# Internet Güvenliği Konusunda Yönetici Görüşleri: Bir Ankara Örneği

**Özet:** Günümüzde Internet hayatımızın vazgeçilmez bir öğesi olup çıkmıştır. Böylesi önemli bir yapının güvenliğini sağlamak veya güvenliği konusunda bilgi sahibi olmak herkes için önem taşımaktadır. Bu durum farklı bir konumda karar verici rolünü üstlenen bireyler için daha da önem taşımaktadır. Çünkü bir yönetici hem kişisel Internet güvenliğinden hem beraberinde çalışan bireylerin Internet güvenliğinden, hem de genel olarak çalıştığı kurumun bilgilerinin korunması adına Internet güvenliğinden sorumlu olacaktır. Bu çalışma Ankara ili içerisinden seçilmiş, karar verme yetkisine sahip 12 genç yöneticinin (3 kadın, 9 erkek) Internet güvenliği hakkında görüşlerini içermektedir. Uygun örnekleme yöntemiyle seçilmiş ve gönüllü olarak çalışmaya katılmış olan bu genç yöneticilerin görüşleri anket üzerinden toplanmıştır. Çalışmanın sonuçlarına göre yöneticiler Internet'i daha çok eposta, alışveriş ve sosyal medya olarak kullanmaktadır. Yöneticiler yüksek oranda Internet'ten film ve müzik indirmekte bir sakınca görmediklerini belirtmektedir. Yöneticiler, Internet güvenlik problemlerinin en önemli nedeninin kurum içi politikalardaki zayıflıklar olduğu noktasında hemfikirdir. Ayrıca, Internet'in problemlerinden birisi olarak Internet üzerindeki özel bilgilerin korunmasındaki yetersizlikleri belirtmektedirler. Yöneticiler, Internet'in var olan yapısının sabotaja ve suiistimale açık olduğunu ve bu yapının özellikle e-ticaret konusunda önemli bir sorun olduğunu belirtmektedir. Yöneticiler Internet'in en önemli güvenlik açığının ağ dinleme ve şifre tabanlı saldırılar olduğunu belirtmişlerdir. Buna bir çözüm olarak ise Internet güvenliği sağlama açısından Authentication (Kimlik kontrolü), Access controls (Erişim kontrolleri) ve Encryption (Şifreleme) tekniklerini önermektedirler.

**Anahtar Sözcükler**: Internet Güvenliği, Bilgi Güvenliği, Internet Güvenlik Açıkları, Internet Güvenliğini Sağlama, Yönetici Görüşleri

**The Perspectives of Managers on Internet Security: A Case from Ankara**

**Abstract:** Today, the Internet is getting an indispensable element to our life. It is really crucial for everyone both to secure a structure having an importance like that and to have knowledge about its security. This situation is more essential for the people who take a decision-making role with different positions because a manager is a charge of both personal and the colleagues' security of the Internet, and also institution's security of the Internet to protect information of the institution. This study involves the opinions of the 12 young managers (3 female and 9 male) selected from the Ankara and having a decision making authority regarding the security of the Internet. The opinions of the managers selected with convenience sampling strategy and participating voluntarily to the study survey. According to the results, managers use the internet mainly for the e-mail, the shopping, and the social media. Managers see no harm to download a movie and music from the Internet. They are in agreement with each other about one of the reasons of the security of the Internet is weaknesses in any institution's politics. Moreover, inadequacies of the private information's protection over the Internet are considered as one of the problems of the Internet. Managers state that the Internet's current structure is open to the sabotage and the misuse, and this structure is also a significant problem for the e-business. They note that the most important security gaps over the Internet are lurking in the network and crypto based attacks. As a solution to this problem, authentication, access controls and encryption techniques are offered by them to provide security of the Internet.

