Bu makalede; küreselleşme ve bilişim arasındaki ilişkiyi, **hacker kavramını** ve bunların **siber güvenlik** ile daha geniş bağlamını çeşitli açılardan ele alınmaktadır.

Küreselleşme ve Bilişim

Küreselleşme, bağlantılılık, zamanın hızlanması, teknoloji, mekânın küçülmesi ve sermaye gibi beş ortak özelliğe sahiptir. **Bağlantılılık**, farklı kültürlerden veya aynı kültürlerden olup farklı yerlerdeki insanların bağlantılı hale gelmesini ifade eder. **Teknolojinin gelişmesi**, bilginin, paranın ve yatırımın döngüsünü (sermaye) mümkün kılmış ve aynı zamanda farklı kültürlerin değerleriyle daha fazla karşılaşmayı beraberinde getirmiştir.

Enformasyonel devrimlerin temel altyapısı internet ve bilgisayardır. Bilişim sistemleri, veri işleme, saklama ve iletmeye yönelik bilgisayar, çevre birimleri, iletişim altyapısı ve programlardan oluşur. Günümüz teknolojilerinin oluşumunda **hackerların büyük bir payı bulunmaktadır**. Onların tutku dolu çalışmalarıyla yazılım dünyası gelişebilmiş ve güncel olarak kullanılan birçok teknolojik aygıt ortaya çıkabilmiştir. **Hackerların kamusal alana müdahalesi kodlama ve yazılım geliştirme ile mümkün olmaktadır**. Üretilen birçok teknolojik aygıtın (bilgisayar, cep telefonu vb.) hackerların özgür çalışma ritimleri ile üretildiği belirtilmektedir.

Ağ toplumu, teknolojik devrimlerin toplumsal yapıyı dönüştürmesiyle ortaya çıkmış, zaman ve mekanı aşan, sanallık kültürü inşa eden bir yapıdır. Ancak ağ toplumunda eşitsizlikler, kutuplaşma ve dışlama üzerine kurulu bir düzenin gezegene yayıldığı ve bu durumun direniş kimliklerinin ortaya çıkmasına neden olduğu belirtilmektedir.

Hacker Kavramı

Hacker kelimesinin anlamı zaman içinde değişmiştir ve hem iyi hem de kötü anlamları barındıran tanımları mevcuttur. Tanımlayan kişinin siyasi ve ideolojik görüşü, toplumsal konumu ve bilişim sistemlerine bakış açısı bu tanımı etkilemektedir.

Başlangıçta, **1960'larda MIT'de ortaya çıkan ilk hackerlar, bilginin kısıtlanmasına ve sadece belirli bir kesimin kullanımına açık olmasına karşı olmuşlardır**. Onlar için temel yaklaşım **bilginin daima özgür ve herkese açık olmasıydı**. Bu dönemdeki "hack" fiili, bir sistemin sırlarını ortaya çıkarmak veya sistemi yeniden programlamak anlamına gelmekteydi ve hackerlar yetenekli ve üretken programcılar olarak görülmekteydi. Açık kaynak hareketi, Linux temelli işletim sistemleri, Firefox tarayıcı gibi konular hackerlık kavramının merkezinde yer alır. Hackerlık, öğrenme ve öğrendiklerini paylaşma faaliyeti içinde bir tür yaratımdır.

Ancak zamanla, özellikle **1980'lerden sonra hacker kelimesi suç ile anılmaya başlanmıştır**. Hackerlar ise sistem güvenliklerini kıran kişilere **"cracker"** demeye başlamışlardır. Crackerlar, bilgisayar sistemlerini bozan ve telefon sistemlerini izinsiz kullanan kişilerdir. Temel fark, üstatların (hackerların) bir şeyler kurması ve inşa etmesidir.

Hacker Çeşitleri

Günümüzde hackerlar, **niteliklerine ve amaçlarına göre** farklı kategorilere ayrılmaktadır:

- **Beyaz Şapkalı Hacker (Etik Hacker):** İyi niyetli hackerlardır, sistemlerdeki güvenlik açıklarını tespit edip bildiren ve siber güvenliği sağlamaya çalışan kişilerdir. “Ofansif güvenlik” ve “etik hacking” gibi yaklaşımlar siber güvenliği sağlamaya yöneliktir.
- **Siyah Şapkalı Hacker:** Kötü niyetli hackerlardır, izinsiz erişim sağlayarak bilgi hırsızlığı, zarar verme gibi faaliyetlerde bulunurlar. Yazılımların kopyalama korumalarını kıranlara “cracker” denir.
- **Gri Şapkalı Hacker:** Hem iyi niyetli hem de kötü niyetli faaliyetlerde bulunabilen, yasallık sınırında dolaşan hackerlardır.
- Diğer türler arasında lamer, script kiddie, hacktivist (politik amaçlı eylemde bulunan), devlet destekli hacker, ajan hacker ve siber teröristler sayılabilir.

