yunanistan'ın Ege Denizi'nde karasularını 6 deniz milinden 12 deniz miline çıkarması durumunda, Türkiye Büyük Millet Meclisi, 08 Haziran 1995 tarihinde, Türkiye Cumhuriyeti Hükümetine, askeri bakımdan gerekli görülecek olanlar da dahil olmak üzere tüm yetkilerin verilmesi kararını almıştır. Yunanistan'ın, Deniz Hukuku Sözleşmesinin açık denizler ve okyanuslar için belirlenmiş bazı hükümlerinden yararlanarak karasularını 12 deniz miline çıkarma isteği ile başlayan güvenlik riski, bir tehdit haline gelince TBMM karar almıştır. Bir başka örnek, PKK terörüne ilişkin çıkartılan ilave kanunlar ve kanun hükmündeki kararnameler olabilir. PKK terörüne karşı alınan önlemler yeterli olmadığı için olağan dışı hukuk tedbirleri alınarak terörle mücadele, tehdit bölgesine taşınmıştır. Oysa güvenlik riskinin yönetimi için böyle ilave bir hukuka ihtiyaç duyulmayacaktır.

Hangi konuların tehdit, hangi konuların güvenlik riski olacağına yönetimi elinde bulunduranlar, yönetimin imkân ve kabiliyetlerini dikkate alarak karar verirler. Bir olay veya olgunun güvenlik riski mi yoksa tehdit mi olacağı, güvenlik riski veya tehdidi oluşturan unsurlar ile yönetimin kazandığı yeni kabiliyetlerin mukayeseli olarak değerlendirilmesi neticesinde belirlenebilir. Varılan sonuca göre tehdit ise, gerekli tedbir alınır, risk ise, yönetilmeye devam edilir. Bu noktada,

bu tespiti ve ayırımı sürekli olarak yapacak, hafızası güçlü bir mekanizmaya ihtiyaç olacaktır.

Bu mekanizmalar, tehdit veya güvenlik riski oluşturan konuları yaşadıkları ortamda bulacaklardır. Sivil toplum kuruluşlarının çalışmaları, medyanın dikkat çektiği konular, üniversite araştırmaları, devletin kurum ve kuruluşlarının elde ettiği sonuçlar ile diğer ülkelerde cereyan eden olaylar birer ipucu oluşturabilecek konuların başında gelecektir. Bu ortam içerisinde kurul tarafından tespit edilen hassas (güvenlik riski ve tehdit olabilecek) konular icra organına arz edilerek, burada güvenlik riski veya tehdit olarak belirlenmesi sağlanacaktır. Mekanizma, icra organının, güvenlik riski olarak kabul ettiği hususları yönetmek üzere kendi sorumluluğuna alacak, buna karşın tehdit olarak belirlediklerini karar organına havale ederek orada görüşülmesini sağlayacak ve gerekli tedbirleri almak üzere güvenlik kurumlarına, görevler şeklinde yöneltecektir.

Güvenlik Riski Yönetimi

Güvenlik risk yönetimi için öncelikle belirlenen hedeflerin gerçekleştirilmesini geciktiren veya buna engel olan sorunların tespit edilmesi ve bu sorunların yönetilebilir olup olmadığının değerlendirilmesi gerekir. "Risk yönetimi" kavramı, riskin yönetilebilir olmasından çıkmıştır. Buna mukabil tehdit, müdahale gerektirdiğinden "tehdit yönetimi" kavramı mevcut değildir. Eğer söz konusu sorun yönetilebilir durumda ise, güvenlik riski olarak nitelendirilir ve yönetim safhasına geçilir. Bu aşamada yönetilecek olan güvenlik riski için risk yönetim stratejisi belirlenir ve stratejinin uygulanmasına (riskin yönetilmesine) geçilir.

