SİBER VATAN VE SAVUNMA ULUSAL ÇALIŞTAYI

31 EKİM 2022 • Pazartesi

09.00 - 17.30

ATO MECLİS SALONU
Söğütözü Mahallesi
2176. Cadde No: 1/1
06530 Çankaya/ANKARA

ÇALIŞTAY DÖKÜMLERİ KİTABI

SİBER VATAN ve SAVUNMA ULUSAL ÇALIŞTAYI

e-kitap

DÜZENLEYİCİLER

ELEKTRİK MÜHENDİSLERİ ODASI • TMMOB • 1954 • ANKARA ŞUBESİ

ato Ankara Ticaret Odası

SPONSORLAR

DIWW DRIVE

emc ekare

Labris NETWORKS

ELEKTRİK MÜHENDİSLERİ ODASI ANKARA ŞUBESİ
Ihlamur Caddesi No:10 Kızılay Ankara, Türkiye Telefon: +90 312 231 44 74 Faks: +90 312 232 10 88
ankara.emo.org.tr ankara@emo.org.tr emoankara emoankara emoankara emoankarasubesi emoankarasubesi

31 EKİM 2022

ATO MECLİS SALONU

Söğütözü Mahallesi 2176. Cadde No: 1/1 06530 Çankaya/ANKARA

09.00 - 17.30

SİBER VATAN GÜVENLİĞİ ULUSAL ÇALIŞTAYI

DÜZENLEYİCİLER

ELEKTRİK MÜHENDİSLERİ ODASI • TMMOB • 1954

ANKARA ŞUBESİ

ato Ankara Ticaret Odası

SPONSORLAR

DIWW DRIVE

emc²ekare

Labris NETWORKS

Ihlamur Caddesi No:10 Kızılay Ankara, Türkiye Telefon: +90 312 231 44 74 Faks: +90 312 232 10 88

ankara.emo.org.tr ankara@emo.org.tr emoankara emoankara emoankara emoankarasubesi emoankarasubesi

ANKARA ŞUBESİ

TMMOB
Elektrik Mühendisleri Odası
Ankara Şubesi

SİBER VATAN VE SAVUNMA ULUSAL ÇALIŞTAYI

BANT ÇÖZÜMLERİ

ATO MECLİS SALONU
ANKARA

31.10.2022

E-KİTAP

ISBN:
EMO YAYIN NO:

SİBER VATAN ve SAVUNMA ULUSAL ÇALIŞTAYI

31 EKİM 2022 • Ankara Ticaret Odası Meclis Salonu

PROGRAM

09:00-09:30 | Kayıt

09:30-10:00 | **Açılış Konuşmaları**

Prof. Dr. Şeref Sağıroğlu, EMO Ankara Şubesi Yönetim Kurulu Başkanı

Sn. Gürsel Baran, Ankara Ticaret Odası Yönetim Kurulu Başkanı

Sn. Yavuz Emir Beyribey, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı

Dr. Ömer Fatih Sayan, Ulaştırma ve Altyapı Bakanlığı Bakan Yardımcısı (Tensipleri halinde)

10:00-12:30 | **Siber Vatan, Siber Güvenlik ve Savunma Oturumu - 1**
Oturum Başkanı: Prof. Dr. Şeref Sağıroğlu, EMO Ankara Şubesi Başkanı
10:00-10:30 "Ulusal Siber Olaylara Müdahale Merkezi Çalışmaları"
Onur Aktaş | USOM-BTD Daire Başkanı, BTK
10:30-11:00 "Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Ekosistem Çalışmaları"
Duygu Fidancıoğlu | Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Türkiye Siber Güvenlik Kümelenmesi Genel Koordinatörü / Siber Güvenlik Dairesi Başkanlığı Birim Müdürü
11:00-11:30 "Dijital Vatan Kavramı, Varlıklar ve Sınırlar"
Oğuz Yılmaz | Labris Networks YK Üyesi / EMO Ankara Şubesi Üyesi
11:30-12:00 "Endüstriyel Kontrol ve Enerji Sistemleri, Siber Vatan ve Güvenlik"
Aykut Açıkgöz, EMCEKARE Genel Müdürü / EMO Ankara Şubesi Üyesi
12:00-12:30 "Siber Vatan ve Caydırıcılık"
Dr. Öğretim Üyesi Mustafa Şenol | İstanbul Gelişim Üniversitesi

12.30-13:30 | Öğle Yemeği Arası

13.30-15:00 | **Siber Vatan, Siber Güvenlik ve Savunma Oturumu - 2**
Oturum Başkanı: Taha Yücel, Bilgi Güvenliği Derneği Başkanı / Aselsan Genel Müdür Yardımcısı
13:30-13:50 "Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Yönetişim Çalışmaları"
Yusuf Tancan | Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı Birim Müdürü
13:50-14:10 "Siber Vatan Varlıklarını Koruma ve Güncel Çözümler"
Yusuf Tulgar, Divvy Drive A.Ş. Genel Müdürü
14:10-14:30 "Siber Terörizmle Mücadelede Açık Kaynak İstihbaratı"
Hüseyin Akarslan, 4. Sınıf Emniyet Müdürü, EGM Terörle Mücadele Daire Başkanlığı
14:30-14:50 "Siber Güvenlik Operasyonları"
Mahmut Esat Yıldırım | USOM İleri Güvenlik Operasyon Koordinatörü

14.50-15:30 | Çay Kahve Arası

15.30-17:10 | **Siber Vatan, Siber Güvenlik ve Savunma Oturumu - 3**
Oturum Başkanı: Prof. Dr. Mustafa Alkan, Gazi Üniversitesi Adli Bilişim Ana Bilim Dalı Başkanı / EMO Ankara Şubesi Üyesi
15:30-15:50 "Üniversitelerde Siber Güvenlik ve Savunma",
Doç. Dr. Murat Dener | Gazi Üniversitesi FBE Bilgi Güvenliği ABD Başkanı
15:50-16:10 "Kalkınma Ajansları Siber Vatan Programı"
Kadir Kağan İnanoğlu, Siber Vatan Program Koordinatörü
16:10-16:30 "Başarı Hikâyesi: Bartın Siber Vatan Projesi"
Dr. Öğretim Üyesi Eyüp Burak Ceyhan | Bartın Siber Vatan Proje Koordinatörü
16:30-16:50 "Siber Vatan, Karanlık ve Derin İnternet (Dark ve Deep Web) ve Tehdit Operasyonları - 1"
Mustafa Öztürk | GaziCyber Öğrenci Topluluk Başkanı
16:50-17:10 "Siber Vatan, Karanlık ve Derin İnternet (Dark ve Deep Web) ve Tehdit Operasyonları - 2"
Burak Özlü | GaziCyber Öğrenci Topluluk Başkan Yardımcısı

17.10-17:30 | **Kapanış ve Değerlendirmeler**

ÖNSÖZ

EMO Ankara Şubesi olarak göreve geldiğimizden bugüne kadar, Odamızın itibarını daha da artırmak, üye ilişkilerini geliştirmek, EMO-Genç yapılanmasını güçlendirmek, meslektaşlarımıza daha iyi hizmet vermek, seçimlerde söz verdiğimiz projelerimizi hayata geçirmek, Odamızı uluslararasılaştırmak, sektör-kurum-üniversite işbirliklerini arttırmak, yeni meslek alanları oluşturmak ve Odamızı geleceğe taşımak için çalışmalarımızı ve mücadelemizi sürdürüyor, Meslek Odamızı daha etkin hale getirmek için çaba gösteriyoruz. Barış Ormanı, 100 temel eser üretim ve EMO Mentor gibi projelerimizi hayata geçirmeye başladık. 9 aylık süre içerisinde 3 çalıştay yaptık. 2 ulusal ve 4 uluslararası etkinliği destekledik, davetli konuşmacı olarak katıldık. Üretim tesislerine teknik geziler ile sosyal etkinlikler düzenliyor, haftalık webinarlar yapıyoruz. Üniversitelerimizle ve kurumlarımızla protokoller yaparak işbirliklerimizi artırıyoruz. EMO Ankara Şubesi olarak engellemelere rağmen aksamadan bülten çıkartıyoruz. Yeşil Mutabakat, Elektrikli Araçlar, Blokzincir, Akıllı Şebekeler, 5G, Siber Güvenlik, Yapay Zeka, Büyük Veri, Veri Bilimi, Veri Mahremiyeti, Sanal Gerçeklik, Sanal Kurgu (Metaverse), Dijital İkiz gibi yeni alanlarda etkinlikler düzenliyoruz. Bu yeni alanların Meslek Odamıza kazandırılması ve meslektaşlarımıza bunların aktarılması için çalışıyoruz. Bu etkinliğimiz de bunlardan birisidir.

Siber ortamlardaki tehditler, tehlikeler, açıklıklar, ihlaller, saldırılar, ifşalar hatta savaşlar; geliştirilen politikalara, uygulanan strateji ve eylem planlarına, yapılan denetim ve testlere, faydalanılan çok sayıdaki standarda, kullanılan araç ve gereçlere, yayımlanan rehber ve genelgelere ve alınan önlemlere rağmen her geçen gün artmaktadır. Casus ve kötücül yazılımların verdiği zararlardan fidye yazılımlarına, siber tehdit istihbaratından derin ve karanlık internet tehditlerine, endüstriyel kontrol sistem (SCADA, DCS, PLC, vb.) saldırılarından ileri düzey kalıcı saldırılara (APT), kural tabanlıdan yapay zekâ tabanlı tehdit ve saldırılara, , kritik altyapılardan sosyal mühendislik ve sanal kurgu saldırılarına, elektrik üretim-iletim-dağıtım şebekelerinden akıllı şebekelere, sabotajdan siber casusluğa, siber zorbalıktan siber suçlara, davranış saldırılardan duygu saldırılarına kadar burada verilmeyen pek çok husus her zamankinden daha fazla kişisel, kurumsal ve ulusal tehdit olmaya, oluşturmaya hatta ülke birlik ve bütünlüğünü tehdit etmeye devam etmektedir. Bunların azaltılması veya önlenmesi için "Hatt-ı müdafaa yoktur, sath-ı müdafaa vardır. O satıh bütün siber vatandır" yaklaşımıyla mücadele edilmesi, dijital topraklarımızın veya varlıklarımızın ko-

runması ve sonuçta vatanın siber ortamlarda tüm taraflar ve paydaşlar ile hep birlikte savunulması gereklidir.

Siber güvenliğin önemini hepinizin bildiğini düşünüyorum. Siber ortamlardaki riskler artarken; geliştirilen politikalara, uygulanan strateji ve eylem planlarına, yapılan denetim ve testlere, faydalanılan çok sayıdaki standartlara, kullanılan pek çok teknolojik çözümlere, araç ve gereçlere, yayımlanan rehber ve genelgelere, yapılan ulusal ve uluslararası tatbikatlara, açılan programlara, yapılan akademik yayınlara, üretilen tezlere, önleyici etkinliklere, hatta alınan tüm önlemlere rağmen her geçen gün artmaktadır. Kuantum hesaplama yöntemleri de dikkate alındığında, tehditlerin artarak devam edeceği de ortadadır. Bu yıl içerisinde ülkemizde sağlık, enerji dağıtım ve savunma sektöründe meydana gelen veri sızıntılarının yüzbinleri etkilemesi buna örnek verilebilir. Sonuç olarak her zamankinden daha çok bu konulara ağırlık verilmesi, bu alanda yapılan çalışmaların gerek sayı ve nitelik gerekse yeni çözüm ve yaklaşımların hayata geçirilmesine bağlıdır. Ülkemizde bu konuda önemli çalışmalar yapılmakta, önlemler alınmakta, siber güvenlik ve savunmada ITU Siber Güvenlik İndeksinde üst sıralarda yer alsak ta, akademik olarak üretilen çıktılar, alınan patentler, geliştirilen ürün ve teknolojilerde istenilen seviyelerde olmadığımız, ülke siber güvenlik farkındalığımızın da düşük olduğu ortadadır. Dünyada Web of Science verilerine göre yapılan çalışmalara bakıldığında, sadece siber güvenlik alanında 25.226 akademik yayın olduğu, bilimsel olarak ülkemizin bu alana katkısının ise %1 e yakın olduğu görülmektedir.

Siber saldırıların ve siber suçların sürekli artış gösterdiği, saldırıların zekileştiği, sürekli kalıcı tehditlerin arttığı, ve siber tehdit vektörlerinin boyut değiştirdiği siber dünyayı daha iyi anlamak, önlem almak ve koruyucu tedbirler geliştirmek ve özellikle de siber vatan ve savunmayı tam anlamıyla gerçekleştirmek için yapılan çalışmalara ilave olarak yeni kavram, konsept veya yaklaşımların geliştirilmesine, veri sözlüğü çalışmalarının tamamlanmasına, özellikle de yeni ontolojik çalışmaların yapılması ve paylaşılmasına ihtiyaç vardır.

Bu etkinliğimizin amacı; burada belirttiğim konuları daha kapsamlı tartışmak, üniversite-sektör-kurum uzmanları ile beraber farklı ve yeni çözüm yollarının geliştirilmesine katkılar sağlamak, dijital topraklarımızı veya varlıklarımızı sonuçta siber vatanımızı tüm taraflar veya paydaşlar ile hep birlikte savunmak için durum tespiti yapmak, yeni yaklaşımlar, çözümler ve fikirler geliştirilmesine katkılar sağlamaktır. Bunlara ilave olarak; alan uzmanları, politika geliştiriciler, sektör-kurum-üniversite temsilcileri, araştır-

macılar, öğrenciler ile konuya ilgi duyanları bir araya getirmek; endüstriyel kontrol ve enerji sistemleri özelinde konuyu değerlendirmek; yeni meslek alanları ve denetim açısından konuyu ele almak; büyüyen siber ve derin dünyada karşılaşılan veya karşılaşılabilecek tehdit ve tehlikeleri kısaca riskleri gözden geçirmek; siber vatan, siber güvenlik ve savunma konuları ile çalışmalara etraflıca bakmak; her dijital vatandaşın anlayacağı ve savunmaya katkı vereceği şekilde bir siber vatan tanımının belirlenmesine katkı sunmak; ve sonuçta elde edilen ortak düşünceleri, fikirleri, çıktıları ve tanımları kamuoyu ile paylaşmak kısaca siber vatan savunmasına kısmen de olsa katkılar sağlamaktır.

Elektrik Mühendisleri Odası Ankara Şubesi ve Ankara Ticaret Odası ile ortaklaşa düzenlediğimiz Siber Vatan ve Savunma Ulusal Çalıştayı`nın verimli bir etkinlik olmasını, paydaşlar arası işbirliklerini arttırılmasını ve sonuç ta siber vatan ve savunma çalışmalarına katkılar sunmasını diliyorum. Bu etkinliğimize ev sahipliği yapan ATO`ya ve Başkanımız Sayın Gürsel Baran`a, çalıştayımızın düzenlenmesine destek veren Sn. Halil İbrahim Yılmaz`a, Ulaştırma ve Alt Yapı Bakanlığı Bakan Yardımcısı Dr. Ömer Fatih Sayan`a, BTK Başkanı Ömer Abdullah Karagözoğlu`na, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı Yavuz Emir Beyribey`e, BTK Haberleşme Genel Müdürü Gökhan Evren`e ve etkinliğimize katkı veren tüm kurum, üniversite ve sektör temsilcilerimize ve etkinliğimize sponsor olan EMCEKARE, DIVVY DRIVE ve LABRIS NETWORKS`e, etkinliğimizi destekleyen Cigre Türkiye`ye, Bilgi Güvenliği Derneğine, Elektrik Tesisat Mühendisleri Derneğine, EMO Genç, IEEE Genç, ACM Genç ve özellikle de GaziCyber öğrenci topluluklarımıza, medya kuruluşlarımıza, EMO Ankara YK üyelerimize, ve son olarak en büyük katkıyı veren çok değerli davetli konuşmacılarımıza huzurunuzda teşekkürlerimi ve şükranlarımı sunarım.

Sonuç olarak; Elektrik Mühendisleri Odası Kamu Kurumu niteliğindeki bir Meslek Odası statüsüyle güvenilir ve yetkin bir paydaştır. Her alanda olduğu gibi Siber Vatan ve savunma gibi kritik alanlarda da kamu adına sorumluluğunu yerine getirmekte, yürürlükteki kanun ve yönetmeliklerden gelen görev ve sorumluklarıyla yaptığı projelendirme – kurulum – işletme - belgelendirme - eğitim ve yetkilendirme faaliyetlerinde de siber güvenlik bakış açısını ve katkılarını sektöre, kurumlara ve ülkemize sunmaya devam edecektir. Özellikle de bu gibi çalışmalarla da bundan sonra yeni meslek alanlarının geliştirilmesinde önemli olan bilgi birikimlerini oluşturmaya, üyelerine en üst düzeyde katkı vermeyi sürdürerek hem meslektaşlarına hem de mesleğin gelişimini ve saygınlığını artırmaya devam edecektir.

EMO bünyesinde kapsamlı olarak ele alınan bu çalıştay'da elde edilen tüm çıktıların kurumsal sayfalarımızda, sunumlarıyla, video kayıtlarıyla, ve çıktılar ile paylaşıldığını bir kez daha hatırlatır, emeği geçen tüm paydaşlarımıza, Düzenleme kurulu üyelerimize, YK üyelerimize ve çalışanlarımıza teşekkür ederim.

EMO ailemize yeni melek alanlarının oluşturulmasına katkılar sağlaması dileğimizdir.

Saygılarımla.

Prof. Dr. Şeref Sağıroğlu

EMO Ankara Şubesi 26. Dönem Yönetim Kurulu Başkanı

SİBER VATAN VE SAVUNMA ULUSAL ÇALIŞTAYI

31.10.2022

SUNUCU- Sayın Bakanım, değerli protokol, kıymetli misafirler; Elektrik Mühendisleri Odası Ankara Şubesi ve Ankara Ticaret Odasının ortaklaşa düzenlediği Siber Vatan ve Savunma Ulusal Çalıştayına hepiniz hoş geldiniz, şeref verdiniz.

Programımıza başlamadan önce Ulu Önder Atatürk ve tüm aziz şehitlerimiz adına sizleri saygı duruşuna, ardından İstiklal Marşımızı okumaya davet ediyorum.

(Saygı Duruşu ve İstiklal Marşı)

Değerli misafirler; açılış konuşmalarını yapmak üzere Elektrik Mühendisleri Odası Ankara Şube Başkanı Prof. Dr. Sayın Şeref Sarıoğlu'nu kürsüye davet ediyorum. (Alkışlar)

Prof. Dr. ŞEREF SARIOĞLU (EMO Ankara Şubesi Yönetim Kurulu Başkanı)- Çok değerli Bakan Yardımcım, değerli başkanlarım, sayın müdürlerim, çok değerli katılımcılar, sevgili öğrenciler; Elektrik Mühendisleri Odası Ankara Şubesi Yönetim Kurulu adına hepinizi saygıyla selamlıyorum. Elektrik Mühendisleri Odası ve Ankara Ticaret Odası olarak beraber üstlenmiş olduğumuz bu etkinliğe hepiniz hoş geldiniz, şeref verdiniz.

Programımız biraz geciktiği için bazı noktalara temas etmeyeceğim, panelistlerimizin bunları konuşacağını düşünüyorum. Ama müsaadenizle bazı önemli hususları burada sizinle paylaşmak istiyorum.

Değerli katılımcılar; siber güvenliğin önemini hepinizin bildiğini düşünüyorum. Siber ortamlardaki tehditler, tehlikeler, açıklıklar, ihlaller, saldırılar, ifşalar, hatta savaşlar; geliştirilen politikalara, uygulanan strateji ve eylem planlarına, yapılan denetim ve testlere, faydalanılan çok sayıdaki standarda, kullanılan araç ve gereçlere, yayımlanan rehber ve genelgelere, yapılan ulusal ve uluslararası tatbikatlara, açılan programlara, yapılan akademik yayınlara, üretilen tezlere, önleyici etkinliklere, hatta alınan tüm önlemlere rağmen her geçen gün artmaktadır.

