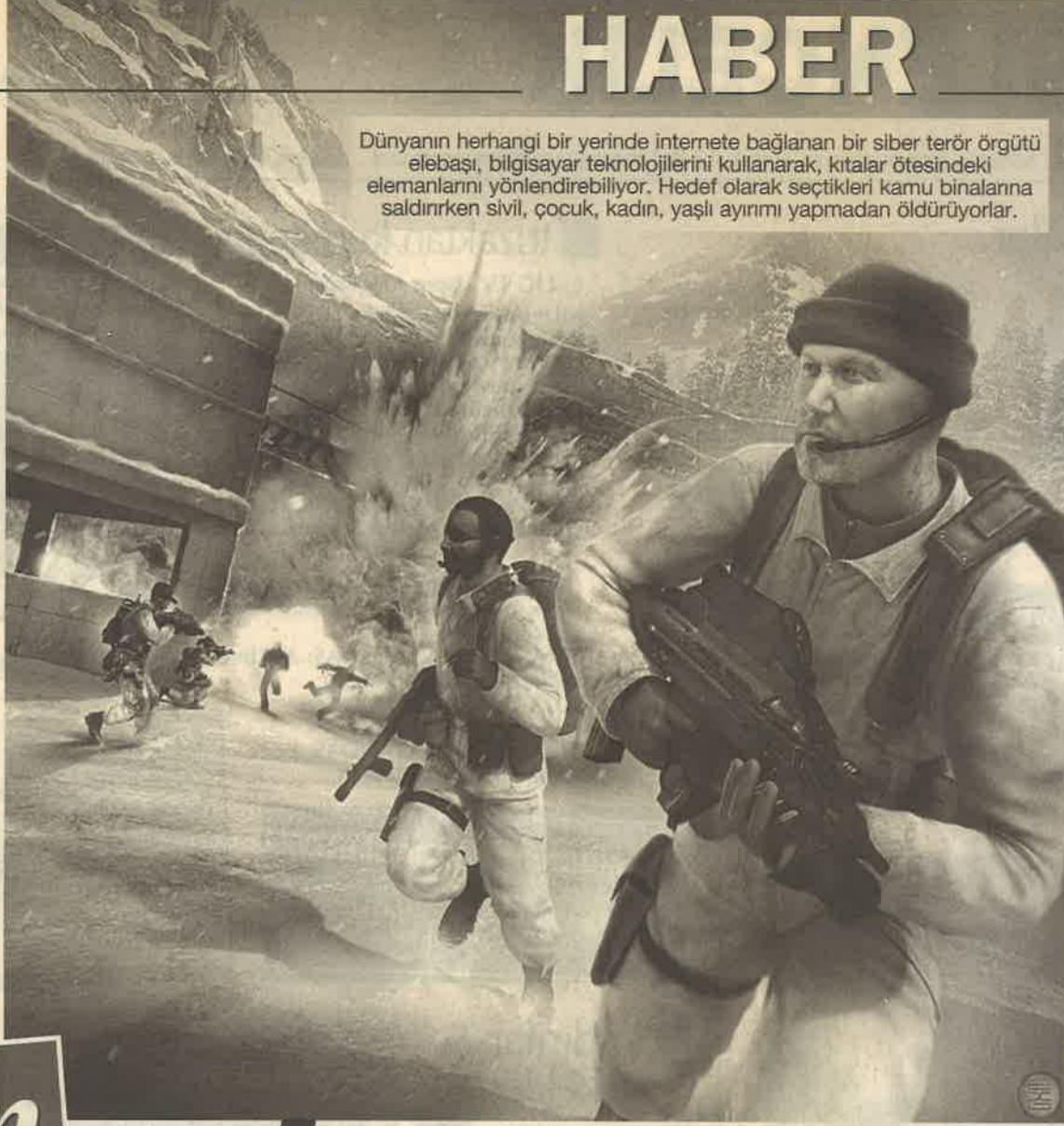


Siber terör nedir?