Güvenlik riskleri beş aşamada belirlenir (Küçükşahin, 2007, s. 62):

Birinci aşama, kişi, kurum veya devletlerin hedefleri noktasında kendisini ilgilendiren her türlü olayın nedenleri açısından irdelenmesi ve söz konusu nedenlerden kendilerine yönelik çıkarımlar yapabilmesinin sağlanması aşamasıdır. Bu aşamada dikkat edilmesi gereken nokta; güvenlik veya güvenliğe konu olan olaylar - sosyal nitelikte oldukları için - gerçekleştikleri ortamlar ayırt edilmeksizin, sebep ve sonuç ilişkileri içerisinde değerlendirilmeleri gerektiğidir.

İkinci aşama, kişi, kurum veya devletlerin sahip olduğu özelliklerin ve gücün ortaya konulması ile ilgilidir. Bu kendini bilmek anlamında değerlendirilebilir. Sun Tzu, Harp Sanatı adlı eserinde; *"Eğer düşmanını ve kendini iyi tanıyorsan, yapacağın yüzlerce muharebenin sonucundan korkmana neden yoktur. Eğer kendini tanıyor fakat düşman hakkında gerekli bilgilerden noksan isen, sonuçta galip gelsen de birçok defa mağlubiyeti tadacaksın. Ama ne kendini ne de düşmanı iyi tanımıyorsan her muharebede bozgun akıbetin olacaktır"* (Tzu, Çev: Gilles, 2007) demektedir.

Üçüncü aşama, mevcut güce dayanarak sınırların belirlenmesidir. Her şeyden önce, tasarlanan hedefler, belirli alanlarla sınırlıdır. Çünkü hedef ile oluşturulacak güç arasında orantısal bir ilinti vardır. Bu nedenle, güvenliği tasarlarken hedefin ve gücün sınırlarını önceden tespit etmek gerekir. Söz konusu sınırlar sistemin sahip olduğu gücün nitelik ve niceliğine göre değişiklik gösterebilmektedirler. Dolayısıyla gücü elinde bulunduranlar kullanma iradelerine bağlı olarak sınırlarını belirlemelidirler. Ancak burada dikkatten kaçırılmaması gereken bir husus, bu sınırların değişken olduğu, gücün büyüklüğüne paralel olarak güç arttıkça genişleme, güç azaldıkça daralma eğilimi göstermesidir. Dolayısıyla, sisteme hükmedenler, gücü kullanma iradelerini de ortaya koyarak sınırlarını kendileri belirlemek durumundadırlar. Çünkü oluşturulacak politikaların en önemli unsuru güçtür.

Dördüncü aşamada, kişi, kurum veya devletlerin ana hedefine ulaşmayı destekleyen kısa ve orta vadeli hedefler ön plana çıkmaktadır. Belirlenen bu hedeflere ulaşma yolunda tehditlere karşı alınması gereken tedbirler, ancak gerekli gücü elinde bulunduran aktörler tarafından alınabilir. Söz konusu birimlerin hedefleri doğrultusunda – bünye kişi dışında bir aktör ise- iş bölümü üzerinden güvenliğin tesis edilmesi önemlidir.

Son aşama olan güvenlik riski ve tehditlerin belirlenmesi aşamasında, kişi, kurum veya devletlerin hedeflerine ulaşmasını engelleyen unsurlar arasında yönetilebilir durumda olanların (risklerin) ele alınması gerekmektedir. Gücü elinde bulunduran birimler, önceki aşamalarda ortaya konulmuş olan sınırlılıklar içerisinde, belirlenmiş hedeflere ulaşmayı engelleyen her bir unsuru ortaya koymalıdır.

Yukarıda ifade edilen yöntemle güvenlik riski olarak belirlenen olgular için bir yönetim stratejisi belirlenir. Belirlenen güvenlik riskinin yönetilmesi stratejisinde, ulaşılması/gerçekleştirilmesi gereken hedef veya hedefler sürekli göz önünde bulundurularak milli gücün, güvenlik riskini oluşturan unsurlara karşı nasıl kullanılacağı dikkate alınır.