Kuantum hesaplama yöntemleri de dikkate alındığında, tehditlerin artarak devam edeceği de ortadadır. Bu yıl içerisinde ülkemizde sağlık, enerji da-

ğıtım ve savunma sektöründe meydana gelen bazı veri sıkıntılarının pek çok kişiyi etkilediği buna örnek verilebilir.

Sonuç olarak; her zamankinden daha çok bu konulara ağırlık verilmesi, bu alanda yapılan çalışmaların gerek sayı, gerek nitelik, gerekse yeni çözüm ve yaklaşımların hayata geçirilmesi gerekmektedir.

Ülkemizde bu konuda önemli çalışmalar yapılmakta, önlemler alınmakta, siber güvenlik ve savunmada Uluslararası Telekomünikasyon Birliği ITU'nun küresel siber güvenlik endeksinde üst sıralarda yer almamıza karşın; akademik olarak üretilen çıktılar, alınan patentler, geliştirilen ürün ve teknolojilerde istenilen seviyede olmadığımız, ülke siber güvenlik farkındalığımızın da düşük olduğu ortadadır.

Dünyada Web of Science verilerine göre yapılan çalışmalara bakıldığında, sadece siber güvenlik alanında 25 binin üzerinde akademik çalışma olduğu bilinmektedir. Ülkemizin bu alana katkısı ise yüzde 1'in altındadır. Dolayısıyla, siber saldırıların ve siber suçların sürekli artış gösterdiği, saldırıların zekileştiği, tehditlerin arttığı ve tehdit büyüklüğünün boyut değiştirdiği günümüzde, dünyayı daha iyi anlamak, önlem almak ve koruyucu tedbirler geliştirmek, özellikle de siber vatan ve siber savunmayı tam anlamıyla gerçekleştirmek için yapılan çalışmalara ilave olarak, yeni kavram, konsept ve yaklaşımların geliştirilmesine, özellikle de yeni ontolojik çalışmaların yapılmasına ve paylaşılmasına ihtiyaç olduğu ortadadır.

Bu etkinliğimizin amacı da, burada belirttiğim konuları daha kapsamlı tartışmak, üniversite-sektör-kurum uzmanlarıyla beraber farklı ve yeni çözüm yollarının geliştirilmesine katkılar sağlamak, dijital topraklarımızı ve varlıklarımızı, sonuçta siber vatanımızı tüm taraflar veya paydaşlarla beraber savunmak, durum tespiti yapmak, yeni yaklaşımlar, çözümler, fikirler geliştirilmesine katkılar sağlamaktır.

Bu etkinliğimize ev sahipliği yapan Ankara Ticaret Odası Başkanımız Sayın

Gürsel Baran Bey'e, çalıştayımızın düzenlenmesine destek veren, bu fikrin olgunlaşmasına katkı veren Yasın Halil İbrahim Yılmaz Bey'e, tabii ki buradaki önemli kurumlarımıza, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığımıza, Bilgi Teknolojileri İletişim Kurumumuza ve etkinliğimize katkı veren diğer kurum-üniversite-sektör temsilcilerimize teşekkür ederim.

Tabii ki bu etkinliğimize sponsor olan EMCEKARE, DivvyDrive ve Labris Networks'a da özel bir teşekkür sunmak istiyoruz. Ayrıca, bu etkinliğimizi destekleyen CIGRE Türkiye, Bilgi Güvenliği Derneği, Elektrik Tesisat Mühendisleri Derneği, EMO Genç, IEE Genç, ACM Genç ve Gazi Cyber'a, öğrenci topluluklarımıza da buradan teşekkür etmek istiyorum.

Yönetim Kurulu üyelerine, Düzenleme Kurulu üyelerine ve özellikle de bu etkinliğimizin başkan yardımcılığını yapan Hatice Bilge Algın Hanımefendi'ye teşekkür ederim.

Son olarak, bizleri kırmayarak gelen, davetimizi kabul eden değerli konuşmacılarımıza da huzurlarınızda teşekkür eder, şükranlarımı sunarım.

Elektrik Mühendisleri Odası Ankara Şubesi ve Ankara Ticaret Odası olarak ortaklaşa düzenlemiş olduğumuz Siber Vatan ve Savunma Çalıştayının verimli bir etkinlik olmasını, paydaşlar arası işbirliklerini arttırmasını ve sonuçta da tabii ki siber vatan ve savunmamıza katkılar sağlamasını diler, hepinize katılım ve katkılarınız için teşekkür ederim, saygılar sunarım. (Alkışlar)

SUNUCU- Ankara Şube Başkanımıza konuşmalarından dolayı çok teşekkür ediyoruz.

Sayın Bakanım, kıymetli misafirler; şimdi de konuşmalarını yapmak üzere Ankara Ticaret Odası Yönetim Kurulu Başkanı Sayın Gürsel Baran'ı kürsüye davet ediyorum. (Alkışlar)

GÜRSEL BARAN (ATO Yönetim Kurulu Başkanı)- Sayın Bakanım, Sayın Vekilim, Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin çok kıymetli Başkan Yardımcısı, Elektrik Mühendisleri Odasının çok kıymetli Ankara Şube Başkanı, çok kıymetli misafirler, değerli konuklar; Ankara Ticaret Odası ve Elektrik Mühendisleri Odası Ankara Şubesi olarak ortaklaşa düzenlediğimiz Siber Vatan ve Savunma Ulusal Çalıştayına hoş geldiniz. Faydalı olacağına yürekten inandığım böyle bir toplantıya ev sahipliği yapmaktan dolayı çok mutlu olduğumu ifade etmek isterim.

Siber vatan kavramı, son yıllarda adını sıkça duymaya başladığımız gerçekten önemli bir konu. Bilgi ve iletişim teknolojilerindeki gelişmeler hayatın

her alanını derinden etkiliyor. Devletlerin güvenlik politikaları da değişen dünyayla birlikte dönüşüme uğruyor. Vatan savunmasının karşılığının bu değişimle birlikte geliştiğini ve genişlediğini görüyoruz. Önceden vatan savunması denildiğinde aklımıza toprak bütünlüğü, kara, hava ve deniz sınırlarımız geliyordu. Oysa şimdi dijital dünyada da sınırlarımız olduğunun ve bunu da korumamız gerektiğinin farkındayız. Egemenlik ve bağımsızlığımız için, tıpkı gerçek dünyada olduğu gibi, dijital dünyada da savunmayı sağlamak durumundayız.

Vatan sınırı tanımıyla birlikte savunma araçları da farklılaştı. Bundan 100 yıl önce tankla, topla, tüfekle, süngüyle vatan savunulabiliyorken, bugün topyekûn savunma için bilgisayar, kodlar, yazılımlar ve adını sayamadığımız nice şeyler devrede.

İnternet ve bilgisayar birbirine bağlanabildiğinden bu yana verilerimiz de dijital ortama taşındı. Kişisel bilgilerimiz, bankacılık işlemleri, tapular, vergiler, faturalar, reçeteler, hemen her şeye artık dijital dünyadan ulaşabiliyoruz. Önceleri evlerimizde, kasalarda, sandıklarda sakladığımız önemli evraklar, kamu binaları önünde almak için sıra beklediğimiz belgeler bir tıkla bilgisayarımıza indirilebiliyor. Dijital dünyadaki dönüşüm ve gelişimin hızına yetişmek mümkün değil, tam bir gelişmeye ayak uyduracakken yenileri devreye giriyor.

Hatırlayacaksınız, Rusya-Ukrayna Savaşı, enerji krizi konuları gündeme gelmeden önce Metaverse dünyanın gündeminde en üst sıradaydı. Metaverse dünyasında ev-arsa alanlar, mağaza açanlar hemen her gün haberlere konu oluyordu. Şu anda ülkelerin içinde bulunduğu durum, koşullar, doğalgaz ve elektrik başta olmak üzere hammadde tedarikinde yaşanan sıkıntılar nedeniyle, her ne kadar eskisi kadar gündemde olmasa da bu evrendeki çalışmaların devam ettiğini ve bundan sonra da devam edeceğini hepimiz biliyoruz.

Değerli konuklar; insanları bireysel olarak ilgilendiren siber dünya, yaşanan gelişmeler sonucunda ülkeleri de yakından ilgilendiren bir mecra haline geldi. Dijital mahremiyete yönelik tehdit algısı sadece insanların değil, ülkelerin de sorunu oldu. Az evvel ifade ettiğim gibi, vatan savunması eskiden tüfekle-süngüyle yapılırken, sınırları belirli bir coğrafyayı koruma anlayışı varken, bu yeni siber dünyada sınırlarınız çok daha geniş, savaş aletiniz de tahmin edemeyeceğiniz kadar çok.

Bu yeni dünya avantajlarıyla insanoğluna hizmet ederek hayatı kolaylaştırırken, yeni kavram ve tehditlerle de karşımızda duruyor. Böylece siber

dünyada siber vatan savunması gündeme geliyor. Yani ülke çıkarlarını sanal ortamda koruyabilmek, bunun için önlemler almak, savunmak için ihtiyaç duyulan teknik ve donanıma sahip olmak ve gerekirse saldırı stratejilerini belirlemek.

Ankara Ticaret Odası olarak, pandemi sürecinde biz de Odamızda dijital dönüşüm çalışmalarına hız verdik. 1923 yılında kurulan Odamız, o günden bu yana arşivimizde yer alan tüm evraklarımızı yok olma riskine karşı dijital ortama taşıdık. Bu sürecin yanı sıra tüm hizmet verdiğimiz evrakların önemli bir kısmını dijital ortama taşıdığımız ATONET Üye Hizmet Platformunu da hayata geçirdik.

Ticaret de dijitalleşiyor ve ticarete dair birçok bilgi dijital ortama aktarılıyor. Kamu kurumlarıyla entegre çalışmalar da yürütülüyor. Siber vatan, siber güvenlik konuları ticaret dünyasını da yakından ilgilendiriyor. Ankara Ticaret Odası olarak, Elektrik Mühendisleri Odası Ankara Şubesiyle birlikte bu çok önemli memleket meselesini mercek altına almaktan büyük bir memnuniyet duyuyoruz.

Elektrik Mühendisleri Odası zaten teknik ve güncel konulara bilimsel bakış açısıyla yaklaşmak konusunda çok deneyimli bir oda. Ankara Şube Başkanı Prof. Dr. Sayın Şeref Sağıroğlu, gerek bilim insanı kimliğiyle, gerek kamu kurumu niteliğinde bir meslek kuruluşu yöneticisi vasfıyla siber vatan kavramını en ince detayıyla açıklayan ve konuya dikkat çeken bir kişi oldu. Kendisini kutluyorum.

Kamu kurumu niteliğinde meslek kuruluşları olarak odalar, bir yandan kamu adına görev yürütürken; diğer yandan sivil toplum kuruluşu olarak, ele alınması ve tartışılması gereken konuları gündeme getiren, tarafların bir araya gelerek görüş bildirmesini sağlayan ve uzlaşma kültürünü ortaya koyan başarılı örnekler sergiliyorlar.

Hepinizin bildiği gibi, savunma temelli sporlarda oyuncu yetiştirirken,

"Şartlar seni zorlamadan sen şartları zorlayacaksın" öğüdünü verirler. Yani sen kendini geliştirmeye zorlamazsan, şartlar seni daha fazla zorlayarak geliştirir. Bu söz, bugünün gündemi olan siber güvenlik konusu için de söylenebilir. Siber vatana herhangi bir tehdit yokken savunma stratejisi geliştirmezseniz, şartlar sizi üzerek geliştirmeye zorlar. Bugün burada siber güvenlik konusunun detaylarıyla ele alınması, şartlar zorlamadan gelişimin en güzel örneğini oluşturuyor.

Ben daha fazla vaktinizi almadan konuşmamı sonlandırmak istiyorum. Burada ele alınacak detayların ülkemizin siber güvenliği konusunda yeni perspektifler ortaya koyacağı inancıyla, sizleri yeniden, sevgi, saygı ve hürmetle selamlıyorum. (Alkışlar)

SUNUCU- Sayın Başkana bu değerli konuşmalarından dolayı çok teşekkür ediyoruz.

Şimdi de konuşmalarını yapmak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı Sayın Yavuz Emir Beyribey'i kürsüye davet ediyorum. (Alkışlar)

YAVUZ EMİR BEYRİBEY (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı)- Sayın Bakan Yardımcım, saygıdeğer başkanlarım, sektörümüzün kıymetli temsilcileri, saygıdeğer misafirler; Siber Vatan ve Savunma Ulusal Çalıştayının düzenlenmesinde emeği geçen herkese şükranlarımı sunuyorum.

Malumunuz, ekim ayının son günündeyiz. Ekim ayı, 2004'te Amerika Birleşik Devletleri'nin başlattığı hayırlı bir iş, siber güvenlik farkındalık ayı olarak belirlenmiş, bizim gibi birçok ülkede de bu kabul görmüş. İnşallah bugün burada yer alan değerli misafirlerimiz, "Dijital topraklarımızın güvenliği için daha neler yapmalıyım?" farkındalığıyla buradan ayrılırlar diye şimdiden diliyorum.

Saygıdeğer katılımcılar; ülkeleri sadece coğrafi sınırları içindeki toprakları, toprakları, karasuları veya hava sahaları temsil etmiyor; ...mızın çalışmasını sağlayan bilişim sistemleri, dijital kimliklerimiz, telekomünikasyon ağımız, dijitalleşmeyi sağlayan tüm yapılar ve buradan üretilen, hatta bunu besleyen kritik veri veya tüm verileri kastediyorum, aslında bunların tamamı dijital ülkeleri oluşturuyor ve siber uzayın bir parçası haline geliyor.

Dijital dünyanın sınırları yok. Evrenin de sınırı yok. Fiziksel mesafelerin siber saldırılarda herhangi bir anlamı da yok. Siz sakin sakin kurumunuzda, şirketinizde oturup çayınızı-kahvenizi yudumlarken, dünyanın öteki ucundan

bir saldırgan bir anda Wi-Fi üzerinden saldırı yapabiliyor, zarar verebiliyor, enerji kesintilerine sebebiyet verebiliyor veya bir anda trafiği tıkayabiliyor. Saldırgan kim, nerede, nasıl ulaşırız, bunun cevabı da yok. Siber güvenliğin zihinlerimize bu şekilde yerleşmesini bekliyoruz. Asker yok, silah yok, bomba yok, füze yok; siber savaşlarda artık saldırılar sessiz. Ülkelerin artık başta gelen savaş mühimmatı, hedefli zararlı yazılımlar, servis dışı bırakma saldırıları, dezenformasyon ... ve bunun gibi şeyler, liste uzayıp gidiyor. Yüzyıllardır süregelen savaşlar artık dijital dünyada yeni yüzüyle de devam ediyor. Siber uzay artık beşinci savaş ortamı olarak ülkeler için ulusal güvenliğin ayrılmaz ve en önemli bileşeni haline yavaş yavaş dönüşüyor.

Değerli misafirler; dünyanın en iyi savaş teorisyenlerinden biri, eski bir general der ki, "En iyi strateji savaşmadan kazanmaktır." Peki, savaşmadan kazanmak mümkün mü? Geçtiğimiz günlerde, siz de takip etmişsinizdir belki, Arnavutluk, İran'ı siber saldırılarla suçlayarak, tüm İranlı diplomatların 24 saat içerisinde ülkeyi terk etmelerini istedi. Görülüyor ki, diplomatik ilişkilerin tamamen kesilmesi kararını aldıracak kadar kritik, hayati düzeyde bir saldırı yaşanmış. Yine şubat ayından itibaren bütün dünyayı etkileyen Ukrayna-Rusya Savaşında da benzer durumlara şahit olduk.

Kıymetli katılımcılar; geleceğin teknolojileri, geleceğe yönelik güvenlik bakış açılarını kökten değiştirmiş durumda. Güvenliği biraz kısaltacağım, konuşmamı biraz hızlandıracağım. Eskiden normal saldırgan seviyesinde olan şeyler artık devletler düzeyinde yapılan siber saldırılar haline dönüştü. Yeni teknolojilerin gelmesiyle beraber biz bunlara karşı savunma yapacağız, etki gücümüzü arttıracağız diyoruz. Ama yeni teknolojiler ne yazık ki saldırganların da elini kolaylaştırıyor. Bunlardan en önemlisi yapay zekâ. Yapay zekâ, güvenlik konusunda ne tür yıkıcı etkiler oluşturacak, bunu henüz bilmiyoruz. Yeni nesil teknolojilerle beraber artık saldırılar da kolay hale geliyor. Siber saldırılara karşı geliştirilen birçok farklı sistem var; ama biz hacker'ların insan olduğunu farz ediyoruz ve savunmamızı buna göre kuruyoruz. Bunun çıktısı olarak da, uzun vadede biz konvansiyonel şekilde

ilerlemeye devam ederse, ne yazık ki, siber savunmamızı tam anlamıyla sağlamış olamayacağız. Düşünelim, daha önce insan-makine etkileşimi vardı, sonra makine öğrenmesi geldi. Bulutu takip ediyorsunuz, bulut başını aldı gidiyor; bulut altyapısında artık makineler insan gibi. Makinelerin birbiriyle etkileşiminde saldırgan da makine, savunma da makine haline dönüşecek. Bu, hepimizin gelecekte, 3-5 sene sonra karşılaşacağı bir şey. Artık saldırganlar da yapay zekâ olacak, savunma da yapay zekâ olacak.

Şöyle ki: Sosyal medyayı takip ediyorsunuz. Bot hesaplar var. Bot hesaplar yapay zekâ temelli, insanı taklit ediyor. Bunu engellemek için sosyal medya şirketleri ne yapıyor? Yine yapay zekâ temelli çözümler üretiyor. Yani aslında problemi üreten şeyin çözümü de kendi içinde saklı.

Nihayetinde biz bu tür tehditler karşısında öyle güçlü bir siber güvenlik yapılanması kurmalıyız ki kimse bize saldırmaya cesaret edemesin. Bu da bizi uluslararası arenada güçlü bir siber devlet konumuna ve aynı zamanda caydırıcı bir güç haline getirecektir. Aslında büyük resim bu. Peki, resimdeki detaylara biraz yakından bakalım.

Güçlü siber devleti nasıl sağlarız? Askeri ve politik kurumları yanında devletin tüm kurumlarının bir koordinasyon içinde çalışmasıyla biz mukavemet sağlayabiliriz. Koordinasyon ve işbirliği kaslarının, net görev ve sorumluluklarla, kurumların birbirleri arasındaki ilişkilerin açık ve belirgin tanımlanmasıyla güçleneceği de bu anlamda aşikârdır.

Savunma gücümüzün artması, siber gücün anahtarıdır. Düşmanı ve kendinizi iyi biliyorsanız, yüzlerce savaşa girseniz bile sonucundan emin olursunuz; kaybedeceğinizi de bilirsiniz, kazanacağınızı da bilirsiniz. Siber güç hale gelmek için etkin bir siber teknik istihbarat altyapısı ve hatta her safhada proaktif bir yaklaşım gerekir. Bilmek yeterli mi peki? Ürettiğiniz, satın aldığınız, kullandığınız bütün teknolojiye, edindiğiniz bütün bilgiye hâkim olmalısınız.

Kıymetli konuklar; güçlü Türkiye yolunda tüm kurumlarımızla koordineli olarak Türkiye'nin siber güvenlik gücünü arttırmak hedefine emin adımlarla ilerliyoruz. Dijital Dönüşüm Ofisi Başkanlığı, kurulduğu tarihten bugüne dek Türkiye'nin kritik altyapılarının güvenliğinin arttırılması, kamuda dijital dönüşümün sağlanması, siber güvenlik kapasitesinin arttırılması, ekosistemin geliştirilmesi gibi pek çok alanda birçok proje yaptı, geliştirdi ve geliştirmeye devam ediyor. Nihayetinde hepimiz bu gelen dev dalganın, tsunami dalgasının karşısında durmaya çalışıyoruz. Bu manada dijital altyapımızın korunmasıyla ilgili güçlü dalgakıranlar inşa etmek zorundayız.

Sözlerime son verirken şunu belirtmek isterim ki, kurumlardan bireylere tüm katmanlarda topyekûn ve koordineli, ekosistemin tüm paydaşlarıyla birlikte, hep beraber ve bir olmalıyız. Unutmamalıyız ki, bir olmadan lider veya birinci olmak şansımız yoktur.

