Hacker kültürü ve Tarihi hakkında çeşitli bilgiler bulunmakta ve bu bilgileri **Hacker Kavramı ve Siber Güvenlik** ile daha geniş bir bağlamda tartışılmaktadır.

Hacker Kavramının Kökenleri ve Tarihsel Gelişimi

- Hacker terimi, **1960'ların başlarında Massachusetts Teknoloji Enstitüsü'nden (MIT)** bir grup tutkulu programcının kendilerine hacker demesiyle ortaya çıkmıştır. Bu dönemde MIT, bilgisayar çalışmalarına çok fazla adanmış öğrencilere bağımsız çalışma izni vermiştir.
- İlk hackerlar, **bilginin kısıtlanmasına, gizlenmesine ya da sadece belli bir kesimin kullanımına açık olmasına karşı olmuşlardır**. Onlar için temel yaklaşım **bilginin daima özgür ve herkese açık olmasıydı**. Bu dönemde "hack" fiili, bir sistemin bilinmeyen sırlarını ortaya çıkarmak veya sistemi belli bir amaca hizmet edecek şekilde yeniden programlamak anlamına gelmekteydi. Bu açıdan hackerlar, **son derece yetenekli ve üretken programcılar** olarak görülmekteydi.
- **1980'lerin ortalarına gelindiğinde hacker kavramında bir değişim** ortaya çıkmıştır. Hacker kelimesi artık sadece olumlu bir kavramı değil, **suç ile ilişkili olarak bilgisayar korsanlarını ifade etmek için de kullanılmaya başlanmıştır**. Hackerlar ise bu kavram karmaşasını önlemek amacıyla **sistem güvenliklerini kıran kişilere "cracker" demeye başlamışlardır**. Ancak bu ayrım kamuoyunda her zaman net olmamıştır.
- Hacker kültürünün **üç kuşak** geçirdiği belirtilmektedir. İlk kuşak, açık akademi modelini benimsemiş ve bilgi paylaşımını esas almıştır. İkinci kuşak, ilk kuşağın etik değerlerini benimsemekle birlikte, uzak sistemlere erişimi ve bu erişimi paylaşmanın zararlı olmadığı düşüncesini benimsemiştir. Üçüncü kuşak ise, yaptıkları işlerden para kazanabilecekleri ticari mekanizmalar kurmuştur.
- **Günümüzde** hem olumlu hem de olumsuz anlamları barındıran tanımları mevcuttur ve tanımlayan kişinin bakış açısına göre bu tanım değişmektedir.

Hacker Kültürünün Beslendiği Kaynaklar ve Etik Değerleri

- Hacker kültürünün **temelinde bilgiye erişimin kısıtlanmasına karşı olma ve bilginin özgür olması gerektiği inancı yatmaktadır**.
- **Steven Levy'nin "Bilgisayar Devriminin Kahramanları" adlı eserinde** hacker kültürünün temel etik kodları sıralanmıştır. Bu etik değerler genel olarak şunlardır: bilgisayarlara erişimin kısıtlanmaması, bilginin özgür olması, otoriteye güvenilmemesi, hackerların yaptıkları işlerle değerlendirilmesi, bilgisayarların yaşamı olumlu yönde geliştirmesi ve iyi işler için kullanılması. Ancak tüm hackerların bu etik değerlere uymadığı belirtilmektedir.
- **Pekka Himanen'in "Hacker Etiği" adlı eserinde** hackerların çalışma etiği, network etiği ve para etiği gibi farklı etik kodlarla hareket ettikleri belirtilmektedir. Hacker para etiği genellikle bilgiyi paylaşmayı esas alırken, çalışma etiği iş odaklı yaklaşımdan

tutku odaklı bir yaklaşıma kayışı gösterir. Network etiği (netik) ise İnternet üzerindeki ifade özgürlüğü ve herkesin İnternet'e erişebilme özgürlüğü gibi fikirleri kapsar.
- Hacker kültürü, **Hofstadter'in "Gödel, Escher, Bach" adlı eserinden, cyberpunk kültüründen ve Jargon File gibi ortak kültürel miraslardan beslenmektedir**.

Hackerların Motivasyonları

- Hackerların motivasyonları çeşitlilik gösterir. **Linus Torvalds'a göre** hackerlığın dürtüsü temel olarak üç seviyeden oluşur: hayatta kalma, toplumsal hayat ve eğlence (tutku). Hackerlar bilgisayarları toplumsal hayat için kullanmakta ve kodlarla yeni şeyler yaratarak hem eğlenmekte hem de toplumsallaşmaktadırlar.
- Diğer motivasyonlar arasında **merak, öğrenme isteği, beceri gösterme, bilgiye erişim, maddi kazanç, politik ve sosyal aktivizm (hacktivizm), zarar verme ve eğlence** sayılabilir.