Belirlenen risk ve tehditlerin sürekli takip edilmesi gerekir. Tehditler, varlığa zarar verme noktasına geldiklerinde mutlaka müdahalede bulunulur; güvenlik riskleri ise yönetilemez duruma geldiklerinde tehdit kategorisine yükseltilerek varlığa zarar vermemeleri için tedbirler alınır. Riskin varlığa veya değerlere zarar vermesini önlemek ve bir noktada yok olmasını sağlayabilmek için, belirlenmesinden tehdit düzeyine çıkmasına veya yok olmasına kadar geçecek sürede yönetilmesi gerekir. Bu süre içerisinde yapılan işleme "güvenlik risk yönetimi" veya daha kısa olarak güvenlik alanında "risk yönetimi" denir.

Sonuç olarak, güvenlik riskinin yönetimi; yukarıda izah edildiği gibi, ilave güç gerektirmez, ancak ilave önlemler mevcut hukuk kurallarının içerisinde alınır, takip ve kontrol için ilave bir teşkilat kurulabilir veya kurulmayabilir. Güvenlik riskinin tehdide dönüşmemesi için mevcut hukuk içerisinde her türlü önlemin alınmasına ihtiyaç duyulmaktadır. Riskin tehdide dönüşmesi durumunda kriz yönetimi anlayışı devreye sokulabilir ve ilave hukuksal kararlar alınabilir. Ayrıca, milli güç unsurlarının etkin şekilde devreye sokularak kullanılmasını da gerektirebilir.

Riskin yarattığı psikolojik durum, Türkçe'de kullanılan sıkıntı kelimesiyle de izah edilebilir. Günlük yaşamda kullanıldığı haliyle sıkıntı, gerginlik ve endişe yaratan geçici bir durumu ifade eder veya öyle kabul edilir. Bir müddet sonra aşılacağı yönünde yaygın bir anlayış vardır. Ancak bazen bu anlayışın tersine sıkıntı büyüyerek arzu edilmeyen noktalara kadar varabilir. Sıkıntı bazen kendiliğinden, bazen de sıkıntının kaynağı/kaynaklarının olağan koşullar içerisinde ortadan kaldırılması yoluyla aşılır. Ancak sıkıntı yaratan olay veya olgunun üzerine güç tatbik edilmez. Fakat sıkıntı, var olduğu süre içerisinde sürekli maruz kalanı tedirgin ve rahatsız eder. Güvenlik bağlamında kullanılan risk kavramı ve sıkıntı kelimesinin anlam olarak birbirlerine

yakın olmaları nedeniyle güvenlik çalışmalarında, risk terimi yerine sıkıntı kelimesinin kullanılabileceği değerlendirilmektedir.

Sonuç

Güvenlikle ilgili konuların algılarla ilgili olduğu, algının ise içgüdü, yaşanan ortamın hafızalarda bıraktığı izler, geçmişteki hatıralar, kişilik özellikleri ile ilintili olduğu söylenebilir. Bu nedenle bir olayın hangi tahammül sınırından sonra bir güvenlik sorunu olarak kabul edilebileceği değişkendir. Çünkü, güvenlik riski göreceli bir kavramdır.

Hangi konuların tehdit, hangi konuların güvenlik riski olacağına, yönetimi elinde bulunduranlar, yönetimin imkân ve kabiliyetlerini dikkate alarak karar verirler. Bir olay veya olgunun güvenlik riski mi yoksa tehdit mi olacağı, güvenlik riski veya tehdidi oluşturan unsurlar ile yönetimin kazandığı yeni kabiliyetlerin mukayeseli olarak değerlendirilmesi neticesinde belirlenebilir. Varılan sonuca göre tehdit ise, gerekli tedbir alınır, risk ise, yönetilmeye devam edilir. Bu noktada, bu tespiti ve ayırımı sürekli olarak yapacak, hafızası güçlü bir mekanizmaya ihtiyaç olacaktır.