Bu vesileyle, çalıştayın düzenlenmesinde emeği geçen herkese tekrar teşekkür ediyorum. Etkinliğin verimli geçmesini diliyor, hepinizi saygıyla selamlıyorum. (Alkışlar)

SUNUCU- Sayın Beyribey'e çok teşekkür ediyoruz.

Değerli misafirler; şimdi de konuşmalarını yapmak üzere Ulaştırma ve Altyapı Bakanlığı Bakan Yardımcısı Dr. Sayın Ömer Fatih Sayan'ı kürsüye davet ediyorum. (Alkışlar)

ÖMER FATİH SAYAN (Ulaştırma ve Altyapı Bakan Yardımcısı)- Sayın Başkanım, değerli misafirler, sayın basın mensupları, kıymetli katılımcılar ve genç arkadaşlarım; öncelikle, içinde bulunduğumuz ve yüzyılın en önemli kişisel ve toplumsal güvenlik risklerinden olan siber güvenlik konusuna yoğunlaşacağımız Siber Vatan ve Savunma Ulusal Çalıştayının düzenlenmesinde emeği geçen Elektrik Mühendisleri Odası Ankara Şubesi ve Ankara Ticaret Odasına teşekkür ediyor, bu önemli organizasyonda sizlerle bir araya gelmekten büyük mutluluk duyduğumu belirtmek istiyorum.

Kıymetli katılımcılar; gerek EMO Ankara Şubesinin, gerek ATO'nun kucaklayıcı bir anlayışla, siber güvenlik konusunda Siber Vatan ve Savunma Ulusal Çalıştayını düzenlemesi, birçok diğer kuruluşumuza örnek olması açısından önemli.

Biliyorsunuz, günümüzde bilgi iletişim teknolojileri hayatımızın adeta her alanına girmiş durumda. Küresel internet kullanıcı sayısı 5 milyara ulaştı. Bu, dünya nüfusunun yüzde 63'ünü oluşturuyor. Tabii, her geçen gün sürekli ilerleyen bir şekilde siber güvenlik tehditlerine de maruz kalıyoruz. İnsanlık tarihinde bilgi iletimi hiçbir zaman bugünkü kadar hızlı olmadı. Sıkça şu örnek verilir: İnsanlık tarihinin tamamı kadar sürede elde edilen veri miktarı kadar verinin sadece geçtiğimiz yıl içerisinde üretilmesi gibi bir durum söz konusu.

İnternet ve internete bağlı teknolojilerin son 20 yılda birçok alanda farklı şekilde kullanıldığını; kurumların, bireylerin bilgi iletişim teknolojilerine ihtiyacının oldukça arttığını görüyoruz. Bugün artık dijital dönüşüm dediğimiz olgu bir seçim ya da tercih değil, adeta bir zorunluluk, hepimizin maruz kaldığı ya da işlerini kolaylaştırdığı bir zorunluluk. Bu teknolojilerin

de güçlü altyapılarla mümkün olduğunu biliyoruz ve bugüne kadar yapmış olduğumuz doğru ve yerinde yatırımlarla; karada, denizde, havada, uzayda güçlü ve alternatif altyapılarımızla bu gelişmeleri destekleyecek kapasiteye ulaşıyoruz. Ulaştırma-Altyapı Bakanlığı olarak, ilgili tüm kurumlarla birlikte bunu yapıyoruz. Dijital Dönüşüm Ofisimiz, Sanayi Teknoloji Bakanlığımız, Savunma Sanayi Başkanlığımız, Bilgi Teknolojileri İletişim Kurumu, bütüncül bir şekilde konuya yaklaşarak hep birlikte çalışmalar yapmakta, işin kalbi durumunda da Ulusal Siber Olaylara Müdahale Merkezimiz bulunmakta ve 7/24 esasına göre çalışmalarını yapmaktadır.Ülkemizdeki duruma bakacak olursak; 89.5 milyon geniş bant internet abonesi bulunuyor ve teknolojik gelişmelerle birlikte, gerek kamu, gerek özel sektör faaliyetlerini her geçen gün daha fazla bu ortama taşıyor. Bugüne kadar haberleşme deyince daha çok insanların arasındaki haberleşmeden söz ediliyordu; ama önümüzdeki 3-5 seneye baktığımız zaman, insanlar arasındaki haberleşme bütün haberleşmelerin yüzde 10'u civarında kalacak, diğer kısmı makineler arasında olacak, daha doğrusu her şeyin her şeyle haberleştiği bir dünya olacak.

Küresel boyutta gerçekleşen siber saldırılara baktığımızda, 2022 yılının ilk 3 ayında kaydedilen saldırı sayısı ilk kez 1 milyonu aştı. Dünya Ekonomik Forumunun rakamlarına baktığımız zaman, 2022 küresel risk raporuna göre, siber saldırılar, iklim değişikliği ve kısa süre önce yaşamış olduğumuz salgın benzeri salgınlardan sonra en büyük küresel risklerden bir tanesini oluşturmakta. Yani üçüncü büyük küresel risk siber saldırılar ve araştırmalara göre her 11 saniyede bir siber saldırı gerçekleşmekte.

Siber saldırıların amacı maddi çıkar temininin de ötesine geçti ve adeta bir ülkenin, şehrin altyapısını çökertmek; hastane, su, elektrik, trafik sistemleri gibi hayati yapıları da işlemez hale getirip, ülkelerin itibarını zedelemek gibi sonuçları da olmakta.

Avrupa Ağ ve Bilgi Güvenliği Ajansı ENISA tarafından yayınlanan rapora göre, kritik altyapıların hedeflenmesinde artış gözlenmekte; gerçekleştirilen saldırılarda sağlık, ulaşım, enerji sektörlerinin ana hedef olarak seçildiği belirtilmekte.

Biliyorsunuz, biz, Ulaştırma ve Altyapı Bakanlığı olarak, başta ulaşım sistemleri olmak üzere, ulaşımın her boyutunda dijitalleşmeyi destekliyoruz. Geçtiğimiz cumartesi günü, Sayın Cumhurbaşkanımızın önderliğinde, yerli-milli akıllı cihazımızın fabrika açılışını, ilk banttan inme törenini Cumhuriyetimizin 99. yılını kutlarken yaptık.

Günümüzde otomobilden ev eşyasına kadar her türlü nesne artık internete

bağlı ve bu anlamda siber güvenlikle de ilişkili. Özellikle yerliliğin öneminin bu kadar öne çıktığı bir zamanda siber güvenlik alanında da yerlilik ve millilik noktasında çalışmalar sürdürdüğümüzü ve orada da Savunma Sanayi Başkanlığımız, Dijital Dönüşüm Ofisimiz ve Sanayi Teknoloji Bakanlığımızla birlikte, bir konsorsiyum halinde bu yerlilik-millilik çalışmalarını da yürüttüğümüzü belirtmek istiyorum.

Siber saldırılara ilişkin en ilginç bilgi, esasında bu saldırıları gerçekleştiren kişilerin yüzde 70'inin dışarıdaki, kalan yüzde 30'unun ise içerideki kişilerden oluşması. Bir başka deyişle, ortalama her 3 siber saldırıdan bir tanesi, saldırıya uğrayan yapıyla bağlantılı kişiler tarafından gerçekleşiyor. Buna da artık içimizdeki İrlandalılar mı dersiniz, içimizdeki hainler mi dersiniz, nasıl derseniz. Bu anlamda kendi iç eğitimimize, kurumlarımızın kendi eğitimlerine de daha önem vermesi gerektiği bir kez daha ortaya çıkıyor.

Kıymetli katılımcılar; biz, siber güvenliği ulusal güvenlik meselesi olarak görüyoruz. Siber güvenlik, doğası gereği, teknik, sosyal, hukuksal bakış açılarıyla çok yönlü olarak ele alınması gereken bir konu. Bu nedenle, siber güvenliğin sağlanmasında gerek uluslararası düzeyde, gerekse ulusal çapta işbirlikleri ve koordineli çalışmalar hayati önem arz ediyor. Biraz önce söylediğim gibi, 2013 yılında Bilgi Teknolojileri İletişim Kurumu bünyesinde Ulusal Siber Olaylara Müdahale Merkezini kurduk, 7/24 orada çalışmalar yürütüyoruz. Siber olaylara müdahale ekiplerinin sayısı 2100'ü aştı ve USOM ile birlikte çalışan siber güvenlik uzmanlarının sayısı ise 6500'e ulaştı. Tamamıyla yerli-milli imkânları kullanıyoruz orada. Yerli-milli yazılım olarak Avcı, Atmaca, Kasırga, Akıncı, Kule gibi projelerimizle siber sahayı koruyoruz. Sadece Kasırga projesiyle 16.7 milyon IP adresine zafiyet taraması yaparken, Atmaca projemizle 726 adet farklı zafiyetin ülke genelinde tespit edilmesi ve raporlaması yapılıyor. Bütün bunlar ülkemizi siber güvenlikte daha da güçlendirmek için yürüttüğümüz çalışmalar. Biliyorsunuz, ITU bizim kurucu üyesi olduğumuz Uluslararası Telekomünikasyon Birliği ve siber güvenlik endeksini her yıl

yayınlıyor. ITU tarafından en son yayınlanan siber güvenlik endeksi verilerine göre, ülkemiz, 200'e yakın ülkenin yer aldığı bu endekste, dünyada 11. sırada, Avrupa'da da 6. sıraya yükselmiş durumda. Yeter mi? Yetmez. Siber güvenlikte çokça bilinen bir kavram var; mümkün olan en zor ... bir tanesi olacaksınız. Yani biz ödevimizi sonuna kadar yapacağız, ondan sonra da saldırı geldiği zaman ona karşı koyabilmeyle ilgili de çalışmalarımızı yapmış olacağız.

Yine ITU ile ilgili şunu söyleyeyim: Biliyorsunuz, geçtiğimiz ay ITU'nun yönetim seviyesinde 193 üye ülkeden 48 üyeli seçimle belirlenen konseyde etkin bir şekilde yer alıyoruz ve buraya Avrupa bölgesinden bir kez daha, 22 ülkenin oyuyla altıncı kez seçilmiş olduk. Bu noktada da ITU'daki başarılı serüvenimize destek veren tüm paydaşlarımıza burada, sizlerin huzurunda bir kez daha teşekkür etmek istiyorum.

Kıymetli misafirler; siber güvenlikten sorumlu kurumlar ve kişiler olarak yetkinliklerimizi her zaman bir üst noktaya taşımamız önem arz ediyor. Teorik ve teknik bilgileri uygulamaya ve pratiğe döktüğümüz tatbikatlar, siber güvenlik olgunluğumuzu ölçmek, güçlü ve zayıf yanlarımızı tespit etmek için bize çok önemli fırsatlar sunuyor. Biz de, bu anlamda, geçtiğimiz yıl, ikisi büyük olmak üzere, birçok tatbikat gerçekleştirdik. Farklı kurumlarımızın da tatbikatları gerçekleşiyor. Burada değerli gençlerimiz var, buralara onların katılımını önemsediğimizi bir kez daha hatırlatmak istiyorum.

Siber alanda yetişmiş insan kaynağı ülkemiz için en önemli zenginlik. Biliyorsunuz, bu alanda uzman ihtiyacının karşılanması amacıyla, gençlerimize yönelik, "Siber Yıldız Bayrağı Yapın" yarışmalarıyla genç yeteneklerimizin keşfi noktasında çalışmalarımıza devam ediyoruz. Buralarda başarılı olan arkadaşlarımıza Siber Yıldız Fetih, Siber Talimhane diye adlandırdığımız programla siber güvenlikte laboratuar eğitimi yapıyoruz.

Sayın Cumhurbaşkanımızın çizmiş olduğu Milli Teknoloji Hamlesi Vizyonu çerçevesinde, insan kaynağına yapılan yatırımın en değerli yatırım olduğu inancıyla eğitim çalışmalarımızı da sürdürüyoruz. Biliyorsunuz, BTK Akademi'de 1 milyon kullanıcıyı hedeflemiştik, geçtiğimiz günlerde 1 milyonuncu kullanıcı da sisteme dâhil oldu. Online ve tamamıyla ücretsiz olan bu eğitimlere burada katılmayan arkadaşlarımız varsa onları da bekliyoruz.

BTK Akademi aktif katılımcısı kimler var diye sorsam, bu salonda hiç de küçümsenmeyecek bir rakam olduğunu görmekten dolayı memnuniyet duyduğumu da bir kez daha belirtmek istiyorum.

Bilgi ve iletişim alanında, insanımızın hayatını kolaylaştıran, refahına katkı

sağlayan her tür çalışmada, bizler, tüm paydaşlarımızla birlikte, her gün daha güçlü bir motivasyonla yer alıyoruz. Amacımız, ülkemizi her alanda daha da ileriye taşımak. Gerçekleştirilen bu önemli çalıştayın da siber güvenlik konusunda önemli çıktıları olacağına ve paydaşlarımızla işbirliğimize de önemli katkılar sağlayacağına inanıyorum. EMO Ankara Şubesine bu çalıştayın düzenlenmesinde etkin bir rol üstlendiği için teşekkür ediyorum. EMO Ankara Şubesi, bu sene başından beri çok daha farklı bir yönetim tarzıyla, ciddi anlamda, hem üyelerini, hem de ülkemizin elektronik ve elektrik noktasında sahip olduğu tüm kaynakları en iyi şekilde nasıl kullanırız arayışı içerisinde birçok çalışmalar yapıyor. Ben ilk defa Şubenin düzenlemiş olduğu bir programa katıldım. Bu değerli hizmetlerinden dolayı, başta EMO Ankara Şubesi Başkanı Şeref hocam olmak üzere, tüm yöneticilerine teşekkürü bir borç biliyorum ve sizlerin huzurunda teşekkür etmek istiyorum. Ankara Ticaret Odamız da öyle. Bizim 5908 sayılı Yasamız var, Elektronik Haberleşme Kanunu. Orada geçtiğimiz yıl çok önemli değişiklik yaparak, üyelerin bir anlamda çok rahatlamasını sağlayan kanuni düzenlemeleri birlikte gerçekleştirdik. Gürsel Başkanın orada emeği çok fazla. O anlamda yine sizlerin huzurunda Gürsel Başkana da teşekkür ediyorum.

Konuşmama burada son verirken, Siber Vatan ve Savunma Ulusal Çalıştayının düzenlenmesinde emeği geçen herkesi tebrik ediyor, ülkemizin bu anlamda başarıya ulaşmasında hayırlara vesile olmasını temenni ediyor, siz değerli katılımcıları saygı ve sevgiyle selamlıyorum. Teşekkür ederim. (Alkışlar)

SUNUCU- Sayın Bakanımıza teşekkür ediyoruz.

Sayın katılımcılar; ilk oturuma geçmeden önce Ankara Ticaret Odası Başkanımızın bir teşekkür belgesi takdimi olacak.

Takdim belgelerini almak üzere Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcımız Sayın Yavuz Emir Beyribey'i ve Ankara Ticaret Odası Yönetim Kurulu Başkanımız Sayın Gürsel Baran'ı sahneye davet ediyorum. (Alkışlar)

Değerli katılımcılar; şimdi birinci oturumumuza geçiyoruz.

SİBER VATAN, SİBER GÜVENLİK VE SAVUNMA OTURUMU - 1

Oturum Başkanı: Prof. Dr. Şeref SAĞIROĞLU
EMO Ankara Şubesi Yönetim Kurulu Başkanı

OTURUM BAŞKANI- Değerli katılımcılar; Siber Vatan ve Savunma Ulusal Çalıştayının ilk oturumuna hepiniz hoş geldiniz.

Bu oturumda çok değerli konuşmacılarımız var. Açılış konuşmalarını dinledik, ülkemizde bu alanda pek çok çalışma var, yapılan pek çok faaliyet var. Ama tabii ki bu çalışmaların kurumlar tarafından yapılması, ilgili kurumlar tarafından icra edilmesi önemli olduğu kadar, bunun tüm toplum tarafından anlaşılması ve kavranması da gerekiyor. Siber güvenliğin büyük bir risk olduğunu anlamak, buna göre de risklerin önüne geçmek, herhalde bundan sonra daha farklı, yeni bakış açılarını hayatımıza kazandıracak diye düşünüyorum. Bu çalıştayı yaparken de bu bakış açısıyla planladığımızı ifade edeyim. Çünkü her zaman değişimleri farklı bakış açılarıyla konuşmak, bunları hayatımıza kazandırmak zorundayız. Dijital rakam diyoruz; dijital kavramının içeriğini doğru anlamak gerekiyor. Siber vatanı dijital topraklar olarak ifade edersek, bu dijital toprakları korumak zorundayız. Üreten hepimiziz; korumayı da başkası değil, biz yapmalıyız, korumayı da hep beraber yapmamız gerekiyor. Şöyle düşünmek gerekiyor: Bizim sınır komşularımız var. 8 kara komşumuz var. Deniz komşularımız olduğunu son dönemde Mavi Vatan'dan öğrendik, burada da 6 komşumuz olduğunu biliyoruz. Ama genele baktığımızda ise komşularımızın sayısı daha fazla. 40'ın üzerinde. Uzay komşularımız var, uzayda olan ülkelerle komşuluk içerisindeyiz, haberleşme sinyalinin olduğu her yerde, elektromanyetik dalganın olduğu her yerde varız. Bunları internete taşıdığımızda ise, internetle de bütün dünyayla komşu olunuyor. Dolayısıyla, dijital topraklar dünyanın her yerinde. Dijital vatandaşlarımız da dijital topraklarımızı korumak için çaba sarf etmek zorunda. Bunu ilgili kurumlarımızdan tabii ki bekleyeceğiz, onlar gereken çalışmaları yapıyorlar ama bizim de son kullanıcı olarak, toplum olarak faaliyet yürütmemiz gerekiyor. Dolayısıyla, tabii ki kendi vatandaşlarımızı bu konuda eğitmek gerekiyor. Tüm dijital varlıkların üretildiği her ortamda verilerin korunması gerekiyor. Eğer dijital topraklar-

dan, siber vatandan bahsediyorsak, bunları da bugün burada tartışacağız.

Siber konusunu tartışıyoruz, ama Türk Dil Kurumunun web sitesine girdiğimizde, siberin bir tanımı olmadığını görüyoruz. Bunları biraz konuşmamız gerekiyor. Bakın, "Tanım ve terminolojiye çok takıyorsunuz hocam" deniliyor; ama tanım ve terminolojiyi eğer doğru oturtmazsak, anlamazsak, ilişkilendiremezsek, o büyük resmi görmemiz de pek mümkün değil.

Bugün programı biraz sarkıttık. Çok değerli konuşmacılarımız var, ama böyle bir girişten sonra konuşmacılarımıza söz vereyim istedim.

Şimdi müsaadenizle konuşmacılarımıza geçelim.

İlk konuşmacımız USOM'dan, USOM-BTD Daire Başkanı Onur Aktaş.

Evet Onur Bey, sizi dinliyoruz, buyurun.

ONUR AKTAŞ (USOM-BTD Daire Başkanı)- Çok teşekkür ederim hocam.

Merhabalar. İsmim Onur Aktaş, Ulusal Siber Olaylara Müdahale Merkezinde daire başkanıyım. Aynı zamanda ilk personellerden biriyim. 2013 senesinde ilk kuruluyor. Kurulduğundan bu yana neler yapılmış, neden böyle bir şey var, neler yapılmakta, bunlardan bahsedeceğim.

Aslında CERT dediğimiz Computer Emergency Response Team'ler ulusal çapta hemen hemen her ülkede olan bir organizasyon. Farklı ülkelerde farklı amaçları var, ama o amaçlar belli: Ulusal siber güvenliği sağlamak; hem vatandaşlar, hem ülke için. Her ülkenin kendi kritik sektörlerini farklı tanımlar. Bizim eylem planımızda da bunlar var. Ama aynı zamanda her ülke kendi siber güvenliği için kendi CERT'üyle alakalı yaptığı çalışmaları farklılaştırır. Fakat Amerika Birleşik Devletleri'ndeki bazı üniversiteler ve bazı organizasyonlar, national safety, yani ulusal çaptaki güvenlik için yeni bir ... modelliyorlar.