Hacker Çeşitleri

- Hackerlar **niteliklerine ve amaçlarına göre** çeşitli kategorilere ayrılmaktadır. En yaygın sınıflandırma **"şapka renklerine"** göre yapılan ayrıştır:
  - **Beyaz Şapkalı Hacker (Etik Hacker):** İyi niyetli hackerlardır. Sistemlerdeki güvenlik açıklarını tespit edip bu açıkları kapatmaya veya ilgili kuruluşlara bildirmeye çalışırlar. Savunma amaçlı çalışırlar.
  - **Siyah Şapkalı Hacker:** Kötü niyetli hackerlardır. İzinsiz olarak sistemlere sızarak bilgi hırsızlığı, dolandırıcılık, zarar verme gibi faaliyetlerde bulunurlar. Yazılımların kopyalama korumalarını kıranlara "cracker" denir.
  - **Gri Şapkalı Hacker:** Yasallık sınırında dolaşan hem iyi niyetli hem de kötü niyetli faaliyetlerde bulunabilen hackerlardır.
  - **Kırmızı Şapkalı Hacker:** Kendilerini diğer hackerlardan ayıran, genellikle hacktivizm eylemlerinde görülen bir türdür. Redhack kendisini kırmızı şapkalı hacker olarak tanımlamaktadır.
- Diğer türler arasında **lamer (bilgisi olmadan hacker gibi davranan), script kiddie (başkalarının araçlarını kullanan), hacktivist (politik amaçlı eylemde bulunan), devlet destekli hacker, ajan hacker ve siber teröristler** sayılabilir.

Hacker Kültürü ve Siber Güvenlik

- Siber güvenlik, **kötü niyetli hackerların neden olduğu tehditlere karşı sistemleri ve bilgileri koruma çabalarını içerir**.
- **Siyah şapkalı hackerlar**, siber güvenlik için doğrudan bir tehdit oluştururlar.
- **Beyaz şapkalı hackerlar (etik hackerlar)** ise sistemlerdeki güvenlik açıklarını bularak ve bu açıkları gidermeye yardımcı olarak **siber güvenliğin sağlanmasında önemli bir rol oynarlar**. "Ofansif güvenlik" ve "etik hacking" gibi yaklaşımlar, kötü niyetli saldırıları engellemeye yöneliktir.
- **Hacker taggers** kavramı, hackerların veya siber güvenlik uzmanlarının hackledikleri

sistemlere sanal bir işaret bırakmalarını ifade eder. Bu etiketler, saldırıların izini sürmek ve saldırganların motivasyonlarını anlamak için incelenebilir.
- **Birçok devlet**, hackerların (özellikle yetkisiz erişim ve zarar verme eylemlerini) suç olarak nitelendirmekte ve buna göre yasal düzenlemeler yapmaktadır.

Türkiye'de Hacker Kültürü

- Türkiye'de hacker kültürü, Batı'daki gelişiminden farklılıklar göstermektedir. Toplumsal algıda hacker ve cracker kavramları medya etkisiyle genellikle olumsuz anlamlar yüklenmiştir.
- Akademik düzeyde yapılan araştırmalar, Türkiye'deki hackerların çoğunlukla **genç yaştaki erkek öğrenciler** olduğunu ve hackerlık bilgilerini forumlardan öğrendiklerini göstermektedir. Motivasyonları arasında **eğlenmek ve ülke menfaatleri çerçevesinde milli bir duruş sergilemek** öne çıkmaktadır.
- Türk hackerların etik anlayışları da Batı'daki özgürlükçü yaklaşımdan farklı olarak daha çok **ülkü, kişisel ahlak ve milli değerler** üzerine kuruludur.
- Türkiye'de **milliyetçi ve muhafazakâr görüşlerden beslenen (örneğin Turk Hack Team, Ayyıldız Tim)** ve **siberpunk yaklaşımını benimseyen (örneğin Redhack)** gibi farklı hacker grupları bulunmaktadır.

Sonuç olarak, hacker kavramı ve hacker kültürü, kökenlerinden günümüze kadar önemli dönüşümler geçirmiştir. Başlangıçta yetenekli programcıları ifade eden ve bilgi paylaşımını savunan bir anlam taşırken, kötü niyetli kullanımların artmasıyla birlikte suçla özdeşleşen bir algı da oluşmuştur. Siber güvenlik bağlamında hem tehdit unsuru (siyah şapkalı hackerlar) hem de savunma mekanizması (beyaz şapkalı hackerlar) olarak önemli bir rol oynayan hackerlar, farklı motivasyonlara ve etik anlayışlarına sahip çeşitli grupları içermektedir. Türkiye'deki hacker kültürü ise kendine özgü dinamikleri ve toplumsal algısıyla Batı'daki örneklerinden farklılaşmaktadır. Medyanın hackerları genellikle suç odaklı bir şekilde sunması, kamuoyundaki algıyı önemli ölçüde etkilemektedir.