**Keywords:** Internet Security, Information Security, Internet Security Tools, Providing Internet Security, Manager Perspectives

## 1. Giriş

Internet'in önlenemez yükselişi, Internet'in olumlu ve olumsuz yönlerini tartışmamıza yol açmıştır [10]. Her an iletişimde kalabilme, her an istediğimiz her bilgiye erişebilme ve bunun gibi birçok avantajı ile Internet hayatımızda önemli bir yer elde etmiştir. Uzun süre faydaları üzerinde konuştuğumuz Internet'in süreç içerisinde yaşattığı olumsuz çıktılar, başta bireyler olmak üzere, bilim adamlarının ve teknoloji

geliştiricilerinin dikkatini Internet güvenliği konusuna çekmiştir [4,6]. Günümüzde Internet'in kendisine yapılan yatırım kadar, Internet üzerindeki bilgilerin gizliliği ve güvenliği konusuna da yatırım yapılmaktadır. Bu nedenle günümüzde Internet'in güvenliği konusu bir hayli önem kazanmıştır.

Internet güvenliği konusu her ne kadar sadece Bilgi ve İletişim Teknolojileri alanını ilgilendiriyor gibi görünse de Internet güvenliği ekonomi, politika, eğitim ve etik gibi birçok bilim dalını da ilgilendirmektedir [7]. Bu konunun en son örneklerinden birisi olarak WikiLeaks belgeleri (http://wikileaks.org/) gösterilebilir. Ortaya çıkarılan bilgilerin gerçekliği bir yana, neden olduğu politik sorunlar (Wikileaks kurucusu Julian Assange için Ekvator'un verdiği sığınma hakkı gibi) etkisini hala göstermektedir.

Yapılan istatistikler, Internet üzerinden işlenen suçların her geçen gün arttığını ve bu nedenle de Internet güvenliğinin hiç olmadığı kadar önem kazandığını açıkça ortaya çıkarmaktadır [10]. Bu nedenle en başta devletler üstü organizasyonlarda (Avrupa Birliği, Avrupa Konseyi gibi) ve daha sonra devletler düzeyinde gerekli yasal önlemler alınmaya başlamıştır [11]. Ülkemizde de güvenlik birimleri içerisinde bilişim suçları dairesi bünyesinde suçları tespit ve önleme adına çalışmalar yapılmaktadır. Maalesef, birçok durumda siber suçları kimlerin işlediğini de bulabilmek mümkün olmamaktadır [1].

Bu süreç içerisinde önemli görevlerden birisi de özel ya da kamu kuruluşların yöneticilerine düşmektedir. Bulundukları konum itibariyle hem bireysel olarak hem de kurumsal olarak Internet güvenliği noktasında bilgi sahibi olmak zorunda olan bu yöneticilerin, Internet güvenliği noktasında sergileyecekleri duruş, gün geçtikçe daha da önem kazanmaktadır.

Yapılan çalışmalar göstermektedir ki, Internet kullanımında ve Internet'e karşı oluşan tutumda kişisel değer yargıları oldukça önemli bir yer tutmaktadır [8]. Bu nedenle kurum yöneticilerinin oluşturacağı ve yöneteceği Internet güvenliği politikalarının tespiti güvenliğin sağlanması adına oldukça önem taşımaktadır. Ayrıca geleceğe yönelik tahminler göstermektedir ki, Bilgi ve İletişim Teknolojilerinin kullanıldığı her alanda görev alacak yöneticilerin güvenlik konusunda bilgili ve hassas olmaları gerekecektir [3].

Yöneticilerin Internet üzerindeki duruşları, diğer bir ifade ile çevrimiçi kimlikleri, güvenlik konusundaki duruşlarını da doğrudan etkileyecektir. Çevrimiçi kimliklerini yönetme işi gönüllü ve gizlilik arttırıcı olmalıdır. Bu sayede hem kendilerinin hem de kurumlarının güvenliğini sağlama noktasında başarılı olacaklardır [6, 9]. Günümüzde ortaya çıkan bazı güvenlik açıklarının sadece basit ve tahmin edilebilir şifreler yüzünden olduğu düşünülürse, Internet güvenlik sistemlerinde hızlı bir değişim yaşanmasının gerekliliği ortaya çıkmıştır [5].