Biz bu işe ilk başladığımızda ilk yaptığımız şey koordinasyondu. Önceki konuşmalarda siber silahlardan bahsedildi. Bunların yazılımlarını yazmak gerçekten ciddi bir iş. Yani şunu yapamazsınız; ben internetten bulduğum bir şeyle öyle bir yazılım yazarım, mümkün değil. Bunun için gerçekten para harcamak lazım, net. Bu para harcanıyorsa, bu bir ülkeye karşı istihbaratta kullanılacaksa, bir veri elde edilecekse, takdir edersiniz ki, veri sadece bir kurumda bulunmaz, bir sürü yerde bulunur. Yani ben sadece bu kuruma göndereyim, bu kuruma göndermeyeyim, yok. Dolayısıyla, ilk yapılması gereken şey bu koordinasyonu sağlayabilmek. Bir kurum şunu söylüyor; açıyor telefonu, diyor ki, "Bana bir siber saldırı var, ben bunu test ettim, şu, şu, şu yöntemle saldırıyor, burayı hedefliyor, bilginiz olsun" diye-

cek ki, diğer kurumlar da bunun farkına varsınlar. Bu işe ilk başladığımızda biz bu deep yazılım sayesinde gelen çeşitli ihbarları değerlendirmeye başladık. Bu kolay bir iş gibi görünebilir; ama sayıları günde binlerce oluyor. Yani açık kaynaklardan, diğer yerlerden, diğer organizasyonlardan, yurtiçi ve yurtdışındaki çeşitli istihbarat örgütlerinden düzenli bir veri akışı var ve bunları eleyip, evet, bu bizim ülkemizle alakalı, ben bunu ilgili kuruma bildirmeliyim, daha sonra bunu takip etmeliyim diye başlıyoruz.

Daha sonra şunu fark ettik, süreç bize şunu gösterdi, aynı zamanda akademik çalışmalar da bu yönde: İnternette erişilebilir varlıkların zafiyetlerini tespit etmek gerçekten kolay. Bir grafik canlandırın gözünüzde; zafiyetlerin sayısı artıyor, çünkü çok fazla şey dijitale geçiyor, yani kapsama alanı büyüyor, ama tespit etme yaşı ve zamanı giderek azalıyor. Çünkü 13-14 yaşındaki bir çocuğun bir tab'dan indirdiği kodlarla ... ... O zaman, şunu dedik: Madem bu zafiyetler kolay tespit ediliyor... Ve çalışmalar diyor ki, kardeşim, birisi gol yiyecekse, yüzde 80 bu zafiyetlerden diyecek. Çünkü günümüzde artık ürünler, yazılımlar gerçekten buzdolabı gibi. Yani fişe tak, çalıştır, doğru işletilirse... Mesela Google çalışanlarının bir çalışması var; diyor ki, eğer bir yerde veri ihlali olacaksa, yüzde 99 oranda insan hatasıdır. Biz burada şunu yaptık: İnternette erişilebilir varlıklardaki zafiyetleri tespit ettik. Neden? Çünkü bu zafiyet internette varsa, düzgün kontrol edilmediyse bu zafiyet, büyük ihtimalle saldırganlar bunları sömürecek. İlk bunları bot ettik. Bu işe ilk başladığımızda kapsam 16 milyon ... ve bu teknik anlamda zor bir iş. Yani yer değiştirelim, siz bu tarafta olsanız şunu istersiniz: Bugün ... bir zafiyet çıktı, bütün kurumların mailleri down edilebiliyor ya da ... zafiyet çıktı, bilgiler içeride sızdırılabiliyor. O zaman ben bu ... içerisindeki zafiyeti dakikalar, saatler içerisinde bulabilmek isterim dersiniz. Bu işe başladığımızda bir sürü firmayla konuştuk, yanında bol sıfırlı rakamlar teklif edildi. Fakat şu güce sahip olamıyorduk hiçbir zaman: Ben bu zaafı kıracağım, ben bu tasarımı yaptım, senden bağımsız olarak bunu çalıştıracağım diyemiyorduk. Çünkü birbirine bağımlılık vardı.

Çıkış da şöyle olacak: Biz Türkiye olarak kendi varlığımızla bu zaafı çözmek istiyoruz, buna izin vermemiz lazım. Çok makul bir süreç değildi. Çünkü şöyle düşünün: Yakın zamanda 9.9, en kritik ... ... Bir firmanın bunu kendisinin bertaraf etmesini beklemektense, bizim kendi analizlerimiz şu an, dünyanın herhangi bir yerinde zafiyetle alakalı çıkan bir ...'yi kendi sistemlerimize entegre edebiliyoruz. Kasırga sayesinde... Kasırga projesinin başlangıcı budur. Yani dakikalar içerisinde dağıtık bir şekilde ben bütün ülkede bir işgücü mekanizması kuruyorum. ... ...Yani dağıtık bir işgücü. Ve şu an kendi analizcilerimiz 700 tane farklı zafiyeti tasarladılar. İnanılmaz bir süreçti. 4 sene boyunca inanılmaz teknik sorunlar, süreç problemleri yaşadık. Ama şu an rahatlıkla şundan bahsedebilirim: Yeni çıkan bir zafiyette, zafiyet saat 3.00 gibi yayınlandı, ortalık yangın yeri tabii, sosyal medya, sürekli telefonlarımız çalıyor, ne yapacağız, çünkü henüz şey yok; zafiyet 3.00'te yayınlandı, biz saat 4.00'te, Türkiye'de bunları kimler koyuyor, bunun ... ne, bunu nasıl talep edeceğimizi bulduk, saat 5.00'te elimizdeki bütün verilerimiz hazırdı, o gün akşam saat 5.00'ten bir sonraki sabah 2.00'ye kadar binden fazla telefon görüşmesi yaptık, 800'den fazla e-mail, yüzlerce kuruma mail attık ve 24 saate kalmadan hızlı bir şekilde zafiyetin giderilmesini sağladık. Daha sonra bu bize topyekun bir veri üretti. Düşünsenize, 16 milyon IP'nin bir sürü portları için düzenli haftalık, günlük olarak şey yapıyorsunuz, buna bir merak yaratıyorsunuz, yeni bir zafiyet çıktığında, kim koyuyor, anlık sorgulayabileceksiniz. Bu bize başka sorunlar çıkarttı, başka büyük veriye ulaşmamız gerektiğini anladık.

Daha sonra kendi içerimizde bu verilerle ilgili kendi altyapımızı kurduk. Şu an herhangi bir ürün, herhangi bir yazılım kullanmıyoruz; bizim kullandığımız sistemler açık kaynak, aynı zamanda teknik personelin de çalışmaktan keyif aldığı sistemleri burada kullandık.

Daha sonra gözümüzü vatandaşlarımıza çevirdik. Burada da şunu fark ettik: Saldırganlar o kadar hızlı davranıyor ki. Çünkü bu bir meslek onlar için. Bunlar çalıntı bir kredi kartıyla internete reklam veriyor, dergi reklamı zannedersin. Yani dakikalar içerisinde bu iş oluyor bitiyor. Bunu yaptığımız operasyonlarda da gördük. Bu işin güçlü tarafı, ilerleyen bölümlerde Mahmut Esat Bey size bahsedecektir, çok güzel operasyonlar yapıyoruz. Saldırgan, kredi kartı çalmak için sistem kuruyor, biz saldırganın kurduğu sistemi ele geçirip, saldırıda neler yapmış bakabiliyoruz. Teknik anlamda gerçekten güçlü bir ekibiz. Ve şunu gördük: Yahu arkadaş, bu adamlar her şeyi kullanıyorlar. Adamın arayüzünde şu var: Bir tane buton var, tıklıyor butona, Google'da onun başlığı yazıyor, diyelim ki başlık şey olsun, Covid ödemeleri olsun, Covid yardımları olsun, yazıyor başlık, Google'da

hesap makinesi görünümü altında bir uygulama çıkıyor ya da herhangi bir kamu kurumu bir şey yapsın, örneğin çiftçiye yardım, arayüze giriyor, hemen bunu takip ediyor, çiftçiye yardım diye bir mobil uygulama çıkartıyor ki kredi kartını alabilsin. Sonra biz buna manuel, yani insanla buraya giremeyeceğimizi fark ettik. Sonra yine bir çalışma başlattık. Bu çalışma 2 ay, 4 ay, 5 ay, 6 ay derken, 1 sene sonunda şu anda yapay zekâ kullanarak büyük veri analizi yapıp, zararlıları tespit edebiliyoruz. Şu an USOM'un web sayfasına girerseniz, bizim erişimini engellediğimiz alan adlarını göreceksiniz. Ne demek bu? Yani siz cep telefonunuza ben bunu indireceğim arkadaşım, kredi kartını vermek istiyorum deseniz bile, o uygulamanın bağlantı şeyine Türkiye'de erişim yok. Yani oraya kredi kartı bilgilerini göndermek istese bile gönderemiyor; çünkü blokluyoruz. 200 bin alan adını engelledik. Günümüzde engellediğimiz 10 alan adından 1 tanesi yapay zekâ modüllü ve dakikalar mertebesinde. Çünkü başka türlü gerçekten onun önüne geçmek neredeyse imkansız.

Daha sonra, yaklaşık 1.5 sene çalıştığımız bir şey, şöyle bir uygulama geliştirdik: Çok fazla istihbarat akıyor. Gerçi şimdi düzelmiş olabilir, biz şimdi çok istihbarat almaya çalışıyoruz. Çünkü ne kadar çok veri, o kadar anlamlı. Fakat şöyle bir problemimiz var: Elinizde bin tane zararlı yazılım varsa, evet, dert yok. Ama elinizde 10 bin tane varsa, o zaman triyaj yapmanız lazım. Yani şunu demeniz lazım: Bu 10 bin tanenin hangisi diğer ülkelerin ülkeme gönderdiği zararlı yazılım, hangisi daha çok son kullanıcıyı hedef alan, herkesin yapabileceği zararlı yazılım, analiz etmeniz lazım. Bunun için başka projeler başlattık.

Bunun dışında, USOM'un o bahsettiğim projelerde port ettiğimiz diğer işlerimiz var. Ne bunlar? Teknik sıkı bağlantı. İnanılmaz faydalı ve inanılmaz ölçüde ülkeye katkı sağlayan bir iş. Bunu çözen bir ekibimiz var. Açık kaynak istihbarat topluyor. Mesela az önce operasyonlardan bahsetmiştim; bizim teknik istihbaratımız, yaptığı operasyonlar sayesinde saldırganların kullandığı arayüzü görebilme şansına sahip. Daha 1.5 ay oldu, ülkemize ait 6 bin tane kredi kartına yönelik saldırıyı bertaraf ettik. Bildirdiğimiz kredi kartı şu an on binlerle ifade edilir. Yani eğer çevrenizde birilerinin kredi kartı iptal olduysa, büyük ihtimalle biz onu bildirmişizdir. Çünkü on binlerce kredi kartı bildirdik. Saldırgan şunu yapmış: Cep telefonuna ulaştı ya, cep telefonunun ekran görüntüsünü alıyor, ilgili bankaya yazıyorlar, kendisi yönetici paneli açmış; diyor ki, "Şu bankayı kullanıyor, bu adam şu işi yapıyor, üzerine kredi çektim, takip et." Çünkü 6 bin tane kredi kartı var. Demiş ki, "Bu adam ticaretle uğraşıyor, ama borcu var, bundan iş çıkmaz, çizmiş üstünü." Hepsini tek tek incelemiş, bütün hesap bilgilerini, kendine

notlar almış. "Bu adam maaşını şu tarihte alıyor, şu tarihte tekrar bak" gibi notlar almış saldırgan kendisine. Bunu gördük ve bunun karşısında, o 6 bin kredi kartına, belki daha da fazlasına yönelik saldırıyı bertaraf ettik. Ve artık öyle bir seviyeye geldik ki, şöyle bir terim ortaya atıldı: ... ... Saldırganlar şöyle yapıyor ya... İki türlü saldırgan var diyelim. Bir sürü var, ama biz kendi kafamızda ikiye bölelim. Birincisi, bu işi yazılımla yapanlar, yani teknik anlamda yapanlar. Diğeri de, "Kardeşim, ben teknikten anlamam, ama..." Yani eskinin tefecisi, mafyası, günümüzün bu iş yapanı. "Teknikten anlamam, ama bu işte para varmış, ben üç beş çocuk bulayım, bu işi yapsın" diyenler. Bu adamlar yazılım satın alıyorlar. Biz de satın alıyoruz. İkimiz de gidiyoruz, para verip yazılım alıyoruz. Yazılım satan adamlar kavga etmeye başlıyor. Çünkü diyor ki, "USOM yedi bunu, yani USOM engelliyor bunu" ve parasını iade etmek istiyor.

O yüzden şöyle bir terim ortaya çıktı: Araba ilanı giriyor, ... adını koyuyorlar, ... adı, çalıştığı sistemler; "USOM tanır mı? Evet, hayır" diye yazıyorlar. Çünkü şunun farkında: Yapay zekâ var, büyük veri var, verinin kendisi bizde, incelemelerimiz var, dakikalar içerisinde engelleyebiliyoruz. Hatta saldırganlar içerisinde USOM geçen alan adlarıyla bize mesaj gönderiyorlar: "USOM ne olur yapma etme bana teta." "USOM bu da mı godi teta." İşte tahmin edersiniz, USOM'la başlayıp inanılmaz küfürlerle devam eden yüzlerce liste. Çünkü artık bu yapay zekayla... Hatta bize karşı şey yapmak için şunu yapmış: Zararlı yazılımı yazmış, ... komuta kontrol merkezini USOM göstermiş. Bu niye sıkıntılı bir durum? Çünkü güvenlik ... usom.gov.tr'yi şey diye görüyor artık; "Bu sıkıntılı bir site, buraya erişimi engelleyelim, alarma çıkartalım" diye göstermeye başlamış. Bize telefon ediyorlar, biz biliyoruz o adamın kim olduğunu, ama yurtdışında, sesini değiştirerek, "Bunu nasıl yapıyorsunuz, şunu nasıl yapıyorsunuz" falan, ihbar gönderiyor. Artık rakiplerini ihbar etmeye başladılar; çünkü alanları daraldı. Yani birbirlerini ihbar ediyorlar, "Bu

adam böyle bir şey yapıyor, bilginiz olsun" diye.

Şu an gelinen noktada, USOM, kendi içerisinde onlarca projesini geliştiren, gerçekten güçlü bir teknik ekiple çalışan ve son dünya teknolojilerini kullanan, hem vatandaşlarımıza yönelik, hem de aynı zamanda kritik sektör ve kamuya yönelik onlarca olaya müdahale gerçekleştirmiş bir yapı konumunda. Daha önce yaptığımız bir etkinlikte, bize 5 sene önce bir devletin APT'sini gönderen bir kişiyle el sıkıştık. "O ihbarı ben göndermiştim" dedi. Tek bir ihbar yani, tek bir e-mail. O mail'den yola çıkarak 4 binden fazla alan adı engelledik ve hâlâ da engellemeye devam ediyoruz. Az önceki konuşmalarda hangi ülke olduğundan bahsedildi. Düzenli olarak takip ediyoruz bunu.

Gerçekten güçlü bir altyapımız var. Yavaş yavaş da bu altyapıyı belli bir seviyede tutup, daha çok entegrasyonlu bir süreçte çalışacağız. Niye? Şöyle bir yazılım yaptığımızı düşünelim: Bütün zafiyetleri bütün kurumlara gönderdiğimizi varsayalım. Diyelim ki Türkiye bu kadar güçlü olsun. Şu an şunu yapabiliriz: Eğer mevzuat izin verirse, evinizde bir bebek kamerasını açık unuttuğunuz zaman… Bu altyapıya sahibiz. Ya da bir kamu kurumunda çalışıyorsunuz, … interneti açtığınız zaman, bunu size bir-iki dakika içerisinde tespit edecek bir altyapıya sahibiz. Daha da ilginci, şöyle bir yapı kuralım: Bütün kurumlarımıza, bütün vatandaşlarımıza bu ihbarı gönderebildiğimizi varsayalım. Maalesef, çip daha yeterli değil. Neden yeterli değil? Çünkü gerçekten teknik altyapıda güzel işler yaptık, ama bunların katkısını sağlamadığımız sürece bu bizi mutlu etmiyor. O yüzden şuna çalışıyoruz: "Evet, ben bunu bildirdim; ama ilgili kurum bunu ne kadar sürede yapacak, ne kadar hızlı kapatabilecek, doğru işi yapıyor mu ya da kapattığını sanırken başka hatalar yapıyor mu?" diye daha çok süreçlere, daha çok entegrasyona dokunan işler yapmak istiyoruz. Çünkü ülkeye ancak böyle katkı sağlayabiliriz. Yani biz tek bacağımızı güçlendirerek katkı sağlamak yerine, doğru ve sürdürülebilir bir şekilde siber güvenliği sağlamak adına, entegrasyon, süreç, eğitim gibi konulara dokunmak istiyoruz.

Teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Onur Bey'e teşekkür ediyoruz.

Evet, bir soru alalım.

Buyurun.

SALONDAN- Onur Bey'e bu güzel sunumu için çok teşekkür ederim.

Benim kredi kartım da o şekilde alındı, banka beni uyardı, ama tabii, ben

sürekli ekstreleri takip ettiğim için herhangi bir olay yaşanmamıştı. Peki, bu işi yapanları tespit ettiğinizde, yasal olarak bunlara bir ceza uygulayabiliyor musunuz veya bu yeni yasadan sonra mı gündeme gelecek?

ONUR AKTAŞ- Bu zaten bir siber suç aslında. CMK'da tanımlı; yani bilişim suçuyla dolandırma zaten bir siber suç. Biz yaptığımız çalışmalarda, eğer IP'nin Türkiye'de olduğunu ve adresini bulabiliyorsak, ilgili kuruma gönderiyoruz zaten; diyoruz ki, "Biz böyle bir çalışma yaptık, böyle bir IP var, bu IP Türkiye'den geldi, bir bakın buna, kimmiş bu, belki de gerçekten saldırgandır" diye gönderiyoruz. Çoğu yurtdışı oluyor. Ama bazen yeni başlayanlar, daha genç yaşta olanlar Türkiye'de olabiliyor. Onları tespit ettiğimizde, o bilgileri alıp ilgili kurumlara yazıyla gönderiyoruz; diyoruz ki, "Bakın, böyle bir panel var, saldırgan bunların, bunların kredi kartlarını çalmış, bizim tespit ettiğimiz IP adresi de budur, gerekli çalışmayı yapın lütfen" diye gönderiyoruz. Onlar da işlem başlatıyor. Bu konuda haberlere çıkmış, çok güzel çalışmalarımız var.

OTURUM BAŞKANI- Onur Bey'e bir kez daha teşekkür ediyoruz.

İkinci konuşmacımız, Duygu Fidancıoğlu. Kendisi Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Birimi Müdürü.

Buyurun Duygu Hanım, sizi dinliyoruz.

DUYGU FİDANCIOĞLU (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkalığı Birim Müdürü)- Değerli katılımcılar, saygıdeğer misafirler; hoş geldiniz, hepinizi saygıyla selamlıyorum. Bu etkinliğin düzenlenmesinde emeği geçen herkese teşekkür ederim.

Siber savunma, hakikaten, ulusal siber gücümüzü sağlamamızda önemli konulardan bir tanesi. Ama ben biraz daha siber savunmayı besleyen bir konudan başlamak istiyorum, siber güvenlik kapasitesinin geliştirilmesi konusundan.

Ekosistem nedir, bunu tanımlamadan önce siber güvenlik kapasitesinden bahsetmemiz lazım. Çünkü benden önceki konuşmacılar, siber güvenlikle ilgili, neden siber güvenliğe önem vermemiz gerektiği gibi birçok noktadan bahsettiler.

