

Amerika, Hegemonyasını Korumak İçin Küresel Bilgi Teknolojileri Güncellemelerini Kolaylıkla Bir Silah Olarak Kullanabilir

Dünyanın en kötü Bilgi teknolojileri (BT) kesintisinden birkaç hafta sonra, Microsoft'un siber güvenlik ortağı CrowdStrike şirketi hem yatırımcıların hem de şirketlerin açtığı davalarla karşı karşıya kaldı. Zira 18 Temmuz'da meydana gelen ve havayolu şirketleri, bankalar, sağlık hizmeti sağlayıcıları ve televizyon yayıncıları da dahil olmak üzere dünya genelinde kritik sektörleri etkileyen Bilgi Teknolojileri kesintisi, operasyonel kaosa ve büyük ekonomik kayıplara yol açtı.

CrowdStrike'nin hatalı güncellemesi, dijital ekosistemlerin birbirine bağımlılığı nedeniyle 8,5 milyon cihazı etkiledi ve sistem arızasına yol açarak Windows cihazlarda "mavi ölüm ekranlarına" neden oldu. Bu da kesintiden doğrudan etkilenmeyen şirketlerin hâlâ müşteri işlemlerini gerçekleştiremediği anlamına geliyor. Örneğin havayolu şirketleri biletleme sistemini kullanamadı ve CrowdStrike'ın CEO'su George Kurtz, Bilgi Teknolojileri kesintisinin küresel bir siber saldırıdan dolayı değil, insan hatasından kaynaklandığını vurguladı. Ancak bu tür güvenceler, bireysel cihazlarda manuel onarımlar yapmak zorunda kaldıklarından dolayı işletmeleri çok az teselli etmiştir.

Aslında burada yeni olan bir şey yok; zira Dünya Ekonomik Forumu (WEF) yıllık raporunda, siber saldırıları, daha geniş bir siber güvensizlik kategorisi içinde büyük bir küresel risk olarak sınıflandırmaktadır. Bu arada siber saldırılara karşı savunmayı güçlendirme çabaları devam etmektedir; zira küresel Bilgi Teknolojileri sistemlerinin birbirine bağlı olması, zengin ve gelişmekte olan ülkelerin suç ve terör saldırılarının yanı sıra insan hatalarına maruz kalmaya devam edeceği anlamına gelmektedir.

CrowdStrike'ın neden olduğu Bilgi Teknolojileri kesintisi insan hatasından kaynaklansa da bazı yönetim danışmanları ve tedarikçiler bu fırsatı değerlendirerek siber güvenlik araçlarının ve risk yönetimi uygulamalarının önemini vurguladılar. Örneğin McKinsey, teknoloji, dayanıklılık ve sınıfının en iyisi olan siber güvenlik ve risk yönetimine odaklanan bir makale yayınladı. Ancak hiç kimse dijital ekosistemlerimizin birbirine bağıllığıyla ilgili apaçık ortada olan soruyu sormuyor!

Peki ya bir sonraki küresel Bilgi Teknolojileri kesintisi geleneksel aktörler dışında başka bir şeyden kaynaklarsa; o zaman insan hatası mı, para sızdıran bir suç çetesi mi, yoksa terörist bir grup ya da haydut bir devlet tarafından yürütülen bir siber saldırı mı olacak? Nitekim CrowdStrike olayının normal tehdit aktörleri dışındaki jeopolitik yansımaları büyük ölçüde göz ardı edildi ve Georgetown Üniversitesi'nin jeopolitik etkileri hakkındaki çok az sayıdaki yorumdan biri, sadece küresel teknolojik altyapının kırılganlığı ile sınırlı kaldı.

Peki ABD, Microsoft güncellemelerini ya da diğer ABD şirketlerinin benzer hizmetlerini silah olarak kullanırsa ne olur? O zaman bu tehdit senaryoları, küresel siber güvenlik, Amerikan teknolojisine duyulan güven ve devletler arası ilişkiler konusunda büyük korkulara yol açması gerekir. Nitekim Amerika, SWIFT'i (Yurt içi ya da yurt dışındaki banka hesaplarına döviz olarak gerçekleştirilen tüm para

transferleri) bir silah olarak kullanmaya ve Rusya, İnan ve Kuzey Kore gibi hükümet odaklarını cezalandırmaya yönelik hazırlık yaptığını zaten göstermiştir.