Internet güvenliği konusunda ortaya çıkan açıkların büyük bir kısmı kaynak yetersizliklerinden ortaya çıkmaktadır [10]. Her ne kadar Internet güvenliğini sağlamak noktasında birçok yazılım kullanılsa da halen güvenlik açıkları ve sorunları tamamen halledilebilmiş değildir [11]. Gelecekte yapay zekânın ortaya çıkaracağı daha fazla Internet güvenliği sorunu oluşacaktır. Ortaya çıkacak olan bu siber sorunlar bizleri siber savaşlara kadar götürebilme kapasitesine sahip olacaktır [8]. Bu siber suçların ya da savaşların nedenleri, siyasi muhalefet, hoşnutsuzluk ya da protesto, azınlık hakları ve bağımsızlık hareketleri, dini inanç, kültürel değerler, ya da tarihsel iddiaları hakkını içerebileceği ön görülmektedir[4].

## 2. Yöntem

### 2.1. Örneklem

Bu çalışmanın örneklemi Ankara ili merkezinde farklı kurumlarda çalışan 12 (11 özel, 1 kamu kuruluşu) yöneticiden (3 kadın, 9 erkek) oluşmaktadır. Yöneticilerin yaşları 23 ve 32 arasında değişmektedir. Yöneticilerin hepsi bilgi ve iletişim teknolojileri alanında, en az 1.5 en fazla 10 yıllık görev yapmaktadır. Yöneticilerle bire bir görüşülerek anketi doldurmaları istenmiştir. Çalışmada uygun örnekleme yöntemi kullanılmıştır [2].

### 2.2. Veri Toplama Aracı

Araştırmacı alanyazın üzerinde yer alan anketlerden, daha önceki araştırmalardan ve sonuçlarından yararlanarak bir anket geliştirmiştir. Hazırladığı anketi iki farklı konu alan uzmanına göstererek görüşlerini almış ve ankete son halini vermiştir. Anket ilk başta yöneticilerin temel demografik bilgilerini toplamaktadır. Bu kısım içerisinde Internet kullanımına yönelik sorular da yer almaktadır. Daha sonra 41 farklı madde ile yöneticilerin Internet

güvenliği konusunda görüşleri 1 (kesinlikle katılmıyorum) - 5 (kesinlikle katılıyorum) arasında Likert ölçeğiyle toplanmıştır. Daha sonra verilen beş Internet güvenliği açıklarını en az önemliden en çok önemliye doğru sıralamaları istenmiştir. Son olarak Internet güvenliğini sağlama tekniklerini en az önemliden en çok önemliye doğru sıralamaları istenmiştir.

### 2.3. Verilerin Analizi

Çalışmanın verileri SPSS 17.0 istatistik paket programı kullanılarak analiz edilmiştir. Betimsel istatistik verileri kullanılarak, frekanslar, minimum ve maksimum değerler, ortalamalar ve standart sapmalar hesaplanmıştır.

## 3. Bulgular

### 3.1. Genel Internet Kullanım Bilgileri

Tablo 1'den görülebileceği gibi yöneticiler Internet'i daha çok eposta, alışveriş, sosyal medya ve sohbet amaçlı olarak kullanmaktadır. Bunun yanı sıra yöneticilere hiç hackerlik ve crackerlık yapıp yapmadıkları da sorulmuştur. Yöneticilerin iki tanesi daha önce hackleme yaptıklarını, 4 kişisi ise crack yaptıklarını söylemiştir.

**Tablo 1. Yöneticilerin Internet Kullanım Amaçları**

| Amaç | n |
|---|---|
| Flört | 2 |
| Üniversite ile ilgili | 3 |
| Oyun oynamak | 5 |
| Vakit geçirmek | 6 |
| İş aramak | 6 |
| Finansal işlemler | 9 |
| Sohbet | 9 |
| Sosyal medya | 11 |
| Alışveriş | 11 |
| E-posta | 11 |

### 3.2. Internet Güvenliği Görüşleri

Yöneticiler kendilerine verilen 41 soruya kesinlikle katılmıyorum – kesinlikle katılıyorum Likert ölçeğinde 1-5 arası puanlama yapmışlardır (Tablo 2). Tablodan en dikkat çekici sonuçlardan bir tanesi genç yöneticilerinin Internet üzerinden müzik (X=4.75) veya film (X=4.66) indirme konusunda hiçbir sakınca görmemeleri noktasında neredeyse tamamen hemfikir olmalarıdır. Internet kullanmanın riskinin yüksek olması noktasında kararsız (X=2.75) bir duruş sergileyen yöneticiler, web sitelerden yayınlanan uyuşturucu ve cinsellik içeren öğeler konusunda endişeli olduklarını belirtmişlerdir (X=3.83).