Teknolojik gelişmeleri hepimiz görüyoruz. Her gün yeni bir terimle, yeni bir teknolojiyle karşı karşıya kalıyoruz. 5G, Metaverse, blokzincir, yapay zekâ, böyle bir sürü terimle her gün karşı karşıyayız ve bunlar birbirlerini besleyecek şekilde çalışmaya devam ediyorlar. Tabii, bu birbirleriyle beslenerek çalışmaları, etkileşim halinde çalışmaları, bizi karmaşık, grift bir teknoloji

yığınıyla karşı karşıya getiriyor. Dijital tsunami diye tanımlanıyor bu. Dijital tsunami beraberinde siber güvenlik alanında büyük bir tehditler yığınını da getiriyor. Bu bizim için ne anlama geliyor peki? Bizim korumamız gereken varlıklarımız var. Bu varlıkları korumak için de bu tehdit düzeyindeki açıklıkları kapatmamız lazım. Peki, nasıl yapacağız bunu, bunu kapatmamız mümkün mü? Buna yönelik dünyada pek çok çalışmalar yürütülüyor. Siber güvenlik yönünden zafiyetlerinizi kapatmak için öncesinde yapılacaklara ilişkin çok güzel çalışmalar var. Ama yüzde yüz güvenlik mümkün değil. Ne yapacağız o zaman? Bizim siber güvenlikle ilgili riskleri elemine etmemiz gerekiyor. Güvenlik sistemiyle ilgili çalışma yapanlar bilirler, belli süreçlerimiz vardır bizim: Planla, uygula, kontrol et ve önlem al.

Aslında bu süreci, siber güvenlik alanı düşünüldüğünde, ulusal siber güvenlik alanı çalışmalarında da kullanıyoruz. Ne yapıyoruz? Burada yaptığımız işlem, basit anlamda, bu sürecin ulusal çalışmalara yansıtılmasından oluşuyor. Planlıyoruz; neler yapabileceğimize, riskler neler, tehdit ortamımız neler, bu tehditlerle nasıl baş edebileceğimize ilişkin politikalar oluşturuyoruz, stratejiler geliştiriyoruz. Sonrasında varlıklarımızı korumak için tedbirler oluşturuyoruz, bu tedbirleri uygulamaya koyuyor kurumlarımız. Tabii, tedbirleri uygularken, uyguladığı noktada boşluk var mı, tam olarak uyguladı mı uygulamadı mı diye kontrol ediyoruz. Kontrol ettikten sonra da boşluk kalan kısımlarla ilgili önlem alma çalışmalarını yürütüyoruz. Aslında burada bir süreç işletiyoruz. O yüzden, siber güvenlik aslında kullandığımız teknolojiler değil, süreçsel bir yönetim işidir; siber güvenlik bir yönetim işidir, yönetebilme işidir diyoruz. Elimizdeki kaynaklarımızı politikalarımız çerçevesinde kullanarak, varlıklarımızı korumak için bir süreç işletiyoruz.

Siber güvenlik ekosistemi de bu kaynaklardan bir tanesidir. Yürekte, beyinde Ürettiğiniz, kullandığınız teknolojiler, bu teknolojinizi çalıştıran, yürüten, opere eden işgücünüz, siber güvenlik farkındalığı yüksek vatandaşlarınız, bu aslında sizin bütün kaynaklarınızı oluşturuyor ve ülke olarak

da siber güvenlik kapasitenizi bunlar belirliyor. Ben, politika geliştiren bir kurumun personeli olarak bugün buradayım. Politika geliştiriciler için de bu konuyu ele almak, siber güvenlik kapasitesinin geliştirilmesine yapılan yatırımlar, diğer politika girişimlerimizi doğrudan etkilediği için, bunun başarısı bizim için önemli.

Kapasitenin güçlü olması siber savunmayı doğrudan etkiliyor. Bu anlamda, kapasitenin güçlü olması demek, güçlü ekosistem, farkındalığı yüksek vatandaşlar, nitelikli-yetkin işgücü, markalaşmış yerli ve milli teknolojimiz, üretkenliğini kullanan, yabancıya muhtaç olmayan bir ülke anlamına geliyor.

Peki, güçlü ekosistemi nasıl sağlarız? Ekosistem terimi bize aslında biyolojiden geçmiş bir terim. Der ki biyoloji kitapları, belirli bir alanda bulunan canlılar ile bunları saran cansız çevrelerinin karşılıklı ilişkileriyle meydana gelen ve süreklilik arz eden ekolojik sistemler ekosistem olarak tanımlanır. Yani burada ekosistemi güçlü kılan iki parametre var aslında; karşılıklı etkileşim ve bu etkileşimlerin sürekliliği. Bugün burada bulunduğumuz bu etkinlik de aslında etkileşimin bir örneği. Bu etkileşim siber güvenlik çalışmalarındaki bütün kurumlarımızın, bütün paydaşlarımızın birlikte çalışmasıyla belli bir sonuca erişecek. Dijital Dönüşüm Ofisi de siber güvenlik ekosisteminin bir paydaşı, bir parçası durumunda.

Siber güvenlikte ekosistemi oluşturanlar nelerdir diye baktığımızda, geniş bir ağla karşı karşıyayız. Bugün bu salonda sivil toplum örgütlerimizden Ankara Ticaret Odası, Elektrik Mühendisleri Odamız, siber güvenlik alanında faaliyet gösteren diğer derneklerimiz var, hepsi birer paydaş. Üretici firmalarımız da burada bugün, yani bu siber güvenlik teknolojisini üreten firmalarımız, onlar da birer paydaş. Üniversitelerimiz ha keza öyle. Bireyler olarak siz katılımcılar bile bu ekosistemin birer parçasısınız esasen.

Dijital Dönüşüm Ofisi olarak bizler, standart geliştiriciler, politika geliştiriciler ve strateji belirleyiciler olarak bu ekosistemin içerisindeyiz.

Türkiye Siber Güvenlik Kümelenmesini duyanlarınız vardır. Kümelenme, ekosistem dediğimizde akla gelen ilk parametrelerden bir tanesi. 2017 yılında Savunma Sanayi Başkanlığımızın önderliğinde kuruldu Türkiye Siber Güvenlik Kümelenmesi. Üniversitelerimiz, akademisyenlerimiz, kamu kurumlarımız ve sektör temsilcisi firmalarımızın yer aldığı geniş bir kümeden bahsediyoruz burada. Yerli ve milli teknolojinin geliştirilmesi gibi, yeteneğe erişim gibi, inovasyon gibi faaliyetlerle teknolojik üstünlüğün sağlanması, pazara erişim, yerli ürünlerimizin hem iç pazarda, hem de dış pazar-

da yaygınlığının arttırılması hedefiyle çalışan bir platform.

2020 yılında Savunma Sanayi Başkanlığımızda yaptığımız toplantıyla birlikte Dijital Dönüşüm Ofisi olarak biz Siber Güvenlik Kümelenmesini birlikte yürütmeye başladık. Birlikte yürütmekten kastım şu: Bir yönetim kurulumuz var. Ben, yönetim kurulunda Dijital Dönüşüm Ofisi koordinatörü olarak yer alıyorum. Dört üyesi var yönetim kurulumuzun; ikisi Savunma Sanayi Başkanlığımızdan, ikisi de Dijital Dönüşüm Ofisinden var. Ne yapıyoruz peki? Aslında iki kurumun ortaya koyduğu siber güvenlik ekosisteminin geliştirilmesi anlamında stratejileri birlikte oluşturuyoruz, birlikte karar veriyor ve yerli teknolojimizin gelişmesi için adımlar atıyoruz.

Küme, ülkemizdeki yerli-milli siber güvenlik teknoloji üretici ve … tek bir kanalda toplamış durumda. 200'ün üzerinde firmamız var burada ve 300'ün üzerinde ürün, 600'ün üzerinde de hizmete sahip firmalarımız. Türkiye Siber Güvenlik Kümelenmesinin bu firmaları ve ürünleri tanıttığı bir katalogu var, web sitemiz üzerinden bu katalog erişilebilir durumda. Bugüne kadar yerli teknolojimizin iç pazarda tanıtılmasında birçok güzel faaliyet gerçekleştirdik, bundan sonra da gerçekleştirmeye devam edeceğiz. 200'ün üzerindeki firmamızın 300'ün üzerindeki ürününün Türkiye iç pazarındaki kullanımı maalesef az. Kamu kurumlarımız dahi, özel sektörümüz dahi yerli ürünlerimize biraz imtina ile yaklaşıyor.

Dijital Dönüşüm Ofisi olarak bizim ana amaçlarımızdan bir tanesi de bu yerli ve milli teknolojimizin kullanımını yaygınlaştırmak. Bunun için birçok projemizi Türkiye Siber Güvenlik Kümelenmesi üzerinden başlattığımız gibi, Dijital Dönüşüm Ofisi kaynaklarıyla desteklemeyi de başlatmış durumdayız. Türkiye Siber Güvenlik Kümelenmesi olarak, öncelikli siber güvenlik gelişim alanlarını belirleyerek, yerli oyuncularımızın pazardaki pozisyonlarının güçlendirilmesi yönünde çalışmalarımıza devam ediyoruz.

İç pazarda yerli ve milli teknolojimizin kullanımını yaygınlaştırmak için, geçtiğimiz sene, bir inisiyatifle, kamu kurumlarının oluşturduğu bir inisiyatifle çalışmaya başladık. Sayın Bakanımız da konuşmasında kısaca bahsetti, esasında bir konsorsiyum diye bahsetti. Dijital Dönüşüm Ofisi koordinasyonunda, Savunma Sanayi Başkanlığımız, Devlet Malzeme Ofisi, Kamu İhale Kurumu, Sanayi ve Teknoloji Bakanlığı, Strateji Bütçe Başkanlığından oluşan 6 kurumla birlikte biz inisiyatif aldık. Kamuda diye başladık, ama şu anda daha gelişti bu, yerli ve milli ürünlerin kullanımının globale yaygınlaşması için çalışma yürütüyoruz. Teşvik mekanizmalarından yerli-milli teknolojilerin kamuda kullanımının yaygınlaşması için gerekli mevzuat altyapısı tesisine, politikaların geliştirilmesine, ürünlerin olgunlaşma sürecine

kadar giden değişik başlıklarda bir çalışma gerçekleştiriyoruz.

Ekim ayında toplantılar yaparak başladık, bir dizi toplantı seansımız oldu burada. Bu toplantılarda konuyu masaya yatırdık; 6 kurum, ortak akıl yöntemiyle, öncelikle neden yerli ürünlerin kullanılmadığını ortaya çıkardık. Peki, nasıl yaygınlaştırabiliriz bunu? Kurumlarımız bu konuyu da her biri önce kendi başlarına çalıştılar, sonra yine ortak toplantılarla çalıştık ve nasıl yaygınlaştırabileceğimize ilişkin 170'in üzerinde öneri listesi ortaya çıktı. Tabii, 170 tane adımı bir anda yapmak çok kolay değil. Dedik ki, o zaman ne yapalım; biz bu önerileri kısa dönem ve uzun dönem olarak gruplara bölelim. Kısa dönemli adımlara baktık, yine çok yüksek; o zaman, hızlı ve yavaşı şeklinde de bölelim dedik. 100 günde yapılabilecek, hızlı, somut çıktısı olan, ölçülebilir hedefler koyalım kendimize. Kamu kurumlarımızın her biri 5'er tane öneri getirdi masaya ve bu önerileri üzerinde tartışarak, 18 tane ana aksiyon ve 31 tane faaliyetten oluşan bir eylem listesini 100 gün içerisinde uygulamak üzere karar aldık ve ilk faz çalışmaları için 21 Aralıkta düğmeye bastık. İlk faz çalışmaları devam ederken, biz doğru yolda mıyız diye de kamuya sorduk. Geçtiğimiz sene içerisinde bir çalıştay gerçekleştirdik. "Kamu, ben doğru yolda mıyım? Teşvik için ben bunları düşünüyorum; ama senin düşündüğün noktalarda eksiğin ne, senin neye ihtiyacın var? Satın alma süreçleriyle ilgili neler düşünüyorsun, ne yaparsak sen yerli-milli ürünlerin kullanımı sana cazip gelir? Ürünler olgun mu? Olgun değilse neden olgun olmadığını düşünüyorsun, hatta olgunlaştırmak için bana ne tavsiye ediyorsun?" diye bir çalıştay gerçekleştirdik. Aldığımız önerileri de ikinci dönem çalışmalarında baz aldık. İkinci dönem çalışmalarımız başladı, devam ediyor.

Bu, aslında kamunun birlikte çalışması için güzel bir işbirliği örneği. Tabii, yerli-milli ürünlerin gelişmesi için birçok faaliyetimiz oldu. Dış Ekonomik İlişkiler Konseyiyle bir çalışma yaptık; ... diplomasisinin gelişmesi, yurtdışına açılım için biz bu kanalı kullanıyoruz. Haziran ayında gerçekleştirdik bunu.

Bunun yanında, işgücünün gelişmesi için de birçok faaliyet gerçekleştiriyoruz. Siber güvenlik konusunda farkındalığın arttırılmasına ilişkin dijital karakterli çizgi filmler, Teknofest kapsamında yaptığımız yarışmalarla odağı siber güvenlik noktasına çevirmeye çalışıyoruz. İşgücünün geliştirilmesi noktasında siber liseyi biliyorsunuz, Türkiye'nin ortaöğrenimdeki ilk siber güvenlik lisesi. Teknoparkın içerisinde, sektörle bir arada çalışan böyle bir modelimiz vardı. Biz bu yıl bu modeli meslek yüksekokulları için de uygulayalım dedik ve Yükseköğretim Kuruluyla bir protokol imzaladık. Siber güvenlik meslek yüksekokulu açılması için gerçekleştirilen bir protokol bu. Siber güvenliğin farklı ihtisas alanlarında eleman yetiştirmek; ara eleman değil, aranan eleman yetiştirmek amacıyla böyle bir proje başlattık.

Dijital Dönüşüm Ofisinin bu çalışmalarını aktarma fırsatı verdiğiniz için hepinize çok teşekkür ederim. Kapasitenin geliştirilmesiyle ilgili daha birçok çalışmamız var, ama vaktimiz sınırlı, o yüzden onlara değinemeyeceğim. Dinlediğiniz için teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Duygu Hanım'a teşekkür ediyoruz.

Bir sonraki konuşmacımız, Oğuz Yılmaz. Oğuz Bey, "Dijital Vatan Kavramı, Varlıklar ve Sınırlar" başlıklı sunumunu gerçekleştirecek.

Buyurun Oğuz Bey.

OĞUZ YILMAZ (Labris Networks YK Üyesi)- Merhabalar. İsmim Oğuz Yılmaz, Labris Teknoloji Bilişim Çözümleri'nin kurucu ortağı ve yönetim kurulu üyesiyim. Bugün size biraz daha kavramsal bir sunum yapmaya çalışacağım. Ancak, öncesinde, şirket olarak biz ne yapıyoruz, biraz ona değinmek istiyorum.

Labris Teknoloji, 2002 yılında kuruldu, 20 yılı aşkın bir süredir faaliyet göstermekte. 20 yıldan bu yana sadece ar-ge odaklı üretim yapan, herhangi bir al-sat işi olmayan, sadece ürettiğini müşterilerine sunan ve servisini veren bir firmadır. Türkiye'nin bu alanda var olan ilk siber güvenlik üreticisidir. 2003'te ticari güvenlik duvarlarıyla başladık, daha sonra UTM ürünleri, DDoS, HARPP, ilerledikçe Common Criteria (Ortak Kriterler) alanlarında Türkiye'de ilk EAL4+ sertifikası alan bir firma oldu. En yakında, 2020 yılında uluslararası sertifikasyon ödülünü aldık.

Tabii, buraları geçeceğim, bu sunum biraz daha kavramsal bir sunum.

Bu slaytla başlamak istiyorum.

Bu, Dünya Ekonomik Forumunun küresel riskler tablosu. 2020-2021 tablosu. Bu tabloda, dünya ekonomisini ne tehdit eder dediğimizde, ne varsa

onların tamamı var. Yani iklim krizinden tutun da biyoçeşitlilik kaybına kadar uzanan, dünya ekonomisini tehdit eden her şey. Burada siber saldırılar, yani bilgi altyapılarının çalışmasını engelleyici veya bozucu siber tehdit, siber saldırılar, 2020'de dünya ekonomisini tehdit eden tehditler arasında hem etki olarak yüksek, hem olasılık olarak yüksek alanda bulunuyor. Sonraki yıl da yine aynı şekilde bu devam ediyor. En son yıldaki tabloda da siber tehdit ve saldırırla, siber güvenlikte başarısız olmak durumunda dünya ekonomisini tehdit eden ilk 10 tehdit arasına konuldu.

Tabii, kurumlarımız da gittikçe dijitalleşiyor. Evlerimiz dijitalleşiyor, süreçler sayısallaşıyor ve teknolojinin kullanımında bir patlama var, daha önce kullandığımızdan katbekat daha fazla teknoloji kullanıyoruz. Dolayısıyla, bu tabloyu biraz da böyle anlamlandırabiliyoruz.

Şimdi, bu noktada, bu bilgiler ışığında, dijital vatan kavramına bir giriş yapmak istiyorum.

Bunu ilk bir köşe yazımda tanımlamıştım, 2020 yılının Şubat ayında, yani bundan neredeyse 3 yıl önce. Dijital vatan, "ülkelerin siber hâkimiyet alanları, yani ülkelerin dijital topraklarıdır". Bir devlet nasıl bir toprağı vatan yapıyor; ona bir sınır çiziyor ve "Ben buraya hâkimim, burada benim söylediğim geçerli" diyor. O zaman, dijital vatan da siber hâkimiyet oluşturabildiğimiz alanlardır diyebiliriz.

Toprağın üstünde görünenler, her türlü bilişim sistemi, yazılımlar ve bunların bağlı olduğu ağlardır. Toprağın altında ise devletimiz ve milyonlarca vatandaş tarafından üretilmiş her türlü veri var. Yani toprağın altındaki kaynak veri; üstündekiler ise bizim gördüğümüz bilgisayarlar, yazılımlar, sistemler ve benzeri şeyler. Bu şekilde bir benzetme yapabiliriz.

Peki, dijital sınırları nasıl anlatabiliriz? Dijital sınırlar daha muğlak, coğrafya sınırlarımız gibi düşünülemez. Hatta bazı durumlarda, verimiz neredeyse, bu veri Türkiye Cumhuriyeti toprakları içerisinde olmasa dahi, o verinin olduğu yer bizim dijital sınırlarımız içerisinde kabul edilebilir. Örnek verelim.

Rusya'nın anakarası Orta Asya'dan Kaliningrad'a kadar uzanır, Baltık Denizi'nde biter, bir de Rusya'yla kara bağlantısı olmayan, ama Rusya toprağı olan, Ekslav olarak tanımlanan bir bölge var. Benzer şekilde, dijital sınır çizerken de biz verimizin nerede olduğuna bakmalı ve verimizin olduğu yerlerde, hâkimiyet alanımızın olduğu yerlerde burayı dijital vatan tanımı içerisine sokmalıyız.

Peki, dijital vatanın karayolları nelerdir? Aslında bu, iletişim ağlarıdır. Bu iletişim ağları, bugün baktığımızda, fiber hatlar, bakır hatlar ve benzeri, mobil hatlar, bunların tamamıdır. Nasıl ki bu karayollarında sahip devletse -işletme hakkını verse dahi sahip her zaman devlettir- burada da, dijital vatanda da, bu dijital vatanın karayollarının, yani iletişim hatlarının tüm sahibi devlet olmak durumundadır.

Dijital vatanın toprak altı kıymeti veridir dedik. Burası çok önemli. Veri bir maden aslında. Kelime olarak veri madenciliği denilmesinin nedeni de belki bu. Gerçekten toprağın altındaki bir şey gibi onu çıkarıp işlemeniz gerekiyor. Peki, bu veriye kim sahip olacak? Bu biraz tartışmalı bir alan.

Ben şimdi burada bir soru sormak istiyorum: Yeraltı kaynaklarımız devletinse, neden vatandaşın sosyal medya verileri sosyal medya şirketlerinin malı oluyor? Mesela benim Facebook verim Facebook'un malı. Hatta Facebook şirketi değerleme yaparken, kaç kullanıcısı var, buna göre şirket değerlemesi yapılıyor. Aslında benim verim. Bu bir soru olarak aklımızda kalsın.