Hacker Kültürü

Hacker kültürünün temelinde bilgiye erişimin kısıtlanmasına karşı olma ve bilginin özgür olması gerektiği inancı yatmaktadır. Hacker etiği, bilgisayarlara erişimin kısıtlanmaması, bilginin özgür olması, otoriteye güvenilmemesi, hackerların yaptıkları işlerle değerlendirilmesi, bilgisayarların yaşamı olumlu yönde geliştirmesi ve iyi işler için kullanılması gibi ilkeleri içerir. Ancak tüm hackerların bu etik değerlere uymadığı belirtilmektedir.

Türkiye’de hacker kültürü

Türkiye’de hacker kültürü, Batı’daki gelişiminden farklılıklar göstermektedir. Toplumsal algıda hacker ve cracker kavramları genellikle olumsuz anlamlar taşımaktadır. Ancak popüler algının ötesinde hackerların bir kültürü ve hatta bir alt/karşı kültürü temsil ettiği belirtilmektedir. Türkiye’deki hackerların çoğunlukla genç yaştaki erkek öğrenciler olduğu ve motivasyonları arasında eğlenmek ve ülke menfaatleri çerçevesinde milli bir duruş sergilemek öne çıkmaktadır. Türk hackerların etik anlayışları da daha çok ülkü, kişisel ahlak ve milli değerler üzerine kuruludur. Türkiye’de milliyetçi (Turk Hack Team, Ayyıldız Tim) ve siberpunk (Redhack) gibi farklı hacker grupları bulunmaktadır.

Siber Güvenlik Bağlamı

Siber güvenlik, **kötü niyetli saldırganların neden olduğu tehditlere karşı bilgisayar sistemlerini, ağları ve dijital verileri koruma sürecini ifade eder**. Web servisleri siber güvenlik açısından potansiyel hedeflerdir ve saldırganlar veri ihlalleri, kimlik hırsızlığı gibi tehditler yaratabilirler.

Siyah şapkalı hackerlar siber güvenlik için doğrudan bir tehdit oluştururken, beyaz şapkalı hackerlar (etik hackerlar) sistemlerdeki güvenlik açıklarını bularak ve

gidererek siber güvenliğin sağlanmasında önemli bir rol oynarlar.

Hacker taggers, 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 tarafından hackerların (özellikle yetkisiz erişim ve zarar verme eylemleri) suç olarak nitelendirildiği ve buna göre yasal düzenlemeler yapıldığı belirtilmektedir. Türk Ceza Kanunu'nda bilişim sistemine girme (m.243), sistemi engelleme, bozma, verileri yok etme veya değiştirme (m. 244), banka veya kredi kartlarının kötüye kullanılması (m. 245) gibi bilişim suçları düzenlenmiştir. Siber saldırılar bilgisayar ağları ve web uygulamaları üzerinde gerçekleştirilen kötü niyetli eylemlerdir ve siber güvenliği ihlal ederek kullanıcıların verilerini tehlikeye atabilir.

Daha Geniş Bağlam

Küreselleşme ve bilişimin yaygınlaşması, dünyayı daha bağlantılı hale getirirken siber güvenlik tehditlerini de artırmıştır. Sınırların ortadan kalktığı bu dijital dünyada, kötü niyetli hackerlar dünyanın herhangi bir yerinden saldırılar düzenleyebilirken, etik hackerlar da küresel çapta bilgi paylaşımı ve işbirliği yoluyla siber güvenliği güçlendirebilirler.

Hacker kavramının tarihsel gelişimi, teknolojinin ve toplumun etkileşimiyle şekillenmiştir. Başlangıçtaki idealist ve bilgi paylaşımcı yaklaşım, zamanla suç ve güvenlik odaklı bir algıya dönüşmüştür. Medyanın hackerları genellikle suçla ilişkilendiren bir şekilde sunması bu algının pekişmesinde etkili olmuştur.

Ancak hacker kültürünün açık öğrenim modeli ve bilgiye özgür erişim ilkesi, küreselleşen dünyada farklı alanlar için de örnek teşkil edebilir. "Net akademisi" gibi yapılar, etik anlayış ve bu öğrenim modeliyle yaratıcı kaynaklar üretebilir.

Sonuç olarak, küreselleşme ve bilişim çağında hacker kavramı ve siber güvenlik, karmaşık ve çok boyutlu olgular olarak karşımıza çıkmaktadır. Hackerlar hem teknolojik gelişimin önemli aktörleri hem de siber güvenlik tehditlerinin kaynağı olabilirler. Etik değerleri, motivasyonları ve toplumsal algıları farklılık gösteren hacker gruplarının eylemleri, siber güvenliğin sağlanması ve dijital dünyanın düzenlenmesi açısından önemli bir rol oynamaktadır.