Internet güvenliği noktasında problemlerin en önemli nedeninin kurumların kendi içerisindeki politikalarında oluşan zayıflıklar olduğu yorumuna yöneticilerin katıldıkları görülmüştür (X=3.83). Bu problemlerin tanımlanması noktasında sorulan Internet üzerindeki bilgilerin korunmasında yetersiz kalınmasına ise yöneticiler yüksek oranda katılmışlardır (X=4.27). Bu durumların daha üzerinde yer alan yasal düzenlemeler noktasında sorulan hukuki sınırlamaların Internet'in özgürlük durumunu kısıtlayacağı noktasında yöneticiler kararsız kalmışlardır (X=3.08).

Yöneticilere teknolojinin zayıflığının nedeni olarak yazılım (X=2.66, SS=1.49) ya da donanım (X=2.41, S=1.37) ürünlerinin yetersizliği sorulduğunda bu yoruma katılmama eğiliminde oldukları görülmektedir. Burada elde edilen standart sapmalara bakıldığında tüm diğer maddeler içerisinde en yüksek değerlere sahip oldukları söylenebilir. Bu durumda katılımcıların bu maddeler üzerinde farklı görüşleri olduğu söylenebilir.

Genç yöneticilere sorulan en önemli Internet güvenlik kontrolünün ne olduğu sorusuna ise katılımcılar, bilgisayar (X=4.16), veri iletişimi (X=3.75), donanım

(X=3.08), personel (X=2.83) ve yönetici (X=2.75) kontrolleri olduklarını belirtmişlerdir.