Dijital vatan hukuku: Dijital vatan hukuku kendine özeldir. Bu alanda 1455, 6458 sayılı kanunlar gibi çeşitli kanunlar oluşmaya başladı. Ancak, Türk Ticaret Kanunu ve Türk Ceza Kanununda hâlâ dijital hukuka adaptasyon süreci devam ediyor. Uluslararası hukuk anlamında baktığımızda ise, dijital vatan hukuku neredeyse yok. Bize özel bir durum değil, tüm dünya için böyle; uluslararası hukuk dijitali henüz kapsayabilmiş değil.

Dijital vatanın güvenliği: Biraz önce bahsettik, coğrafi sınırları değil, dijital hakimiyetimizin olduğu her yeri dijital vatan olarak kabul etmek durumundayız ve bunun güvenliğini sağlamak durumundayız.

Sınırları nasıl tanımlayabiliriz? Bugün mavi vatanımızın coğrafyası içerisindeki her sistem bizimdir diyebiliriz; artı, dijital ekslavları bunun üzerine ekleyebiliriz.

Sınır aşan yollarımız da aslında bizim internet bağlantılarımız. Bunlar neler?

Trakya üzerinden Balkanlara uzanan ve Avrupa'nın neredeyse bütününü

dolaşan karasal hat, Edirne çıkışlı Avrupa'ya uzanan karasal hat, Ege Denizi ve Akdeniz altından giden 5 tane farklı bağlantıyla Türkiye'nin yurtdışı internet çıkışı gerçekleşiyor. Dolayısıyla, bu da bizim yolumuz olması hasebiyle korumamız gereken bir başlık haline geliyor.

Üçüncü korumamız gereken bölüm de aslında satıh. "Hattı savunma yoktur, sathı savunma vardır" sözünden hareketle bakarsak; vatanın içerisinde, dijital vatanın içerisinde siber farkındalık ve siber güvenlik çalışmalarıyla mukavemeti nasıl arttırırız? Bunların hepsini birlikte düşünmek gerekiyor.

Dijital vatanın güvenliğinde kullanılan her türlü sistemi millileştirmek; sadece tedarik güvenliği için değil, tedarik edilmiş sistemlerin işletilmesi esnasındaki güven için de oldukça kritik.

Burada bir kavramı daha ele alalım: Dijital emperyalizm ve yeni dünya düzeni.

Emperyal kelimesi, imperial kelimesinden doğuyor. İmperial, güç kontrol etmek demek. Dijital emperyalizm de şu: Dijital dünyada şirketlerin ve devletlerin hakimiyet kurma ve her dijital alana sahip olma çabası. Dijital emperyalizm için sahip olmak demek şudur: O mecrayı kullanıp oradan para ve güç kullanabiliyorsa, o mecranın sahibi odur. Örneğin bir sosyal medya alanı düşünün, bu alanda kim güç kazanıyor ve para kazanıyorsa, o alanın sahibi odur.

Emperyalizmin nihai amacı her zaman devamlılığını sürdürmektir, bunu yaparken de sömürü kartını kullanmıştır. Yıllarca böyle gelmiştir. Bunlar neler olabilir? Toprak, doğal kaynaklar, diğer zenginlikler ve kültür; bunlar sömürülen unsurlar oldu. Şimdi ise farklı bir araç ortaya geliyor, o da veri.

Verinin kıymetini şöyle ifade etmek isterim: Bunu biraz sömürgecilikle birleştirmeye çalıştım. Birleşik Krallık'ın Hindistan'ı sömürdüğü dönemde, 1765'ten 1938'e kadar yaklaşık 45 Trilyon dolarlık bir sömürü yaptığı kabaca hesaplanıyor. Bunu yıla bölersek, Hindistan'da yılda 260 milyar dolarlık bir sömürü yapmış Birleşik Krallık. Şimdi bugünün en değerli şirketlerine bakalım. 2010 yılında dünyanın en büyük 10 şirketinin arasında sadece 2 teknoloji şirketi vardı. Şu anda en büyük 10 şirketin arasında 7'si teknoloji şirketi. Demek ki teknoloji alanı ekonominin büyüdüğü bir yer. Bu şirketler şunlar: Microsoft, Apple, Amazon, Alphabet (Google), Facebook, Alibaba, WeChat. Bunların 4'ü tamamen veri şirketi, bazıları da veri üzerinden faydalanıyor. Değerlerine bakalım. Sadece 1 yılın, yani 2021 yılının geliri; şirket değeri değil, 1 yılda kazandığı kâr: Meta 118 milyar dolar, Google 258 milyar dolar. Şimdi bunu yukarıdaki İngiltere'nin Hindistan'ı sömürmesiyle

karşılaştıralım. Ne kadar benziyor, değil mi? Aslında dijital emperyalizm, tüm dünyaya bir şey satarak ondan parayı almak için yeni bir yöntem bulmuş. Bunun farkında olmak lazım.

İspanyollar ve Kıta Avrupa'sından diğer insanlar Amerika'ya ilk gittiklerinde, oraya, onları uyuşturmak için afyon niteliğinde ne vermişler? Alkol vermişler ve onların topraklarını almışlar. Bugün ne veriliyor, dijital emperyalizm kendini hâkim kılmak için ne veriyor? Dijital içeriği bize veriyor. Bu dijital içeriği veriyor bize, biz bu dijital içeriği güzel bir şekilde tüketiyoruz ve gönüllü olarak verilerimizi biz de vermeye başlıyoruz.

Bu dijital içerik niye önemli? Çünkü kolay, değişik, hızlı, yaygın, çeşit çeşit, pahalı, bazen kaypak, bazen arkasında başka şeyleri gizleyebilir, psikolojiyi iyi kullanır, iyi hissettirir ve uyuşturur. Gerçekten de bugün kitap okuyan bir genç bulmak çok zorken, sosyal medyada iki dakikalık video izleyen genç bulmak çok kolay.

Bu noktada birkaç soru soralım yine.

Facebook'un bizim verilerimiz sayesinde aldığı reklam, hatta sattığı verilerden kazandığı parada bizim, yani veri sahiplerinin hakkı yok mudur?

Google'ın internetteki trilyonca sayfa sayesinde kurduğu imparatorluk sadece Google'ın ve vergi verdiği Amerika Birleşik Devletleri'nin midir?

Veri sayesinde bir bürokratın şantaj altında tutulması mümkün olamaz mı? Bu durumda bağımsızlık nerede kalır?

Geçmiş verinize göre hedeflenmiş sosyal medya reklamlarıyla vereceğiniz oyun rengi değiştirilebilir mi?

Bunlar da aklınızda soru işareti olarak kalsın.

Gerçekten de, ister veriyi alalım, ister verelim, bu tekeller mutlaka kazanıyor bugünkü dünyada.

Burada bir kavram daha getirmek istiyorum, o da şu: Dijital münhasır ekonomik bölgeler.

Münhasır ekonomik bölge nedir? Bana ait, bana özel ekonomik bölge; oradaki ekonomiyi ben yönetirim veya devlet. Burada da öyle bir şey var aslında. Veri, Dünya Ekonomik Forumu tarafından artık bir finansal varlık olarak kabul ediliyor. Peki, eğer veri de finansal bir varlıksa, bu dijital içerik şirketlerinin Türkiye Cumhuriyeti vatandaşlarının verisinden kazandıkları parada bizim de hakkımız yok mudur? Türkiye Cumhuriyetinin gayrisafi milli hasılası kabaca dünyanın yüzde 1.5'u seviyesindeyse, bu şirketlerin

kârının yüzde 1.5'unun da ülkemiz tarafından vatandaşları arasında paylaştırılması artık konuşulmaya başlanmalıdır.

Ancak, bunun karşısında başka bir aksiyon daha var, ondan da biraz haber vermek isterim. Japonya'da yapılan G20 toplantısında, DFFT isminde, Güven İçinde Özgür Veri Akımı diye bir öneri getirdiler. Bu öneri özetle şunu diyor: Hiçbir şekilde dijital platformların verilerinin akışını engelleyemezsin, yasaklayamazsın, verilerini nerede tutacağına karışamazsın. Bu öneriye karşı da ülke olarak çok dikkatli olmamız gerekiyor.

Bir diğer kavram, dijital dezenformasyon. Dijital dezenformasyon çok yoğun kullanılan bir alan. Bu da dikkat edilmesi gereken bir konu.

Bir diğer kavram, siber anarşi. Kısa tutayım, ama baktığımızda, Amerika Birleşik Devletleri'ndeki Trump'ın Twitter hesabının kapatılmasıyla sonuçlanan olaylarda büyük bir siber anarşi gördük. Türkiye'deki Gezi olaylarında da büyük bir siber anarşi gördük. Bu da önemli bir kavram.

Siber terörizm ve psikolojik savaş konusu var. Siber terörü şöyle ifade edebilirim: Korku yaratmak veya bir toplumu ideolojik bir amaç doğrultusunda sindirmek için, yeterli yıkıma veya bozulmaya neden olmak için, bilgisayar veya değişik ağları kullanan veya kullanılan siber saldırılar. Dolayısıyla, siber terörizm de işin başka bir boyutunda yer alıyor.

Dijital terörizm, siber terörizm çok önemli. Neden? Ucuz, anonim, hedef çok çeşitli olabiliyor; kamu, kişiler, kritik altyapılar, havayolları hedef olabiliyor; uzaktan yapılıyor, hızlı yayılıp, çok hızlı sürede çok fazla insanı etki altında bırakabiliyor. Bu anlamda oldukça kritik.

Bir diğer kavram da siber sivil savunma. Sivil savunmayı ortaokulda, lisede hepimiz konuşuyoruz. Lisede aldığımız milli güvenlik dersinde de bundan bahsedildi. Sivil savunma, bir savaş anına hazır olmaktır. Bu daha çok KBRN, yani kimyasal, biyolojik, radyoaktif, nükleer silahlar konusunda buna hazır olmak olarak anlatıldı. Peki, ya siber saldırılara karşı halk nasıl hazır olabilir? Bu anlamda da gerçekten bir güç oluşturmak önemli.

Şimdi burada bir soru daha soruyorum: Antivirüs kullanmayan, kaçak ve güncellemesiz yazılım kullanan, şifresini zayıf seçen vatandaşlar botnetlerin oluşmasına kolayca sebebiyet veriyorlar, bu açıdan ülkenin savunmasını zaafa uğratıyorlar. Peki, kendi bilgi güvenliğini sağlamak bir vatandaşlık görevi midir? Bir soru da bu olsun.

Siber savunmanın bu anlamda son derece kritik önemde olduğunu vurgulamak isterim.

Sonuçta, siber güç, siber dayanıklılık, siber caydırıcılık, siber savunma, siber kapasite, siber antipropaganda gibi birçok alt bileşenin bir bütünü.

Son olarak topyekun harbe de biraz değinmek isterim.

Dünya savaşları öncesinde, bir yerde bir savaş olduğunda, bir adam gidiyor, bu derebeyliğini ele geçiriyor, oranın yeni derebeyi oluyor; halk açısından pek bir şey değişmiyor, halk yine aynı yaşamına devam ediyor. Birinci Dünya Savaşından sonra, özellikle İkinci Dünya Savaşından itibaren ise, savaş, artık ülke halkının tamamının etkilendiği savaşlar haline dönüştü. Buna topyekun harp deniliyor. Topyekun harpte, ülke halk olarak da etkilendiği için, buna karşı durmayı da halk olarak yapmak zorunda. İşte siber sivil savunmanın önemi burada ortaya çıkıyor. Yani olası bir savaşta bunun mutlaka bir siber ayağı olacak. Siber ayağında ayakta durabilmek için, savunma, dijital, medya, sağlık, ekonomi ve sanayi alanlarında mutlaka güçlü olmak zorundayız.

Dijital vatanı koruyan sistemlerimizin yüzde 95'i bugün yerli değil. İyi bir haber vermek isterdim, ama maalesef böyle. Toplasanız, haydi 95 olmasın, 90 olsun. İyi bir durumda değiliz, ama gittikçe iyi hale geliyoruz.

"Yerli ve milli yetmez, artık uluslararası alanda güç gösterecek ürün ve şirketlerimiz olsun demeliyiz." Bu, Cumhurbaşkanlığı Dijital Dönüşüm Ofisinin açıklamasından bir söz. Gerçekten çok doğru. Yani sadece yerli olsun, bizim olsun, dünyada hiç kimse kullanmasın dediğimizde başarı mümkün değil. Dolayısıyla, uluslararası pazarda güç gösterecek ürünler çok önemli.

Millileştirme çok önemli. Dijital emperyalizm bizim için tehdit. Dijital dönüşümü ne kadar arttırırsak bu tehdit daha da büyüyor; çünkü daha da dijitale bağlı hale geliyoruz. Dolayısıyla, buna karşı durmak için de dijitalde milliyetçi olmak durumundayız.

Siber sivil savunma anlamında, Milli Eğitim müfredatına erken aşamalardan itibaren veri güvenliği dersini almak zorundayız.

Son olarak da şunu belirteyim: Türkiye Cumhuriyeti vatandaşlarının verilerini koruma sorumluluğu, nasıl ki toprağı ve toprağın altındaki varlıkları koruma sorumluluğu devletteyse, vatandaşın can ve malını koruma sorumluluğu devletteyse, bunun sorumluluğu da devlettedir.

Çalıştayın ruhuna uygun olarak böyle bir tanımlama yapmak istedim, umarım faydalı olmuştur. Dinlediğiniz için teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Oğuz Bey'e teşekkür ediyoruz.

Oğuz Bey, size sorumuz çok olacak; ama bu konuda ortak bir terminolojide birleşmek için artık şu kavramı bir değiştirelim. Siz söyleyin.

OĞUZ YILMAZ- Siber vatan diyelim.

OTURUM BAŞKANI- Siber vatan diyelim artık. Çünkü ortak terminoloji çok önemli. Çok teşekkür ederiz. Sizi Odamıza daha sık davet edelim, böyle rahat rahat daha çok toplantılar yapalım.

Evet, bir soru alalım.

Buyurun.

İSMAİL ...- Teşekkür ederim.

Ben İsmail ... Orman Genel Müdürlüğünde çalışıyorum.

Oğuz Bey'i dinlerken böyle şok vaziyette dinledim. Bu son derece önemli bir konu. Kavramlar konusunda çok iyi anlaşmak, uzlaşmak lazım.

OTURUM BAŞKANI- Evet, haklısınız. Çok teşekkür ederiz.

Soruların çok olacağını düşünüyorum, aralarda konuşalım diye düşünüyorum. Ama sizinle ayrı bir oturum yapalım hocam, orada daha uzun ve ayrıntılı konuşuruz. Teşekkür ederiz, çok sağ olun. (Alkışlar)

Bir sonraki konuşmacımız, Aykut Açıkgöz, EMCEKARE'den. Tabii ki olayın pek çok boyutu var, ama endüstriyel boyutu hepsinden daha önemli. Çünkü üretim yaptığımız birçok alan var. Aykut Bey de bu alandan bir temsilci.

Buyurun Aykut Bey, sizi dinliyoruz.

AYKUT AÇIKGÖZ (EMCEKARE Genel Müdürü)- Sayın Başkan, başkanlarım, değerli katılımcılar; hepiniz hoş geldiniz.

Ben Aykut Açıkgöz, elektronik mühendisiyim. EMO'da Yenilenebilir Enerji Komisyonu üyesiyim, aynı zamanda Kıraç Grup Yönetim Kurulu üyesiyim, EMCEKARE Genel Müdürlüğünü yapıyorum, aynı zamanda Elektronik Tesisat Mühendisleri Derneğinin de Yönetim Kurulu Başkanıyım. 25 yıldır endüstriyel otomasyon sektörüyle ilgili çalışıyorum ve bu alanda çok ciddi çalışmaları olan birisiyim.

Endüstriyel kısım şu ana kadarki toplantılarda, görüşmelerde hep bilgi güvenliği noktasında ele alındı. Ama bir endüstriyel tesis ele geçirildiği zaman başımıza neler gelebileceğini hiç düşündünüz mü? Bugün aslında bu konuya değineceğim. Örnek veriyorum, 31 Mart 2015'te yaşanan Türkiye'deki elektrik kesintisi. Siber saldırı değildi, teknik bir saldırıydı, teknik

bir problemdi; ama o gün Türkiye'nin herhalde yüzde 80'ine elektrik verilemedi. Yüzde 80'lik kısım içerisinde hayatımız felç oldu; ulaşım sistemleri çalışmadı, telekomünikasyon sistemleri çalışmadı, fırınlar çalışmadı, fabrikalar çalışmadı. Sanırım bize yaklaşık 1 milyar liralık falan bir maliyete sebep oldu.

Bunun farkındalığının önemini vurgulamak açısından ve bunun önüne geçebilmek anlamında Gökhay Bey'le birlikte bir sunum hazırladık. Ben endüstri otomasyon tarafında OT dediğimiz teknoloji içerisinde siber güvenlik meselesini anlatacağım, Gökhay Bey de IT tarafında uzman olduğu için o kısmı anlatacak.

Önce, kritik tesisler ve operasyonel teknolojiler altyapılarında siber güvenlik modelinin uygulanması ve işletilmesine yönelik bir çalışma yaptık. Biraz önce, hoca, siber vatan tanımını yapar mısınız dediğinde, aklıma şu geldi: Atatürk'ün bir sözü var, biliyorsunuz: "Her fabrika bir kaledir." Kalenin korunması lazım; hem fiziksel olarak korunması lazım, hem de aynı zamanda sanal ortamda korunması lazım. Başımıza neler gelebileceğini bir sonraki kısımlarda anlatacağız.

Bu konuyu anlatabilmem için önce EKS nedir, onun bir cevabını bulmamız lazım.

EKS, endüstriyel kontrol ve enerji sistemlerini programlanabilir logic controller, SCADA sistemleri, dağıtılmış kontrol sistemleri, DCS sistemleri gibi, programlanabilir ve bir tesisin devreye alınması ve otomatik hale gelmesiyle çalışan sistemlerdir. Bu sistemlerin olmadığını düşünün, bir çimento fabrikası olamaz, bir üretim tesisi olamaz, bir kâğıt fabrikası olamaz; bir alüminyum, bir demir-çelik fabrikası olamaz. Hatta biraz daha ileri gidelim, akıllı binalar olamaz. Yani ısımızı ayarlayamayız, meteorolojiyi ayarlayamayız, meteoroloji kurumlarından bilgi alamayız. Bundan dolayı, şu anda EKS dediğimiz elektronik sistemler hayatımızın her köşesinde var. Yani kullanmış olduğumuz telefondan tutun da, çalışmış olduğumuz santrallerdeki, çalışmış olduğumuz işyerlerindeki sistemlere kadar, tüm bunlar içerisinde hep var.

Peki, bu sistemler ne yapıyor? Bu sistemler sahadan bilgi alıyor. Sensörler, IND dediğimiz akıllı araçlar veya ölçülebilecek her noktadan bilgiyi alarak, bilginin prosesine göre tasarlayarak bir proses çözümü ortaya çıkartıyor. Bu proses çözümünün sonunda işte bir çimentomuz oluyor, bir ekmeğimiz oluyor, bir kimyevi gübremiz oluyor, yani bir ürün olarak çıkartıyor. Bunun için bizim özellikle bu tarafı ciddi anlamda korumamız lazım. Özellikle su,

elektrik, ulaşım, ürün imalat, endüstriyel otomasyon, petrol-gaz; tüm bunlar EKS'nin olduğu konular.

Şöyle bir söz var: Okul müdürüne soruyorlar: "Niye yönetemiyorsun okulu?" O da diyor ki: "Öğrenciler olmasaydı ben çok güzel okul yönetirdim."

Aslında Endüstri 4.0 olayı olmasa, fabrikalarımızda hiçbir şekilde siber güvenlik tarafımız olmayacak, ihtiyacımız da olmayacak.

