

BİLİŞİM SAVAŞLARINA HAZIR MISINIZ?

Burak DAYIOĞLU, dayioglu@metu.edu.tr

İnternet'in son on yıl içerisindeki hızlı gelişimi bilginin yayılma hızını da inanılmaz bir biçimde arttırmıştır. Dileyen herkes, akla gelebilecek her alanda bilgiye büyük bir kolaylıkla erişilebilmektedir. Geçtiğimiz günlerde webde gezerken elime şans eseri 175 sayfalık bir kitapçık geçti; başlığı "Teröristin El Kitabı" idi ve içerisinde çeşitli patlayıcılara ilişkin detaylı bilgiler ve farklı bombaların nasıl yapılabileceğine ilişkin son derece detaylı tarifler vardı. Bu kitap ve içindeki bilgiler benim bir işime yaramadı ancak terör eylemlerini hedefleyen birisi olsaydım bu kitap çok faydalı olabilirdi.

Bilginin bu denli kolay bir biçimde paylaşılmasını sağlayan İnternet, bilişim sistemleri güvenliğini konu eden çok yüksek miktarda bilgiye de ev sahipliği yapıyor. Yalnızca İnternet'ten ve herkese açık bilgileri toplayan bir saldırgan, çok kısa sürede İnternet'e bağlı pek çok bilgisayar sistemine saldırabiliyor ve ciddi zararlar verebiliyor. İnternet üzerinde bugün gerçekleşen ve gazetelere de yansıyan siber saldırılar gelecek bilişim savaşlarının bir habercisi midir? Bu konuda herkes hemfikir olsa da merak sürüyor; "ilk savaş hangi ülkeler arasında ve ne zaman gerçekleşecek?".

Bazı uzmanlar, daha ileri giderek, bilişim savaşlarının "toplu-tüfekli" geleneksel savaşların yerini alacağını ve önümüzdeki yüzyılda geleneksel savaşlar ile giderek daha az karşılaşacağımızı öne sürüyorlar. Amerikan ordusunun "information warfare - IW" olarak anılan bilişim savaşlarına yönelik çok ciddi hazırlıklarının olması da bu beklentiye doğrular niteliktedir. Amerika ile birlikte dünyada yirmi kadar farklı ülkenin bilişim savaşlarına yönelik hazırlıkları olduğu İnternet'teki çeşitli kaynaklarca öne sürülmektedir.

Medyanın, finans kuruluşlarının, kamu hizmetlerinin ve iletişimin neredeyse tümüyle bilgisayarlı ortamda gerçekleştirildiği ülkeler giderek artan biçimde siber tehdit altındadırlar. Bir ülkenin bilişim altyapısı ele geçirildiğinde ya da çalışamaz hale getirildiğinde, ülkenin yaşamsal faaliyetleri durdurulmuş olacaktır. Böylesine büyük çaplı bir saldırı, başarılı olduğu takdirde, ülkenin haritadan silinmesine kadar giden bir çöküşün başlangıcı olabilir. Medyanın çalışmadığı, iletişimin gerçekleşmediği, banka hesaplarının boşaltıldığı ve kamu hizmetlerini veren bilgisayarların durduğu bir ülke varlığını sürdürebilir mi?

Konu öylesine ciddi ki, askeri literatüre Bilişim Harekatı (ing. Information Operations – IO) olarak girdi bile; NATO belgelerinde bu tamlamaya sıkça rastlamak mümkün hale geldi. Hızlı ve etkin çözümlerin üretilmemesi bir felakete neden olabilir. Bir bilişim harekatı yalnızca düşman bir ülkeden gelmek zorunda değil; terörist gruplar da güçleri ölçüsünde bir bilişim harekatına teşebbüs edebilirler.

Konunun bu hayati önemine rağmen Türkiye’de bu konuya yönelik çalışmalar son derece kısıtlı kalmıştır. Pek çok ülkenin aksine, ülkemizde ulusal ölçekte bir Bilgisayar Acil Durum Müdahale Ekibi (ing. Computer Emergency Response Team – CERT) bulunmamaktadır. Böylesi bir ekip, bilişim güvenliği konularında ulusal bir iletişim noktası oluşturulması, acil durumlara hızlı ve etkin müdahalenin sağlanması ve kurumlar arası koordinasyonun sağlanması anlamlarında oldukça faydalı olacaktır.

Kamu kuruluşlarımızın neredeyse hiç birisinin bir bilişim güvenliği programı yoktur; güvenlik politikaları, beklenmedik durum planları, eğitim ve teknolojik katkı gibi alanlarda hemen hiçbir hazırlık mevcut değildir. Kuruluşlarımızın büyük bir çoğunluğu, İnternet bağlantısının önüne yerleştireceği bir güvenlik duvarının bilişim güvenliği ile ilgili konularda tek başına yetkin bir çözüm oluşturacağını öngörmektedir.

Konunun önemi acil çözümlerin oluşturulmasını gerektirmektedir. Çözümler oluşturulurken göz ardı edilmemesi gereken belki de en önemli nokta bilişim güvenliğinin “Sonuç değil Süreç” olduğudur. Bilişim güvenliği ulaşılabilecek bir hedef değildir, bir süreçtir. Güvenliği sağlamak ve korumak düzenli ve planlı bir çalışmayı gerektirir.