■ **SİBER** terörizm, klasik anlamdaki terör eylemlerinin bilgisayar ve internet sistemleri kullanılarak icra edilmesi; belirli bir politik ve sosyal gayeye ulaşabilmek için bilgisayar teknolojilerinin hükümeti, şahısları, şirketleri veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır. Bölücü terörün gayesi tek başına şiddet değil, bu şiddet yolu ile kamuoyunda oluşturmak istediği baskı ortamı ve bu ortamın sağladığı korku ve yulgınlık ile kendisine taraftar bulmaktır. İngiltere'de 2000 yılında çıkarılan Terörizm Yasasına göre "siber terörizm", "Hükümeti etkilemek ya da toplumu korkutmak amacıyla elektronik sistemlerin içine izinsiz girmek veya bu sistemleri bozmak" olarak tanımlanıyor. Bu yeni yasaya göre bir grup internet eylemcisi başbakanı e-mail protestosu gerçekleştirir ve bu e-mailer başbakanlık internet sisteminde bir çöküntüye sebep olursa, bu eylem, siber terörizme girer.



Dünyanın herhangi bir yerinde internete bağlanan bir siber terör örgütü elebaşı, bilgisayar teknolojilerini kullanarak, kıtalar ötesindeki elemanlarını yönlendirebiliyor. Hedef olarak seçtikleri kamu binalarına saldırırken sivil, çocuk, kadın, yaşlı ayırımı yapmadan öldürüyorlar.

Fare-internet çıktı mertlik bozuldu!

■ **SİBER** teröristler, klasik teröristler gibi eylemlerini gerçekleştirmek için bomba veya silahlara değil sadece bir bilgisayar ve modeme ihtiyaç duyar. Bu sayede hem eylemleri çok daha kolay bir şekilde gerçekleştirebilmekte hem de güvenlik güçlerine yakalanma risklerini minimuma indirmektedirler. Siber terör, yeni yüzyılda terörizmin çirkin yüzü olarak bütün dehşetiyle karşımızda durmaktadır. Teröristlerin, büyük bir barajın kapaklarının kontrolünü ele geçirdiklerini, silahlı kuvvetlerin füze kontrol sistemlerini ele geçirdiklerini ya da büyük bir kentin sabah yoğun trafikte tüm trafik ışıklarını durdurduklarını veya doğal gaz şebekelerinin basıncını kontrol sistemi ele geçirerek basıncı arttırdıklarını düşünün! Ya da sadece büyük bankaların hesaplarına girip "küçük!" değişikliklerle milyonlarca doları kendi hesaplarına geçirdiklerini hayal edin! Hayali bile korkunç bu fantezilerin gerçekleşmesi zor olsa da imkansız değildir.



Yüzyılın kâbusu:

SİBER TERÖR

Bilgisayar ve internet hayatımızı kolaylaştırmakla birlikte teknolojik terör tehdidini artırdı. Yurt dışı kaynaklı 8 bin internet sitesi, Türkiye'nin bütünlüğü aleyhine faaliyet gösteriyor.

■ **STANBUL-** İnternetin dünya çapında yaygınlaşmasıyla, kıtalar arası bilgi aktarımı bir tuşa basmaktan ibaret hale geldi. Zamanın verimli kullanılmasını sağlayan ve mekân kavramını da ikinci plana iten "siber uzay", birçok sahada sağladığı büyük faydaların yanı sıra, organize terör örgütlerinin cirit attığı meydan haline geldi. Uluslararası organize suç ve terör örgütleri, gelişen yeni teknolojileri kullanarak, bilinen suç yöntemlerine ilave olarak, yeni saldırı ve gasp metotları geliştirdiler. Devletlerin iç güvenliğini tehdit eden ve hedefine ulaşmada hiçbir sınır tanımayan terör örgütleri, bilgisayar teknolojileri yardımıyla tahminlerin ötesinde bir hareketlilik kazanarak, uluslararası suç trafiğini daha da tehlikeli hale getirdiler. Globalleşmenin karanlık yüzü olarak adlandırılan bu gelişme, uluslararası barış ve güvenliği olduğu kadar, ülkemizin de millî güvenliğini ve huzurunu ciddi şekilde tehdit etmektedir.