1784 yılında buharın bulunmasıyla, ilk buhar makinesinin hayata geçmesiyle bir sanayi devrimi yaşanıyor. Sanayi devrimiyle birlikte Endüstri 1.0 1784 yılında başlıyor. Tabii, gelişim 1870'li yıllarda artıyor, elektriğin bulunmasıyla artık biraz daha hızlı üretim imkânı ortaya çıkıyor ve bununla da Endüstri 2.0 dediğimiz süreç başlıyor. Bu süreç 1969 yılında endüstriyel otomasyon ve elektronik kontrol sistemleri dediğimiz EKS sistemlerinin ön plana çıkmasıyla dönüşüyor ve Endüstri 3.0 devrimi başlıyor. Buraya kadar hiçbir şekilde siber güvenlikle ilgili veya siber vatanla ilgili bir durum söz konusu değil. Ta ki Endüstri 4.0 devrimi başlayıp, patronların, "Ben cep telefonumda üretim adedini görmek istiyorum, bir problem olduğunda bana e-mail gelsin" dedikleri ve fabrikalarımızı veya ilgili kontrol merkezlerimizi dışarıya açana kadar, işte o anda siber güvenlik olayı başlıyor. Bunlarla beraber, fiber optik haberleşme, kablosuz haberleşmesi, GPS haberleşmesi, aklınıza gelebilecek her türlü haberleşmenin üst segmentasyonda buluşması başlıyor. Yani benim verimi artık ben dünyaya açmış oluyorum. Açmış olduğum veriyi de bir şekilde korumam gerekiyor. Peki, bunu nasıl yapacağız?

Dijitalleşme olayında, şöyle söyleyeyim: Demiştim ki, ben OT tarafındayım; ben endüstriyel otomasyon sistemini yaparım, çalıştırırım. Ben hiçbir zaman yukarıya veya açık bir ortama vermediğim zaman, OT tarafım, benim fabrika alanım güvenli bir şekilde kalacak ve hiçbir şekilde benim verime dışarıdan bir ulaşım söz konusu olmayacak. Ama ben internete çıktığım zaman veya bir haberleşme altyapısına girdiğimde artık benim fabrikaları-

ma saldırır başlamış demektir.

Örneğin, sağınıza solunuza baktığınız zaman şöyle çok fazla GES işletmesi görüyorsunuz, güneş enerji sistemi işletmeleri. Bu güneş enerji sisteminde kaç tane ulaşılabilir nokta olabilir biliyor musunuz? Şöyle anlatayım: EPDK diyor ki, "Üretmiş olduğun enerjinin kalitesini bana bildirmek durumundasın." Oraya haberleşme için bir tane cihaz koyduk. EDAŞ, "Ben de üretmiş olduğun miktarı görmek istiyorum" diyor. İki tane daha koymuş olduk. İlgili teknik servis, "Ben uzaktan bu santrali görmek istiyorum, herhangi bir problemi var mı, yok mu diye" diyor. Bir de ona koymuş olduk. Üç nokta oldu. Bir de, asıl önemli noktası, GES işletmesinin sahibi, "Ben ne kadar para kazandığımı görmek istiyorum" diyor. Benim yapmış olduğum tesislerde, özellikle çıkartıyor telefonu, dakikada ne kadar para kazanmış, bunu gösteren üreticilerim var. Dolayısıyla, burada dört tane açık noktamız var. Yani dört tane açık nokta içerisinde girebileceğimiz kısım var. Yani örneğin, gerekli güvenlik önlemlerini almadığınız zaman, dışarıdan bu güneş enerjisi sistemini rahatlıkla durdurabilir, çalışamaz hale getirebiliriz. Güneş enerjisi santrali işin masum tarafı, bir de üretim fabrikalarındaki durumları düşünün. Dediğim gibi, 2015'teki elektrik kesintisi bir siber saldırı sonucunda olmuş olsaydı, bizim bu elektrik enerjisini verme sürecimizin ne kadar uzun olduğunu anlamış olurdunuz.

Peki, biz Gökay Türksönmez Bey'le birlikte niye buradayız?

Ben diyorum ki, ben OT'nin kontrolünü yaparım. Gökay da diyor ki, ben de IT'nin kontrolünü yaparım. Ama ortada bir tane siyah bölgemiz var. Bunu kim yapacak? Biz ikimiz bir oluyoruz, ben anlatmış olduğum endüstriyel protokolü Gökay'a anlatıyorum; diyorum ki, "Bende mod bas var, profil bas var, mod bas PCPI var" falan, aklınıza gelebilecek her türlü, ne bileyim, ICCP'den tutun da … kadar bir sürü protokolümüz var. Ben protokolün nasıl çalıştığını Gökay'a anlatıyorum. Gökay da bunu nasıl koruyacağını, gelen saldırılara karşı nasıl davranacağını artık öğrenmiş oluyor, ona göre de gereğini yapmış oluyor. Endüstriyel ortamlarda, endüstriyel otomasyon kısmındaki haberleşme protokolleri normal protokollerin dışında olduğu için, normal sistemlere göre endüstriyel otomasyon sistemleri daha az saldırıya uğruyor, ama uğradığı zaman da büyük kayıplar verebiliyor. Yani şunu söyleyebilirim: 2022 yılı itibarıyla Amerika Birleşik Devletleri'nde açıklanan raporlara göre, dünya genelinde endüstriyel tesislere yapılan siber saldırıların sonucunda 500 milyar dolarlık bir kayıp oluşmuş. 500 milyar dolarlık kısım gitmiş. Bu, bilinen kısım. Mesela bazı firmalar da prestij meselesi nedeniyle saldırıya uğradığını söyleyemiyor.

Ben aldım, endüstriyel otomasyon sistemimi kurdum, bunu korumak istiyorum ve IT tarafına geçtiğimde, bir otomasyoncu olarak IT bilgilerim az. Böyle bir durumda da beni koruması için Gökay Bey'e sözü veriyorum, o da onun IT tarafıyla ilgili kısımlarını açıklayacak, böylelikle interaktif şekilde devam edeceğiz.

Buyur Gökay.

GÖKAY TÜRKSÖNMEZ- İsmim Gökay Türksönmez, CBERNET Bilgi Teknolojileri firması Genel Müdürüyüm, aranızda bulunmaktan onur duyuyorum.

Endüstri 4.0'la birlikte, Aykut Bey'in şu ana kadar anlattığı dijitalleşme süreci, IT ve OT birimlerini yakınlaştırdı. Ama bu yakınlaşma bizim sahada yaptığımız analizlerde de tam bir yakınlaşmaya dönemedi. Bunun nedeni, bu alandaki üreticilerin ve bu alandaki haberleşme protokollerinin tamamıyla farklı olmasından kaynaklanmaktaydı. Peki, bu karanlık boşluğa ilk etapta kim girdi dersiniz; IT'ciler mi girmiştir, OT'ciler mi girmiştir? Böyle bir soru sorayım mesela.

OTURUM BAŞKANI- İkisi de girmemiştir.

GÖKAY TÜRKSÖNMEZ- İkisi de girmemiştir. Hocam, en güzel cevabı siz verdiniz. Çünkü o alana ilk girenler hacker'lar oldu. Çünkü haberleşme protokolleri endüstriyel alanda, mod baslar, profil baslar falan dizayn edilirken, aslında ilk etapta güvenlik ön plana alınarak dizayn edilmiş protokoller değildi, sadece işletme kolaylığı ve işletmeye yönelik protokollerdi. Dolayısıyla, hacker'ların bu alana girdiğini ve bu alanda tacizlere başladığını görüyoruz. Aslında 1982 yılından beri. Ben 1980 doğumluyum, ömrüm kadar bir süredir hacker'ların bu alanda cirit attığını söyleyebiliriz.

Peki, bu alandaki hacker profilleri nedir? Çok kısa geçeceğim bunları.

Hackistler; aslında aktivistin hack yapanına biz hacktivist diyoruz. Bugün İran'da mesela bir başörtüsü olayı var, İran'daki hacktivistler bir sürü tesisi hack'leyerek İran'daki yönetimin dikkatini çekmeye çalışıyorlar. Bu işi suç olarak yapanlar var, bunların haberlerine zaten sıkça rastlıyoruz. Genellikle fidye saldırısı kapsamında bu işi yapanlar var.

Insider'lar; bunlar aslında en tehlikeli grup. Insider dediğimiz şu: Aslında şirketimizin güvendiğimiz bir çalışanı; ama gerekli güvenlik tedbirleri alınmadığı zaman veya bunlarla ilgili bir bilinç sahibi olmadığı zaman, gafil muhbir olarak ya da kendi art niyetiyle de burada ciddi tehditler doğurabiliyor.

Burada siber güvenlikle ilgili Aykut Bey'in yaşadığı bir olay var, kendisi

kısaca anlatırsa sevinirim.

AYKUT AÇIKGÖZ- Şöyle: Sabah telefonum çaldı, saat 6.30-7.00 gibi, santralde büyük bir patlama olduğunu, parolanın yanlış olduğunu, patlamış olduğunu, acil müdahale edilmesi gerektiğini söyledi. Bu, 200 megavatlık bir santraldi. Patlama deyince benim aklıma şey geliyor, bir güç kaynağı patlamıştır, bir CPU patlamıştır falan. Daha sonra hemen şirkete geldim, durumu öğrenmeye çalıştım. Bir önceki gün bir çalışma arkadaşları işten çıkartılmış, bunlar da ana … panosuna, PLC kontrol panosuna koymuşlar ve patlatmışlar. Neyse. 200 megavatlık santralin o hasarını elimizdeki malzemelerle birlikte giderdik. 1 hafta içerisinde bunu yaptık. Ama şöyle düşünün: Oradaki üretim kaybı milyonlarca dolardı. Bu santrale herhangi bir siber saldırı olmuş olsaydı ve santrali vurmuş olsaydı ne yapacaktık? 200 megavatlık bir termik santralin yaklaşık olarak 50 bin IO'luk bir sistemi var. Yani bu 50 bin IO'luk sistem içerisinde de yaklaşık olarak 50 bin satırlık bir yazılım var, endüstriyel otomasyon yazılımı olarak. Eğer siber saldırı noktasında, siber saldırganlar programı değiştirmiş olsaydı, örnek veriyorum, bir kazanın olması gereken 100 santigrat derecelik seviyesini 500'e çıkartmış olsalardı, kazan bir şekilde patlardı ve inanılmaz derecede zararlar verirlerdi. Bu açıdan, benim yaşamış olduğum bu örneğin bir de siber saldırı tarafını düşününce, endüstriyel taraftaki zararın çok daha fazla olacağını düşünüyorum, onun için de dikkat etmek gerekiyor. Bu benim başımdan geçen bir olaydı, anlatmak istedim.

GÖKAY TÜRKSÖNMEZ- Bu aslında içerideki bir çalışanın yapabileceği yıkıcı etkiyi anlatmak içindi. Çünkü bütün kurumlar, bütün kuruluşlar içerideki çalışanlarına aslında güvenmekte. Siber güvenlik, insan inisiyatifine bırakılmayacak kadar değerli ve kompleks bir olay aslında. Ben kamuda uzun yıllar çalıştım, eski bir amirimin söylediği bir laf var, burada onu belirtmek isterim. "O insan hata yapabilir, hata yapmasının önüne geçebiliriz; ama önce izlemeliyiz, daha sonra da önleyici tedbirler almalıyız" diye bize verdiği direktifler sayesinde bir siber güvenlik stratejisi geliştirmiştik.

Espiyonaj, terörizmle savaş anlamındaysa siber saldırı, daha doğrusu bu profiller, aslında günümüzde yaşıyoruz. Rusya, şubat ayından beri resmen bir siber savaş yapıyor. Daha geçen hafta Zelenski bir açıklama yaptı, gurbetteki Ukraynalılara dedi ki, "Mart ayına kadar ülkenize dönmeyin; çünkü ben size enerji sürekliliğini ve enerji arzını sağlayamıyorum. Aslında 2015 yılında Black Energy ile başlayan Ukrayna'nın hedeflenme süreci vardı; ama bir türlü Ukrayna bunun önüne geçmedi veya geçemedi. Buna da dikkat çekmek isterim.

Peki, bütün bu anlattıklarımızın dışında siber tehdit hedef sahaları nelerdir diye baktığımızda, devletler ve özel sektör olarak karşımıza çıkmakta.

Kritik altyapılardan bahsedildi daha önceki sunumlarda. Biz, kritik altyapıların aynı zamanda stratejik altyapılar olarak değerlendiriyoruz. Stratejik altyapı dediğimizde; bir ülkenin enerji, su, askeri tesisler ve telekomünikasyon altyapılarının bir şekilde siber saldırganların hedefi olması ve başarıya ulaşmaları durumunda yıkıcı etkileri çok daha fazla olacaktır.

EKS olası saldırı vektörleri nelerdir?

Kurumsal bilgi ağına sızma. Bu genelde bir e-mail yoluyla, fishing yoluyla oluyor ve bu son derecede yüksek oranda başarılıyor.

Kurumsal bilgi sistemleri ağından yönetim ağına, yani SCADA sistemlerinin yönetilmiş olduğu ağa sızma.

Ve sahanın kendisine sızma.

Ekranda gördüğünüz siber saldırılar, 2010-2022 yılları arasındaki büyük olaylar.

Stuxnet zaten bir efsaneydi. Stuxnet, Springfield, Illinois'de olan su hizmetleri şirketine yapılan saldırı veya Puerto Rico'daki akıllı sayaçlara yapılan saldırılar daha çok içerideki, yani insider dediğimiz zafiyetten kaynaklanarak gerçekleşmiştir. Black Energy ile ilgili olanları az önce verdim.

Peki, dünya bunun için ne yapıyor? Dünya bunun için şunu yapıyor: Purdue Model diye bir güvenlik modeli uyguluyor. Bu model uluslararası standartlara uygun ve beş seviyede gerçekleşiyor. Burada da aslında şeyi görüyorsunuz, bu Purdue Modele rağmen hangi katmanda hangi saldırılar gerçekleşmiş, görüyorsunuz. Bu, Dragos firmasının geçen sene yaptığı bir istatistik yayını.

Peki, hal bu kadar kritik ve zorken, Türkiye'de durum nedir? Türkiye'de durum şu: Burada bir turuncu alan görüyorsunuz. Endüstri 4.0'la bu turuncu alan internete açılmıştı, daha doğrusu kurumsal ağ internete açılmıştı. Bizim aldığımız tek tedbir ise o ünlemin yanına bir tane koymak ve kuzey-güney trafiğini kontrol ettiğimizi sanmak oldu maalesef.

Bu bir endüstriyel kontrolün topolojisini göstermekte. Burada sürekli veriden bahsediyoruz; verinin işlenmesi, üretilmesi, işlenmesi, iletilmesinden bahsediyoruz. Burada kritik nokta şu: Endüstri 4.0'la birlikte ERP gibi sistemlerin artık içeriyle konuşur hale gelmesi; yani insandan uzak sistemlerin, insanın müdahalesine çok da açık olmayan, açık olan, ama çok da insan müdahalesi istemediğimiz sistemlerin gelişiyor olması var.

Bakanımız, konuşmasında, pandemiyle birlikte siber saldırıların artmasından, yüzde 300 oranında arttığından bahsetmişti. Uzaktan çalışanların erişmesi, yani remote control'e açık hale getirmeniz, bu siber saldırı yüzeyini son derece genişletti.

Bu alanda, Purdue Model üzerinde uluslararası standartlarda yapılan kontrollerde sıkılaştırmalar şunlar: Birinci olarak, varlıkların yönetimi. Yani içerideki varlıklarınızı şu başlıklar altında yönetmek zorundasınız. İ

kinci olarak segmentasyon yapmak zorundasınız. Bu arada, bunların hiçbirisi benim saha analizleri içinde görmediğim şeyler olduğu için söylüyorum. Koskoca bir fabrika tek bir … gibi çalışıyor. Dolayısıyla, saldırı yüzeyini sürekli arttırıyor oluyorsunuz.

Üçüncü olarak, erişim kontrolü. Erişim kontrolü, basit bir, hani şu IP grubu bu IP grubuna erişsin değil, artık IT'deki … benzer bir şekilde, kullanıcının uygulamaya erişeceği şekilde daha sıkılaştırılması gerekiyor.

Dördüncü olarak, kullanıcı yetkilendirilmeleri. Sağdaki birçok cihaz Windows X1, Windows 7 çalıştırıyor.

Aynı zamanda uzaktan erişim güvenliği. Sahadan artık operatöre yönelik, telefonun da güvenliğini bir şekilde alacak şekilde, kompakt şekilde yapabileceğiniz mekanizmalar mevcut.

Bütün bunları yaptıktan sonra da içerideki ağı sürekli izleyeceğimiz IPS mekanizmasını kurmak. Bunu da özellikle söylüyorum. Çünkü bu alanda IPS çok da uygulanabilir değil. Ve bu alanın 7/24 izlenmesi var.

En son olarak da OT-SOC yaklaşımının geliştirilmesi. Kurumların bunu merkezi düzeyde bir hizmet olarak alıyor olması önemli.

Burada Osman Başkanımız da var, IT tarafında da yıllarca çalışmış birisi olarak şunu da özellikle belirtmek istiyorum: OT-EKS tarafındaki siber güvenlik maalesef son derece prematüre seviyede. Bunun gelişmesi lazım.

Yine siber kümelenme denildi, bizim de böyle çalışmalarımız var. IBS sinyali olarak yazılması olabilir, burada bir uygulaması olabilir. Bunlarla ilgili çalışmaları da orta vadede planlıyoruz.

Arz ederim. (Alkışlar)

OTURUM BAŞKANI- Teşekkür ederiz.

Sizin siber vatan tanımınızı merak ettim. Siz endüstri açısından buna nasıl bakıyorsunuz?

GÖKAY TÜRKSÖNMEZ- Hocam, siber vatan dediğimizde, zaten burada tanımlar yapıldı. Vatan dediğimiz sınırları belirlenmiş alan içerisindeki toprak parçasıdır diye başladık 100 sene önce. Ama biz şunu şöyle değerlendiriyoruz: Vatanını en çok seven, görevini en iyi yapandır. Biz bu savunmanın neresindeyiz, endüstriyel kontrol sistemlerini kullandığımız alanlarda neredeyiz, müsaadenizle ben bu şekilde bağlamak isterim.

OTURUM BAŞKANI- Peki, teşekkürler.

Siz ne diyorsunuz Aykut Bey?

AYKUT AÇIKGÖZ- Hocam, ben şöyle söyleyeyim: Mustafa Kemal Atatürk'ün söylediği gibi, her fabrika bir vatandır. Biz dijital ortamda bunu algılıyoruz. Bu fabrika bizim için bir endüstriyel vatandır. Bunun korunması, sürekliliğinin sağlanması ve yeni nesillere aktarılması bizim için siber vatan savunmasının tanımıdır. Teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Ben teşekkür ederim.

Bir sonraki konuşmacımız, Sayın Mustafa Şenol. Konuşmasının konusu, "Siber Vatan ve Caydırıcılık." Olayın çok boyutu olduğunu görüyoruz. Farklı bakış açılarından bakıldığında aslında siber vatan tanımın içeriğinin gittikçe karmaşık hale geldiğini görüyoruz. Bu karmaşıklığı nasıl basitleştirebileceğimizle ilgili Mustafa hocamız konuyu toparlayacaktır diye düşünüyorum.

Evet, buyurun Mustafa Bey.

Dr. Öğretim Üyesi MUSTAFA ŞENOL (İstanbul Gelişim Üniversitesi)- Sayın hocam, Başkanım, değerli katılımcılar; hepinizi saygıyla selamlıyorum.

Bilgisayar çıktıktan sonra, internetin de yaygınlaşmasıyla birlikte bilgi ve iletişim sistemleri yaşamımızın vazgeçilmezi oldu. Siber uzay, siber ortam, bilişim sistemlerinin oluşturduğu ortam şimdi bir savaş alanı, harekat alanı olarak kullanılmaya başlandı. Bilgi gücümüz, teknolojik gücümüz artarken, tehlikeler de aynı hızla artmakta ve bu tehlikeler felaket boyutlarına da ulaşabilmekte. Dolayısıyla, siber uzay başta olmak üzere pek çok kavram ve terim de hayatımıza girdi. Kavramları, terimleri doğru bilmemiz ve aynı anlamda kullanmamız önemli.