Güvenlik riski aşaması, tehdit aşamasına göre daha hafif koşulları içerir. Her şeyden önce, güvenlik riski aşaması, normal hukuk kuralları içerisinde yürütülür ve ilave bir hukuka ihtiyaç duyulmaz. Tehdit aşaması, ilave hukuksal kararların ve tedbirlerin alınmasını gerektirir.

Tehdit veya güvenlik riski oluşturan konular yaşanılan ortam içerisinde bulacaklardır. Sivil toplum kuruluşlarının çalışmaları, medyanın dikkat çektiği konular, üniversite araştırmaları, devletin kurum ve kuruluşlarının elde ettiği sonuçlar ile diğer ülkelerde cereyan eden olaylar birer ipucu oluşturabilecek konuların başında gelecektir. Bu ortam içerisinde kurul tarafından tespit edilen hassas (güvenlik riski ve tehdit olabilecek) konular icra organına arz edilerek, burada güvenlik riski veya tehdit olarak belirlenmesi sağlanacaktır. Mekanizma, icra organının, güvenlik riski olarak kabul ettiği hususları yönetmek üzere kendi sorumluluğuna alacak, buna karşın tehdit olarak belirlediklerini karar organına havale ederek orada görüşülmesini sağlayacak ve gerekli tedbirleri almak üzere güvenlik kurumlarına, görevler şeklinde yöneltecektir.

Belirlenen risk ve tehditlerin sürekli takip edilmesi gerekir. Tehdit, varlığa zarar verme noktasına geldiklerinde mutlaka müdahalede bulunulur; güvenlik riski ise yönetilemez duruma geldiğinde tehdit kategorisine yükseltilerek varlığa zarar vermemesi için tedbirler alınır. Riskin varlığa veya değerlere zarar vermesini önlemek ve bir noktada yok olmasını sağlayabilmek için, belirlenmesinden tehdit düzeyine çıkmasına veya yok olmasına kadar geçecek sürede yönetilmesi gerekir. Bu süre içerisinde yapılan işleme "güvenlik risk yönetimi" veya daha kısa olarak güvenlik alanında "risk yönetimi" denir.

Güvenlik riskinin yönetimi; yukarıda izah edildiği gibi, ilave güç gerektirmez, ancak ilave önlemler mevcut hukuk kurallarının içerisinde alınır, takip ve kontrol için ilave bir teşkilat kurulabilir veya kurulmayabilinir. Güvenlik riskinin tehdide dönüşmemesi için mevcut hukuk içerisinde her türlü önlemin alınmasına ihtiyaç gösterir. Riskin tehdide dönüşmesi durumunda kriz yönetimi anlayışı devreye sokulabilir ve ilave hukuksal kararlar alınabilir. Milli güç unsurlarının etkin şekilde devreye sokulmasını da gerektirir.

Daha sağlıklı bir yapılanmaya gidilebilmesi ve güvenlik risk yönetiminin daha etkin bir şekilde yapılabilmesi için güvenlik riski kavramının 'olasılık' anlamı yerine, 'hedeflerin gerçekleştirilmesinde sorun yaratan olay ve olguların henüz tehdide dönüşmemiş ve yönetilebilir hali' olarak yazında yerini almasının uygun olacağı değerlendirilmektedir. Bu nedenle risk olarak kullanılan kavramın, güvenlik bağlamında kullanılmasında anlam farklılığını vurgulayabilmek için 'güvenlik riski' olarak ifade edilmesinin amaca hizmet edeceği değerlendirilmektedir. Türkçe'de var olan 'sıkıntı' kelimesinin de aynı vurguyu yaptığı söylenebilir.

Bu kavramdan hareketle güvenlik risk yönetiminin de, normal hukuk düzeni içerisinde yapılmasının, ilave hukuksal tedbire başvurulmamasının ve ancak konu üzerine yoğunlaşılmasının yeterli olacağı değerlendirilmektedir.