**Tablo 2. Internet Güvenliği Anket Maddeleri**

| Anket Maddesi | X | SS. |
|---|---|---|
| 1. Internet'ten müzik indirip dinlemekte sakınca **görmüyorum.** | 4.75 | 0.45 |
| 2. Internet'ten film indirip izlemekte sakınca **görmüyorum.** | 4.66 | 0.49 |
| 3. Eğer bir zararı olmayacaksa birisinin bilgisayarına girmekte sakınca **görmüyorum.** | 1.91 | 1.37 |
| 4. İzin almadan birisinin e-postalarını okumakta sakınca **görmüyorum.** | 1.41 | 0.99 |
| 5. İzin almadan birisinin şifresini kullanmakta sakınca **görmüyorum.** | 1.50 | 1.00 |
| 6. Birisinin kredi kartının kullanarak Internet üzerinden alışveriş yapmakta sakınca **görmüyorum.** | 1.41 | 0.90 |
| 7. Internet üzerindeki verilerin hepsine erişim serbest olmalıdır. | 2.00 | 1.34 |
| 8. Cracker kötü niyetli bir insandır. | 3.83 | 1.58 |
| 9. Hacker kötü niyetli bir insandır. | 4.25 | 1.21 |
| 10. Internet'in yapısı sabotaja ve suiistimale açıktır. | 4.16 | 1.11 |
| 11. Internet üzerindeki diğer kullanıcıların belirsizliği beni korkutur. | 2.91 | 1.24 |
| 12. Web sitelerden yayınlanan uyuşturucu ve cinsellik içeren öğeler beni endişelendirmektedir. | 3.83 | 0.93 |
| 13. Internet kullanmanın riski yüksektir. | 2.75 | 1.35 |
| 14. Kurum içerisinde kullanıcı adı ve şifre verme kurallarını düzenlemek amacıyla bir kılavuz olmalıdır. | 4.27 | 0.46 |
| 15. Internet güvenlik problemlerinin en önemli nedeni kurum içi politikalardaki zayıflıklardır. | 3.83 | 1.02 |
| 16. Internet güvenlik problemlerinin en önemli nedeni Internet'in kendi yapısındaki mevcut risklerdir. | 3.41 | 0.99 |
| 17. Internet güvenlik problemlerinin en önemli nedeni kullanılan teknolojilerin sahip oldukları zayıflıklardır. | 3.41 | 1.16 |
| 18. Internet güvenlik problemlerinin en önemli nedeni yetkisiz erişimlerdir. | 3.91 | 0.79 |
| 19. Internet'in en önemli güvenlik problemi yanlış yönlendirmelerdir (misrouting). | 3.91 | 0.90 |
| 20. Internet'in en önemli güvenlik problemi veri iletimindeki başarısızlıklardır. | 3.83 | 1.11 |
| 21. Internet'in en önemli güvenlik problemi veri bozulmalarından kaynaklanan kayıplardır. | 3.83 | 0.83 |
| 22. Internet güvenlik problemlerinin en önemli nedeni yasal yetersizliklerdir. | 4.25 | 1.13 |
| 23. Internet güvenliği elektronik ticaretin en önemli **sorunudur.** | 4.41 | 0.51 |
| 24. Internet üzerindeki verilerin telif haklarının korunması için yasalar **olmalıdır.** | 4.66 | 0.49 |
| 25. Yasalar Internet ortamının kullanımı ile ilgili olarak yeniden düzenlenmelidir. | 4.50 | 0.67 |
| 26. Internet üzerinden işlenen bilişim suçları için özel bir mahkeme oluşturulmalıdır. | 4.33 | 1.15 |
| 27. Yasal sınırlamalar Internet'in özgürlük potansiyelini tehdit etmektedir. | 3.08 | 1.24 |
| 28. Firmalar Internet'in ciddi bir avantaj sağladığının farkındadır. | 4.41 | 0.90 |
| 29. Internet, firmaların müşterilerinin isteklerini karşılamaya yönelik imkânlarını arttırmaktadır. | 4.83 | 0.38 |
| 30. Internet'in zayıflığının nedenlerinden bir tanesi de iletişim protokollerinin yetersizliğidir. | 3.58 | 0.90 |
| 31. Internet'in problemlerinden birisi de iletişim bilgilerinin doğrulanmasındaki yetersizliklerdir. | 3.50 | 0.90 |
| 32. Internet'in problemlerinden birisi de Internet üzerindeki özel bilgilerin korunmasındaki yetersizliklerdir. | 4.27 | 0.46 |
| 33. Ağ yapısındaki konfigürasyon zayıflıkları ağ yapılarının karmaşıklığından kaynaklanmaktadır. | 3.41 | 0.99 |
| 34. Teknolojinin zayıflığı **yazılım** ürünlerinin yetersizliğinden kaynaklanmaktadır. | 2.66 | 1.49 |

**Tablo 2. Internet Güvenliği Anket Maddeleri**

| Anket Maddesi | X | SS. |
|---|---|---|
| 35. Teknolojinin zayıflığı **donanım** ürünlerinin yetersizliğinden kaynaklanmaktadır. | 2.41 | 1.37 |
| 36. En önemli Internet güvenlik kontrol aracı fiziksel (donanımsal) güvenlik kontrol sistemleridir. | 3.08 | 0.90 |
| 37. En önemli Internet güvenlik kontrol aracı personele yapılan güvenlik kontrolleridir. | 2.83 | 1.46 |
| 38. En önemli Internet güvenlik kontrol aracı yönetici güvenlik kontrolleridir. | 2.75 | 1.42 |
| 39. En önemli Internet güvenlik kontrol aracı veri iletişim güvenlik kontrolleridir. | 3.75 | 1.42 |
| 40. En önemli Internet güvenlik kontrol aracı bilgisayar güvenlik kontrolleridir. | 4.16 | 0.71 |
| 41. En önemli Internet güvenlik kontrol aracı hasar tamiri (disaster recovery) ve geri yüklemelerdir. | 3.50 | 1.08 |

### 3.3. Internet Güvenliği Açıkları

Katılımcılardan (n=12) kendilerine verilen Internet güvenlik açıklarını en çok tehlikeliden (5) en az tehlikeye (1) doğru numaralandırmaları istenmiştir. Tablo 3'den de görülebileceği gibi genç yöneticilere göre en tehlikeli güvenlik açığı "ağ dinleme" ve "şifre tabanlı saldırılardır".