■ Dünya eskisi gibi değil

ABD Devlet Başkanı George W. Bush'un, 11 Eylül 2001 terörist saldırılarının hemen ardından söylediği gibi, "Dünyada artık hiçbir şey eskisi gibi değil". ABD'deki son derece stratejik merkezleri hedef alan ve binlerce insanın hayatına mal olan 11 Eylül saldırıları, siber tehlikenin boyutlarını en açık şekilde gözler önüne serdi. Bu saldırılar, terör örgütlerinin bilgisayar sistemlerini ne kadar etkili kullandıklarının açık bir ispatı oldu. 11 Eylül, o güne kadar birtakım



Sefa Koyuncu

resmî internet sitelerini çökertme ile sınırlı kalan 'siber terör'ün hangi boyutlara ulaşabileceğini gösteren bir başlangıç oldu. Terör örgütleri istihbarat birimlerinin takibinden kurtulabilmek için telefon görüşmesini minimuma indirerek, kamuoyunun ortak kullandığı bilgisayar sistemleri ile iletişim kurmakta ve dünyanın herhangi bir yerinden, örgütleri açısından güvenli gördükleri yerlerden internete girip, planlama, haberleşme ve eylemlerini gerçekleştirmektedir. Siber teröristler, saldırıyı üstlenme, olayla ilgili bilgi ve fotoğrafları yayınlamada da araç olarak özellikle interneti tercih ediyor.

■ 8 bin bölücü site var

Emniyet kaynaklarına göre şu an Türkiye'nin bütünlüğü aleyhine faaliyet gösteren zararlı internet sitesi sayısı yaklaşık 8 bin civarında. Bu sitelerden 150 tanesi aktif olarak her gün ortalama 500-1000 kişinin ziyaret ettiği ve çoğunluğu yurt dışından yönetilen siteler. Genelde com, org.net uzantılı olan bu siteler Amerika, Almanya, Hollanda ve diğer Batı Avrupa ülkeleri üzerinden yayın yapmakta. Gelişen teknolojiyi kullanarak eğitim ve propaganda faaliyetlerini sürdüren terör örgütleri, bilişim teknolojilerinden faydalanarak devletin kullandığı link hatlarını sabote etmeye çalışıyor. Bölücü örgütlerin, bilgi işlem merkezlerine, bakanlıklara, PTT, Telekom, Emniyet Genel Müdürlüğü ve TSK gibi hayati önem arz eden birimlerin sistemlerine siber saldırılarda bulunmak veya tahrip edici virüsler aracılığıyla bu sistemleri çökertmek için uğraştıkları kaydediliyor.



Milletlerarası iş birliği şart

■ 11 Eylül saldırılarından sonra, sanal âleminde eşi görülmemiş bir "siber savaş" başladı. Hem Amerikan yanlıları hem de karşıları yoğun bir karşılıklı saldırı işine giriştiler. Taliban.com veya talibanonline.com gibi adreslerin yanında Filistin, Pakistan ve Afganistan kaynaklı web siteleri de bu yoğun saldırıların hedefi haline geldi. Genelde e-mail bombardımanı şeklinde geçen bu savaş, sitelerin tamamen çökertilmesi şeklinde de gerçekleştiriliyor. Ancak, klasik terör gibi, siber terörün önlenmesi için de milletlerarası iş birliği gerekiyor. Uzmanlar, bilgisayar sistemlerinin tüketicileri olan şahısların, şirketlerin ve özel sektörün de siber suçlarla mücadelede, güvenlik güçlerine yardımcı olabileceğini belirtiyor. Nasıl ki, herkes evini hırsızların giremeyeceği şekilde güvenlik tedbirleriyle donattığında, hırsızlık olaylarında önemli düşüş oluyorsa, bilişim alanında alınabilecek tedbirlerle de siber suçların azaltılabileceğine dikkat çekiliyor.