Summary

When security is associated with "risk and threat", there is a complex relationship among risk, threat and security. These two concepts are frequently used as common phrases in discourse and literature. In this study, of the notions of 'risk and threat' taken as corollaries, 'risk' and its projection on 'risk management' are analyzed distinctively.

Upon evaluating the studies on risk and risk management, it is understood that there is no unity in the approaches to 'risk'. Among scholars, the studies regarding risk are classified in two groups: While the fields of study like finance, banking, insurance, statistics, and combating natural disasters based on mathematical calculations of probability can be considered under the first group; in the light of the social developments, the studies based on socio-cultural and psychological approaches and security studies can be perceived within second group.

When the security studies are evaluated, it is noticed that the meaning attached to the concept of risk resembles that which corresponds to the concept of risk perceived in finance, banking, insurance, and statistics. However, the similarity or distinction in the use of the term affects the structure of security and risk management directly.

Being secure or being in security is essential with regard not to waste energy and allocate more time for prosperity. About deciding on matters of which are to become security matters; traces that the atmosphere leaves, memories of the past, personal attributes etc. are the factors. It is one of the most important aspects for any issue that after which tolerance limit it will be accepted as threat. This tolerance limit is changeable, and it can be accepted as security threshold. Merely because of this, it is not possible to create any standard for security matters.

Security threshold is the last level to endure any negative issue or fact. After this last level is exceeded, the issue is tried to pull down under the security threshold through securitization with the help of precautions. In other words, it is aimed to bring again any issue or fact that can not be tolerated to a level that is tolerable. The securitized

matters can be separated into two categories, depending on the power of actor. First one is security risk and second one is threat. If the issue or fact is manageable, it is accepted as security risk; but if unmanageable and needs to take precaution, it is accepted as threat.

For healthier and more efficient risk management structuring in the field of security, this concept has to be understood and used as "the state of events and phenomena, not yet threats but manageable, that constitute problems in reaching the goals," instead of conceiving of the concept in terms of "probability". In other words, while using the concept of risk within the field of security, this study suggests that term be used to reflect *security risk* in order to emphasize the distinction in meaning. It is also observed that the word "trouble" can also be associated with something similar to the emotional states of the decision-makers who are faced with security risk.

Administrators decide on which matter is to be threat and which is to be security risk according to the facility and capabilities. Any issue or fact can be accepted as security risk or threat, with a comparatively analysis of aspects that create security risk or threat and new capabilities that the administrator gains. If the result is threat, then the necessary precaution is taken; but if it is risk, the issue or fact is continued to manage.

Security risk stage has to have more slight conditions compared to threat stage. In the first place, while security risk stage is managed through standard legal procedures, the threat stage needs to recourse additional legal decisions and precautions. This legal approach adds to the significance of assessing risks apart from threats in the field of security.

Security risks are determined in five stages:

- First stage is the stage in which the reasons creating any issues related to person, establishment or state, taking its targets into account, are analyzed and some conclusions can be reached for these bodies.

- Second stage is about manifesting the attributes and power that the person, establishment or state has.

- Third stage is the stage of deciding on the limits depending on the current power.

- Fourth stage is the stage of determining short-term and long-term targets to reach person's, establishment's or state's main target.

- The last stage of determining security risk and threats is about evaluating the manageable ones among the elements which prevents the person, establishment or state from reaching its targets.

This study also suggests that a center for security risk management be established based on the size of events or phenomena taken as security risks.

Kaynakça

Ağır, B. S. (2004). Soğuk Savaş Sonrası Avrupa Güvenlik Düzenine Kurumsal Bir Bakış. D. K. Kasım, & Z. A. Bakan içinde, *Uluslararası Güvenlik Sorunları.* Ankara: Avrasya Stratejik Araştırmalar Merkezi Yayınları.