**Tablo 3. Internet Güvenlik Açıkları**

| | Min Değer | Max Değer | X | SS. |
|---|---|---|---|---|
| Şifre tabanlı saldırılar | 3.00 | 5.00 | 4.33 | 0.65 |
| IP yakalaması | 1.00 | 5.00 | 2.41 | 1.50 |
| Erişim güvenliğini istismar eden saldırılar | 2.00 | 5.00 | 3.33 | 1.15 |
| Ağ dinleme | 3.00 | 5.00 | 4.66 | 0.65 |
| Teknoloji açıklarından kaynaklanan saldırılar | 2.00 | 5.00 | 4.00 | 0.73 |

### 3.4. Internet Güvenliği Açıkları

Katılımcılardan (n=12) kendilerine verilen Internet güvenliği sağlama tekniklerini en önemliden (5) en az önemliye (1) doğru numaralandırmaları istenmiştir. Tablo 4'den de görülebileceği gibi yöneticilere göre en önemli güvenlik aracı "Authentication (Kimlik kontrolü)", "Access controls (Erişim kontrolleri)" ve "Encryption (Şifreleme)" teknikleridir.

**Tablo 4. Internet Güvenliği Sağlama Teknikleri**

| | Min Değer | Max Değer | X | SS. |
|---|---|---|---|---|
| Access controls (Erişim kontrolleri) | 2.00 | 5.00 | 4.16 | 1.02 |
| Authentication (Kimlik kontrolü) | 4.00 | 5.00 | 4.50 | 0.52 |
| Encryption (Şifreleme) | 2.00 | 5.00 | 4.16 | 1.11 |
| Firewall (Güvenlik duvarı) | 1.00 | 5.00 | 2.83 | 1.46 |
| Anti-virus tools (Anti virüs araçları) | 1.00 | 5.00 | 2.66 | 1.55 |

## 4. Sonuç

Ortaya çıkan yeni Internet teknolojileri bizleri küreselleştirirken, küreselleşme de yeni güvenlik sorunları oluşturmaktadır. Bu durum ise modern toplumların ekonomik refahı noktasında bir tehdit riski oluşturmakta ve vatandaşların güvenliği ve istikrarını bozmaya yönelik girişimlerin oluşmasına neden olabilmektedir [4]. Bu çalışma içerisinde bu kadar önem taşıyan Internet güvenliği noktasına mikro bir çalışma yapılmıştır. Çalışma içerisinde 12 genç Bilgi ve İletişim Teknolojileri kurumlarında çalışan yöneticilerin Internet güvenliği noktasındaki görüşleri toplanmış ve değerlendirilmiştir. Elde edilen ilk sonuçlara bakıldığında yöneticilerin Internet'i birçok farklı amaç (eposta, alışveriş, sosyal medya ve sohbet) için kullandıklarını göstermektedir. Yöneticilerin kullanım amaçları ile yaşıtlarının kullanım amaçları arasında alanyazın incelendiğinde çok fark görülmemektedir [8].

Her ne kadar ülkeler kendi yargı sistemleri içerisinde Internet güvenliğini sağlamak adına hukuki düzenlemeler yapsalar da, bu düzenlenmelerin Internet kullanıcıları açısından manası netleşmemektedir [11]. Bu çalışma içerisinde de katılımcılar Internet hakkında yapılacak olan yasal düzenlemelerin, özgürlüklerini kısıtlayıp kısıtlamayacağı noktasında kararsız kalmışlardır. O halde yasal düzenlemeler konusunda yukarıdan-aşağıya yaklaşımı yerine, aşağıdan-yukarıya yaklaşımı güdülerek, halkın daha etkin katılımıyla yasal çalışmalar yapılabilir. Ayrıca ortaya çıkacak olan yasal yükümlülüklerin daha etkin bir şekilde halkla paylaşılması da gereklidir.