Ayrıca ABD'nin büyük teknoloji şirketlerinin, Pentagon ve Amerika'nın önde gelen sinyal istihbarat örgütü Ulusal Güvenlik Ajansı (NSA) ile iş birliği yaptığı yaygın olarak kabul edilmektedir. Bu ortaklık, eski teknolojilerin yanı sıra bulut bilişim, yapay zekâ, artırılmış gerçeklik ve insansız hava araçları gibi birçok yeni teknolojiyi de kapsamaktadır. Bu teknolojilerin çift kullanımlı doğası hem sivil hem de askeri uygulamalara sahip oldukları anlamına gelmektedir. Aynı zamanda bu, Amerika'nın bu teknolojileri herhangi bir düşmana karşı bir silah olarak kullanabileceği ve üstün siber savunmalar yoluyla kendisini izole edebileceği anlamına gelmektedir. Şayet Microsoft, CoPilot'a (AI) yabancı topraklarda zararlı bir hale gelmesi için bir güncelleme aracılığıyla talimat vermiş olsa neler olabileceğini bir hayal edin; işte o zaman bu tür senaryoların geniş kapsamlı ve potansiyel olarak felaketler doğurabilecek sonuçları olabilir ve çok hızlı bir şekilde nükleer savaşa dönüşebilir.

Birçok ülke, ABD teknolojisine olan bağımlılıkları konusunda giderek daha fazla endişe duymakta ve aktif olarak bağımsız teknoloji kümeleri geliştirmeye çalışmaktadır. Çin bu eğilimi somutlaştırmaktadır; zira ABD teknoloji girdilerinden hali çiplerden uygulamalara kadar tamamen yerli bir teknoloji ekosistemi oluşturmaya çalışmaktadır. Pekin'in dijital altyapısını büyük Amerikan teknolojisinden korumaya yönelik proaktif önlemleri, yazılım güncellemelerini gerçekleştirmek için yerel şirketleri kullanarak elde ettiği CrowdStrike güncellemesi gibi olaylara dayanma kabiliyetiyle ortaya çıkmakta ve teknolojik egemenliğe yönelik bu dürtü, ABD'nin egemen olduğu teknoloji platformlarına ve altyapısına olan bağımlılığı azaltmaya yönelik daha geniş bir küresel değişimi yansıtmaktadır.

Bu arada dünya, Çin'e karşı Amerika gibi iki kutuplu bir teknolojik sisteme doğru kayarken Müslüman ülkelerin ayağa kalkıp bunu dikkate alması gerekiyor. Zira Amerikan ya da Çin teknolojisi arasındaki seçim yapmak köleleşmek anlamına gelmektedir. Nitekim Allahu Teala şöyle buyurmuştur: وَأَعِدُّوا لَهُمْ مَا اسْتَطَعْتُمْ مِنْ قُوَّةٍ وَمِنْ رِبَاطِ الْحَيْلِ تُرْهِبُونَ بِهِ عَدُوَّ اللَّهِ وَعَدُوَّكُمْ وَأَخْرَيْنَ مِنْ دُونِهِمْ لَا تَعْلَمُونَهُمُ اللَّهُ يَعْلَمُهُمْ وَمَا تُنْفِقُوا مِنْ شَيْءٍ فِي سَبِيلِ اللَّهِ يُوَفَّ إِلَيْكُمْ وَأَنْتُمْ لَا تُظْلَمُونَ **“Onlara (düşmanlara) karşı gücünüz yettiği kadar kuvvet ve cihad için bağlanıp beslenen atlar hazırlayın, onunla Allah'ın düşmanını, sizin düşmanınızı ve onlardan başka sizin bilmediğiniz, Allah'ın bildiği (düşman) kimseleri korkutursunuz. Allah yolunda ne harcarsanız size eksiksiz ödenir, siz asla haksızlığa uğratılmazsınız.”** [Enfal 60] Dolayısıyla ayet Müslümanlara, ümmetin düşmanlarına karşı zafer kazanmasını sağlayan egemen teknolojik paketi edinmelerinin emredildiğine delalet etmektedir. Bundan dolayı Müslüman ülkeler, teknolojik bağımsızlıklarını elde edebilmek için bu yönde hareket etmek zorundadır.

Hizb-ut Tahrir Merkezi Medya Ofisi İçin Yazan

Abdulmecid Bahâtî