Adams, A., & Sasse, M. A. (1999). Users Are Not The Enemy. *Communications Of The ACM* , 41-46.

Aras, G., & Crowther, D. (2009). *The Durable Corporation: Strategies for Sustainable Development.* Aldershot: Gower Publishing .

Athearn, J. L. (1969). *Risk and Insurance.* New York : Appleton-Century-Crofts.

Babuşçu, Ş. (2005). *Basel II Düzenlemeleri Çerçevesinde Bankalarda Risk Yönetimi.* İstanbul: Akademi Consulting & Training.

Barka, A., & Er, A. (2002). *Depremini Bekleyen Şehir İstanbul.* İstanbul: Om Yayınevi.

Başbakanlık. (2003). *Bilgi Sistem ve Ağları İçin Güvenlik Kültür.* Ankara: Başbakanlık.

Beck, U. (1992). *Risk Society: Towards A New Modernity.* (M. Ritter, Çev.) Londra; Newbury Park, Calif.: Sage Publications.

Beck, U. (2002). The Silence Of Words and Political Dynamics in The World Risk Society. *Logos* , 1-18.

Betts, R. K. (2007, Ağustos). Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD. *Political Science Quarterly* , s. 585-606.

Bodine, S. W., Pugliese, A., & Walker, P. L. (2001). A Road Map to Risk Management. *Journay of Accountancy , 192* (6), 65-70.

Borge, D. (2001). *The Book of Risk.* New York: John Wiley & Sons Inc.

Campbell, D. (1992). *Writing Security.* Minnesota: Union of Minnesota Press.

Cebeci, M. (2007). Tehdit Algılamasında Yapısal ve Konjonktürel Nitelikler/İthal Tehditler. *Türkiye'ye Yönelik Risk ve Tehditler* (s.33-42). istanbul: Harp Akademileri Komutanlığı.

Crockett, A. (2005). *Financial Risk Management in Practice: The Known, The Unknown and The Unknowable.* Pennsylvania: The Wharton School.

Douglas, M. (1994). *Risk and Blame: Essays in Cultural Theory.* Londra: Routledge.

Erb, C. B., Harvey, C. R., & Viskanta, T. E. (1996). Plitical Risk, Economic Risk, and Financial Risk. *Financial Analysts Journal* , 29-46.

Ergünay, O. (1996). *Afet Yönetimi Nedir? Nasıl Olmalıdır?* Ankara: Tübitak.

Ericson, R. V. (2006). Ten Uncertainties of Risk Management Approaches to Security. *Canadian Journal of Ciriminology and Criminal Justice* , 345-357.

Gebizlioğlu, Ö. L. (ty). *Risk Yönetimi.* Ankara: SATEM.

Giddens, A. (1991). *Modernity and Self-identity: Self and Society in the Late Modern Age.* Stanford: Stanford University Press.

Giddens, A. (2003). *Runaway World: How Globalization is Reshaping Our Lives.* London: Taylor&Francis.

Giddens, A. (1991). *The Consequences of Modernity.* Stanford: Stanford University Press.

Inhaber, H., & Norman, S. (2006). The Increase in Risk Interest. *Risk Analysis* , 119-120.

Johnson, C. W. (tarih yok). *The Paradoxes of Military Risk Assessment.* Nisan 17, 2009 tarihinde University of Glasgow, Department of Computing Science: http://www.dcs.gla.ac.uk/~johnson/papers/Military_Risk/Short_Military_Risk_Assessment_CJohnson.pdf adresinden alındı

Jorion, P. (2000). *Value at Risk: The Benchmark for Controlling Market Risk.* Auckland: Mc Graw-Hill Professional.

Keeley, M. C. (1990, December). Deposit Insurance, Risk, and Market Power in Banking. *The American Economic Review* , s. 1183-1200.

Kindler, H. S. (1998). The art of prudent risk taking. *Training & Development , 52* (4), 32-35.