Kişilerin değer yargılarının Internet güvenliği noktasında ne kadar önemli olduğu düşünülürse [8], genç yöneticilerin hackleme ve crackleme işlemlerini yapmış olmaları, Internet üzerinden film ya da müzik indirmede sakınca görmüyor olmaları, Internet üzerindeki zararlı içerik diyebileceğimiz uyuşturucu ve cinsellik içeren web sitelerinden yüksek oranda rahatsız olmamaları, bu çalışma adına dikkate değer sonuçlardır. Bir başka deyişle, bireysel olarak olumsuz eylemlere karşı tepkisiz ya da eğilimli bireylerin sorumluluklarında olan kurumlara karşı sergileyecekleri tutum ve işlerin de ne kadar başarılı olacağı düşünülmelidir.

Genç yöneticilerin Internet üzerinde güvenlik sağlama adına en önce neyin kontrol edilmesi gerektiğine yönelik sorulara verdikleri cevaplar üzerinde de düşünülmesi gerekmektedir. Elde edilen sonuçlara bakıldığında katılımcılar öncelikli olarak teknolojik araç ve gereçlerin sıkı bir şekilde kontrol edilmesi gerektiğini savunurken, son aşamada ise personellerinin ve kendilerinin kontrol edilmesi gerektiğini söylemektedir. Oysa ki unutulmaması gereken nokta, yazılım ve donanımların insana hizmet eden araçlar olduğudur. Bu nedenle bireylerin Internet güvenliği noktasındaki etik duruşları ve eylemleri donanımın kontrolünden daha da önem taşımalıdır.

Çalışmanın sonuçları değerlendirilirken bu çalışmanın örnekleminin kısıtlı olması, seçilen bölgenin özelliği, çalışmanın sadece nicel veriler üzerine bina edildiği unutulmamalıdır. Bu nedenle bu çalışmanın öncelikle daha büyük bir örneklem grubuyla, yaş aralığı daha da geniş tutularak, nicel ve nitel tekniklerin bir arada kullanılması ile tekrarlanması gerekmektedir.

## 5. Kaynaklar


[1] Brenner, J. F. "Why Isn't Cyberspace More Secure?", **Communications of the ACM**, 53 (11), 33-35. (2010).

[2] Büyüköztürk, Ş. Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş.ve Demirel F., "Bilimsel Araştırma Yöntemleri". **Pegem Yayınları**, Ankara, (2000).

[3] Cetron, M. J. ve Davies, O., "World War 3.0:Ten Critical Trends for Cybersecurity", **The Futurist**, Eylül-Ekim, 40-49, (2009).

[4] Deibert, R. J., ve Rohozinski, R. "Risking Security: Policies and Paradoxes of Cyberspace Security", **International Political Sociology**, 4, 15–32, (2010).

[5] Grant, J. A. "The National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy through Standards", **IEEE INTERNET COMPUTING,** Kasım – Aralık, 80-84, (2011).

[6] Lukasik, S. J. "Protecting Users of the Cyber Commons", **Communications of the ACM,** 54 (9), 54-61. (2011).

[7] Nielsen, S. C. ve Welch, D. "Teaching Strategy and Security in Cyberspace: An Interdisciplinary Approach", **International Studies Perspectives**, 4, 133–144, (2003).

[8] Palesh, O., Saltzman, K., ve Koopman, C. "Internet Use and Attitudes Towards Illicit Internet Use Behavior in a Sample of Russian College Students", **Cyberpsychology & Behavior**, 7 (5), 553-558, (2004).

[9] Schwartz. A. "Identity Management and Privacy: A Rare Opportunity To Get It Right", **Communications of the ACM**, 54 (6), 22-24. (2011).

[10] Walden, I. "Crime and Security in Cyberspace", **Cambridge Review of International Affairs**,18(1), 51-68, (2005).

[11] Wall, D. S. "Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace", **Police Practice and Research**, 8(2), 183–205, (2007).