Klinke, A., & Renn, O. (2002). A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies. *Risk Analysis* , 1071 - 1094.

Knight, F. H. (1921). *Risk, Uncertainty and Profit.* London: LSE.

Küçükşahin, A. (2007). Türkiye'nin Tehdit Belirleme Yöntemi ve Güvenlik Anlayışı Çerçevesinde Düşman Kavramının Değerlendirilmesi. *Türkiye'ye Yönelik Dış Kaynaklı Risk ve Tehditler* (s. 43-73). İstanbul: Harp Akademileri Basımevi.

Lupton, D. (1999). *Risk and Sociocultural Theory: New Directions and Perspectives.* Cambridge: Cambridge University Press.

Mechler, R. (2004). *Natural Disaster Risk Management and Financing Disaster Losses in Developing Countries.* Karlsruhe: Verlag Versicherungswirtsch.

Mussa, M. (2005). *Financial Risk Management in Practice: The Known, The Unknown and The Unknowable.* Pennsylvania: The Wharton School.

Özkök, H. (2004, Ekim 04). *Genelkurmay Başkanının Harp Akademilerinin Yeni Eğitim Öğretim Yılı Açılış Töreninde Yaptığı Konuşma.* Nisan 20, 2009 tarihinde: http://www.tsk.tr/10_ARSIV/10_1_Basin_

Yayin_Faaliyetleri/10_1_7_Konusmalar/2004/harpakademileriacilis_041004.html adresinden alındı

Schrodt, P. A. (1997). Early Warning of conflict in Southern Lebanon using Hidden Markov Models. *Annual Meeting-1997* (s. 1-46). Washington, DC: American Political Science Association.

Straub, D. W., & Welke, R. J. (1998). Coping With System Risks: Security Planning Models for Managemant Decision Making. *MIS Quarterly* , 441-469.

Şengonca, H., Teke, A., & Karaaslan, E. (2002). *Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması.* Nisan 15, 2009 tarihinde Ulakbim: http://csirt.ulakbim.gov.tr/dokumanlar/BilgisayarAglarindaGuvenlikPolitikalarininUygulanmasi.pdf adresinden alındı.

TBMM. (1995, Haziran 08). Genel Kurul Tutanağı. 21 Mayıs 2009 tarihinde www.tbmm.gov.tr/develop/owa/Tutanak_B_SD.birleşim_başlangic?PAGE1=1... adresinden alındı.

TBMM. 27 Ekim 1983 tarih ve 2935 sayılı Olağanüstü Hal Kanunu.

TBMM. 14 Temmuz 1987 tarih ve 285 sayılı Olağanüstü Hal Bölge Valiliği İhdası Hakkında Kanun Hükmünde Kararname.

TBMM. 16 Aralık 1990 tarihli Olağanüstü Hal Bölge Valiliği ve Olağanüstü Halin Devamı Süresince Alınacak İlave Tedbirler Hakkında Kanun Hükmünde Kararname.

TBMM. 12 Nisan 1991 tarih ve 3713 sayılı Terörle Mücadele Kanunu.

Tzu, S., & Gilles, Ç. (2007). *The Art Of War.* Edinburgh: Ullysseys Press.

UK Cabinet Office. (2008). *The National Security Strategy of the United Kingdom: Security in an Interdependent World.* Londra: The Stationary Office Limited.

Vose, D. (2008). *Risk analysis: a Quantitive Guide.* San Fransisco: John Wiley and Sons.

Wiegers, K. E. (2007). *Practical Project Initiation: A Handbook with Tools.* California: Microsoft Press.

Wildavsky, A., & Dave, K. (1990). Theories of Risk Perception: Who Fears What and Why? *Daedalus* , 41-59.

Zegart, A. B. (2005, Güz). September 11 and The Adaptation Failure of U.S. Intelligence Agencies. *İnternational Security* , s. 78-111.