Atatürk'ümüz, Sakarya Savaşı öncesi, "Felaket başa gelmeden evvel önleyici ve koruyucu tedbirleri düşünmek lazımdır. Geldikten sonra dövünmenin yararı yoktur" demiş. Ve bütün dünyada olduğu gibi, ülkemizde de bu siber tehlikelere karşı tedbirler geliştirilmeye başlanmış; savunma stratejileri, güvenlik stratejileri geliştirilerek, yasalar, politikalar bütüncül bir yaklaşımla ele alınmaya başlanmış. Vatanımızın sınırları siber uzayın sınırlarına ulaşmış durumda ve tehlikeleri de. Siber saldırılar ve risklerin, 1980'li yıllardan bugüne baktığımızda, şiddetleri, verdikleri zarar, hasar, karmaşıklığı oldukça artmakta, daha da artmaya devam etmektedir.

Peki, saldırganların bilgi-teknik kapasitesi ne durumda? Yansıda görmektesiniz.

Dünyada pek çok saldırılar yaşandı, yaşanmakta, yaşanmaya da devam edecek. Ülkemizde de saldırılar, suçlar, olaylar yaşandı, yaşanmakta ve yaşanmaya devam edecek.

Saldırılarda neler yapılabilir, nelere sebebiyet verebilir bu saldırılar? Hepimiz biliyoruz, ama kısaca özetlersek; haberleşme sistemlerinden tutun da, elektrik, bankacılık, ulaşım, doğalgaz, barajlar ve nükleer santraller dahil pek çok hasarlar, zararlar verebilir. Bunların verdiği hasarlara, zararlara baktığımızda, bunun adı savaş ve siber ortamda bunun adı siber savaş.

Siber savaş için, ağ savaşı için, internet aracılığıyla bir saldırı için küçük bir bağlantısı yeterli olmakta. 50 dolarlık bir siber silah, milyonlarca dolarlık uçağın, füzenin verebileceği zararı vermekte. Biraz önceki sunumlarda da bunu gördük. Bit ve baytlar, mermiler ve bombalar kadar tahrip edici olabiliyorlar.

Strateji diyoruz, yasa diyoruz, politika diyoruz. Strateji, hedefe giden, gücümüzle hedefe ulaşmamızı sağlayan anayoldur. Geçmişte bu savaş sanatıydı, günümüzde artık bir bilim dalı. Ve ulusal güç unsurlarımızı bir stratejiyle belirleyerek hedefe ulaşmaya çalışmaktayız. Ulusal gücümüzle, ulusal güç unsurlarımızla hedefe varmaya çalışmaktayız. Buna sekizinci güç unsuru

olarak siber güç de dahil olmuş durumdadır.

Siber güç nedir? Siber ortamda sahip olduğumuz bilişim sistemleri ve altyapıları ile bunların etkin kullanılması yeteneğidir. Yani siber güç, siber savaş ve caydırıcılık gücümüzü oluşturmakta.

Siber uzay tanımlarını yapıyoruz. Baktığımız zaman, fiziksel tarafı var, sanal tarafı var. Fiziksel tarafı daha çok donanımlar, sanal tarafı da yazılımlar ve işletim sistemleri. Bunlar bizim değerli varlıklarımız. Şu anda perdede gördükleriniz bizim siber vatanımızı oluşturmakta. Ama burada, perdede bir eksik var: Kullanıcılar. Konuşuyoruz, ama üzerinde çok durmuyoruz gibi geliyor bana. Kullanıcılar da fiziksel tarafı oluşturmakta. Siber vatanımızın güvenliğini düşünürken kullanıcıların da güvenliğini düşünmek zorundayız.

Caydırıcılık diyoruz. Caydırıcılık yeni bir kavram değil. Milattan Önce 500'lü yıllar. Sun Tzu, Çinli stratejist, komutan, "En iyisi savaşmadan baş eğdirmektir veya savaşmadan savaşı kazanmaktır" diyor. Aradan yaklaşık 1000 yıl geçmiş, Anadolu'da yaşayan Doğu Romalı komutan Belisarius, "En mükemmel ve mutlu zafer şudur: Kendiniz zarar görmeden, düşmanı amacından vazgeçmek zorunda bırakmaktır" demiş. Atatürk'ümüz, savaşın bir cinayet olduğunu, zorunlu-yaşamsal nedenlerle olması gerektiğini, ulusal yaşam tehlikeyle karşı karşıya kalmadıkça da cinayet olduğunu vurgulamıştır. Yani savaşmadan baş eğdirmek zorundayız.

Günlük hayatta caydırıcılıkla her gün çok farklı örneklerle karşılaşmaktayız. Hukuk alanında, diplomasi alanında, askeri alanda tabii ki caydırıcılık uygulanmakta.

Siber caydırıcılık da siber ortamda saldırganı caydırmaktır. Zararlarını arttırmak ve faydalarını azaltarak, onu saldırmamaya baştan ikna etmek, saldırıyı hiç düşünmemesini sağlamaktır.

Siber ortamda caydırıcılık, nükleer ve fiziki ortamda caydırıcılıktan hemen sonra gelmekte. Nükleer caydırıcılık, karşı tarafın silahlarının gücünü biliyorsunuz, sizde de var, kolay. Ama siber caydırıcılıkta karşı tarafı tespit etmeniz zor, gücünü de bilemeyebilirsiniz. Onun için siber caydırıcılık çok zor. Tartışmalar devam ediyor. Siber savaşın savaş olmadığını söyleyenler de var, siber caydırıcılığın mümkün olmadığını söyleyenler de var. ABD'nin nükleer caydırıcılığı sağladığını, ama siber savaş açısından caydırıcılık sağlayamayacağını; onun için, "Siber saldırı durumunda askeri tedbirler dahil bütün güç çözümlerini kullanırım" diye bütün dünyaya açıkladığını biliyoruz.

Peki, siber caydırıcılık bu kadar zorsa, nasıl sağlayacağız? Aslında iki bölümü var. Biri, saldırganın saldırısını önlemek, boşa çıkarmak. Diğeri de bunu cezalandırmak.

Nasıl önleyeceğiz, nasıl boşa çıkaracağız? Şu ana kadarki konuşmalarda da söylendi, siber istihbarat, yani saldırganı tespit etmek için gerekli güç ve onu tespit ettiğimiz zaman, onun saldırdığını ispatlamamız gerekiyor. Ona yönelik olarak istihbarat yaparak saldırganı önlemek, ön almak, ön alıcı tedbirleri uygulamak, bunun için güven sağlamak gerekiyor. Bütün bunların hepsi aslında siber güvenlik ve savunmayla mümkündür.

Cezalandırma dedik. Karşı taraf bizim gücümüzü bilecek ve saldırı yaptığında karşılaşacağı yaptırımı bilecek, bunu duyuracağız karşı tarafa. Bizim bunu yapabilmemiz için de saldırı yapana saldırı yapabilmemiz gerekiyor, yani taarruz gücümüzün yüksek olması gerekiyor. Bunun için de kararlılık gerekiyor. Misilleme konusunda hem gücümüz olacak, hem de bu tedbirleri oluşturduğumuz stratejiyi kararlılıkla uygulayacağız.

Bu iki bölümü üç aşamada uygulayabiliriz. Birincisi, saldırganın eylemini boşa çıkarma, yani güvenlik sağlama tedbirleri. Geçmişte savaşlarda bu surlarla, duvarlarla olmuş; günümüzde güvenlik duvarı, saldırı tespit ve önleme sistemleri vesaire diyoruz. Bunları hem kullanıcı boyutuyla, hem donanım, hem yazılım boyutuyla yetkin bir şekilde uygulamamız gerekmekte, ki karşı taraf bizim güvenliğimizi görünce saldırmaya cesaret edemesin. Saldırganı tespit edip… Tabii, önce bunu duyuracağız, saldırırsa tespit edeceğimizi karşı taraf bilecek. Bunun için yine her bakımdan yeteneklerimizin geliştirilmesi gerekiyor ve tespit ettiğimizde de bunun bedelini ona ödeteceğiz. Bu üç aşamayı uyguladığımız takdirde caydırıcılığımız siber ortamda da mümkün olacaktır.

Perdede "Siber Savaş" kitabının yazarı Richard A. Clarke'ın ortaya koyduğu

bir tablo var. Richard A. Clarke bir çalışma yapmış. Tabloda beş tane ülke var. Taarruz konusunda, savunma konusunda değerlendirdiğimizde, örneğin taarruz konusunda en güçlüsü hangisidir diye sorsam farklı cevaplar çıkacaktır. Bu çalışmaya göre taarruz konusunda en güçlüsü ABD görünmekte. Peki, savunma konusunda? Evet, farklı cevaplar çıkıyor yine. Savunma konusunda en düşük puan 10 üzerinden 1 ile ABD'nin. Kuzey Kore 7. Peki, bağımlılık? Bağımlılık konusunda, en bağımlı olan ülkeye en düşük puanı verecek olsanız? En bağımlısı ABD, en düşük puanı almakta. Bu tabloya baktığımızda, bu rakamları topladığımızda, en güçlüsü, en yeteneklisi Kuzey Kore çıkmakta. Yani savunma açısından güçlü olabilirsiniz, taarruz açısından da güçlü olabilirsiniz; ama bağımlılık sizin gücünüzü tüketmekte.

Strateji belgelerimize baktığımızda, ulusal siber güvenlik strateji belgelerimize ve eylem planlarımıza baktığımızda; ilk 2013-2014, sonra devam ediyor. İçeriğine baktığımızda, siber caydırıcılık konusu 2013-2014'te geçmiyor. Ama ana amaçlara, eylemlere baktığımızda, bunları gerçekleştirdiğimizde siber caydırıcılık sağlarız. Kâğıt üzerinde kalmazsa, bunları gerçekleştirirsek, uygularsak, caydırıcılık sağlarız. 2016-2019'da, siber suçlarla mücadelede suçluların caydırıcılığı konusunda eylemlerde de bazı hususlar bulunmakta. Ki bu kapsamda, 2016-2019 strateji belgesi kapsamında Bilgi Teknolojileri İletişim Kurumumuza caydırıcılık görevi verildi. Kamu kurumu ve kuruluşları ile gerçek ve tüzel kişilerin siber saldırılara karşı korunması, saldırılara karşı caydırıcılık sağlanması için her türlü tedbiri alma veya aldırma görevi verildi. Bu kapsamda yetkileri var, cezalar dahi uygulayabilmekte. Ve aynı tarihlerde Başbakanımız da dedi ki, "Siber saldırılarda caydırıcılık geliştirilecek." Başka çalışmalar da yapıldı bu kapsamda. Müteakiben, 2020-2023 strateji belgemizde sekiz ana eylem başlığında siber suçlarla mücadelede caydırıcılık konusu daha ayrıntılı olarak yer aldı. Bilgi Teknolojileri İletişim

Kurumumuza, saldırıların engellenmesi, caydırıcılığın sağlanması konusunda görev ve yetki veren o kanun değişikliği de strateji belgemizde yer aldı. Caydırıcılık konusunda, suçlara karşı caydırıcılığın geliştirilmesi dahil, proaktif savunma kavramı da strateji belgemizde yer alarak; caydırıcılığın sağlanması, ön alıcı tedbirler, saldırgan daha düşünürken tedbirlerin başlamasının vurgulanması, bu konudaki tedbirlerle gücümüzün artması ve ekosistem dedik, sadece ilgili birimler değil, bütün gücümüzle, kurum-kuruluşlarımızla bu tehditlere karşı tedbirlerin arttırılarak caydırıcılığın sağlanması strateji belgemize girdi.

Sonuç olarak; sadece savunmayla savaş kazanmak mümkün değildir. Ön alıcı tedbirler önemli. Caydırıcılık, söyledim, üç aşama çok önemli. Bilgi Teknolojileri İletişimi Kurumumuzun tek başına caydırıcılık görevini sağlaması oldukça zor diye düşünüyorum. 6331 sayılı İş Sağlığı Güvenliği Kanunumuz var. Görüyoruz, bu konuda gerekli tedbirleri almayanlara cezalar da uygulanmakta. "Önce Emniyet" tabelaları var. Siber güvenlik konusunda da böyle zorunluluklar olması gerekir, bu konuda bir kanun çıkması gerekir ve her alanda koordinasyonu sağlayacak tedbirler alarak uygulanması gerekir. 2016-2019 strateji belgemizde, siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi oluşturulması konusu vardı. Bu konuda güçlü bir kamu otoritesi, koordinasyonu sağlayacak güçlü bir otorite olmak zorunda. Yani kurumlar görevlerini yapıyorlar, ama bu konuda sıkıntılar yaşamıyor muyuz? Evet, yaşıyoruz. Bir öneri olarak, Siber Güvenlik Başkanlığı teşkil edilerek, Siber Güvenlik Koordinasyon Kurulu ve Uzmanlar Danışma Kuruluyla birlikte, böyle bir teşkilatla, tek elden, tek merkezden bu koordinenin sağlanması daha iyi olabilir diye düşünüyorum.

Atatürk'ümüzün sözü çalıştayımızın bildirgesinde de yer almakta. Bütün yurdu, kurum-kuruluşları, herkesi kapsayan bütüncül bir yaklaşımla ulusal siber güvenlik diyoruz. Siber vatanın korunması için, yurtta siber güvenlik, dünyada siber güvenlik.

Dinlediğiniz için teşekkür ediyorum. (Alkışlar)

OTURUM BAŞKANI- Teşekkür ediyoruz Mustafa Bey, çok sağolun.

Bir sonraki konuşmacımıza geçiyoruz. Bir sonraki konuşmacımız, Sayın Dr. Hüseyin Bayazıt. Kendisini Cumhurbaşkanlığı Bilim Teknoloji ve Yenilik Politikaları Kurulunun düzenlediği bir etkinlikte tanıdım. Siber güvenlik stratejisi geliştirmede çok farklı bir bakış açısı var, toparlayıcı olacağını düşünüyorum.

Buyurun Hüseyin Bey.

Dr. HÜSEYİN BAYAZIT (Alaaddin Keykubat Siber Akademi Vakfı Danışmanı)- Efendim, siber vatan konusu, çok boyutlu, çok katmanlı, çok aktörlü bir olay. Burada bakış çok önemli. Mesela suyu ele alalım. Suyun üç tane hali vardır. Katı halinde Newton'un mekaniği geçerli, sürtünme katsayısı çok az. Maddenin ikinci haline geçtiğiniz zaman, sıvı haline, akışkanlar mekaniği geçerli. Üçüncü hale, gaz haline geçtiğinde ise termodinamik yasaları geçerli, kapalı sistem ve açık sistemlisi çok çok farklı. Yani bir paradigma değişikliği şart. Türkiye'de bunun olmadığını zaten biliyoruz. Bunun için de bazı şeyleri yeniden tanımlamak gerekiyor. Şeref Sağıroğlu hocanın ontoloji tanımına bakmanızı şiddetle tavsiye ederim, çok çok önemli.

Efendim, benim esas amacım ontoloji kavramının oturtulması ve paradigma. Paradigmanız olduğu zaman, yeni kavramlar, yeni teoriler, yeni modeller geliştirirsiniz. Tıpkı Einstein'ın e=m.c2 ile, kuantum fiziğiyle Newton'dan dönüşümü gibi.

İkinci amacım, biraz önce Sayın Mustafa Şenol hocam söyledi, psiko-sosyal; gönüllerimizi, zihinlerimizi ne işgal ediyor, onu da örneklendireceğim. Yani o kadar katmanlı ki, bizi dumura uğratıyor. Değerlerimizde, düşünce sistematiğimizde, inanç sistemlerimizde, ibadetlerimizde, masallarımızda, hepsinde. Çok katmanlı, çok boyutlu, çok faktörlü bir olayla karşı karşıyayız.

General Valery Gerasimov, "Artık savaşlar ilan edilmeden yürütülüyor" diyor. Yani vekalet savaşları, beşinci nesil falan, bunları göreceğiz.

Yine Amerika Birleşik Devletleri Kara Kuvvetleri Komutanı diyor ki, "Siber alan gelecek yüzyılın muharebesini belirliyor."

Siber vatanda modern orduların yaklaşımına bakalım.

Birincisi, Türkiye'de, nasip oldu, ağ destekli yetenek artışları konusunu, şebeke merkezli muharebe ve operasyonlar konusunu Silahlı Kuvvetler Akademisinde ders olarak verdim. İkincisi, etki tabanlı harekât ya da etki tabanlı muharebe. Muharebenin siber vatanda dört boyutu vardır. Birincisi, biraz önce anlattıkları gibi, fiziki alan. İkinci alan, bilgi alanı. Üçüncü alan, insan veya zihin. Dördüncü alan da sosyal alan. Sayın Dr. Mustafa Şenol hocam ne dedi, çok önemli; psiko-sosyal gücümüzü dağıtıyorlar. Göreceksiniz, örneklerle göreceksiniz.

Bakın, bu, bildiğimiz fiziki alandaki siber uzayın... Bakın, birincisi, uzay. Uzayda bir sınır yok bence. İkincisi, hava vatan. Üçüncüsü, kara vatan. Dördüncüsü, mavi vatan.

Buraya baktığınız zaman, bütün boyutlarıyla görüyorsunuz.

Bakın, deniz. Mavi vatan. Bakın, sathın altında da güvenlikle ilgili, siber vatanla ilgili şeyler var. Mavi vatanın da sathının altında çok değerli madenler var. Bunun sathına kadar olan yer mavi vatan. Mavi vatanın bütün sınırlarının üstünden yukarıya doğru çıktığınız zaman gök vatan. Kara vatanımız da dâhil olmak üzere. Bakın, elektromanyetik spektrumun ele geçirilmesi çok önemli. Biliyor musunuz, Rusya'yı maymun ettiler Ukrayna'da, elektromanyetik muharebeyle. Ruslar kabak gibi ortada kaldılar, bu da pek basına yansımadı.

Evet, görüyorsunuz muharebe biçimleri. Mavi vatan, kara vatan, gök vatan, uzay vatan. Elektromanyetik spektrumun üzerindeki operasyonlar. Amerikan Deniz Kuvvetlerinin FORCEnet denilen tesisleri.

Muharebe sınıflandırılması ve türleri.

Beşinci nesil, bilişsel muharebe. Psiko-sosyal gücünüzü hedef almıştır.

Entropi temelli muharebe. Duydunuz mu? Harp akademilerinde de anlatıyorum bunu.

Bakın, algoritma temelli muharebe.

Epistemolojik, füzyon, sosyolojik, dördüncü nesil muharebe, beşinci nesil muharebe.

Gıda, ekonomik, finans, kur, su savaşları, genetik, sağlık, medya... Bakın, 1992'de Rand Cooperation, "Bilişsel alan muharebesi var" diyor. Tahayyül, değerler oluşturma, düşünme, davranış ve iletişim süreçleri, medya...

Etki tabanlı harekatın tanımı: Dost, düşman, tarafsız ve kardeş ülkelerin karar vericilerinin, kanaat önderlerinin ve o toplumun üzerindeki etkili kişilerin düşünce, davranış, metafor denilen benzetmeler, kullandığı dil, düşünme biçimi, masallarını, misallerini, efsanelerini, destanlarını, fıkralarını, ibadet biçimlerini, inanç sistemlerini değiştirmektir. 33 tane şeyi var. Bunu ben söylemiyorum, NATO ve İngiliz talimnameleri söylüyor.

Ne kadar karmaşık bir yapıyla karşı karşıya olduğumuzu anlatabiliyor muyum?

Bunlar basit, ama ontolojik bakış en önemlisi.

Bakın, kognitif alana bakın şimdi.

1985 yılında iki tane verilen frekansın sonucunda insanın haletiruhiyesini değiştirdiğine dair araştırmalar yapıldı ve Zbigniew Brzezinski York Üniversitesinde hocaydı, daha sonra Eski ABD Ulusal Güvenlik Danışmanlığına geçti, şunu söyledi: "Bundan sonra artık uluslararası ilişkilerde beyin/zihin önemli bir alandır." Söylediği tarih 1985.

Dr. Jacques Benveniste, bu çok önemli, suyun DNA vesairesini alıyor ve suya sürekli bir madde atıyor, milyonlarca kez yapıyor, değiştiriyor suyu, bakıyor madde orada ve yine değiştiriyor falan. Sonunda suya zehir atıyor. Zehirli suyun içine sineği atıyor, sinek ölüyor. Daha sonra o zehrin frekansını içeren bir sinyal yolluyor suya. Zehir falan yok. Yolluyor frekansı, sinek ölüyor. "Aynı şekilde, bu sinyali internet üzerinden yollayabiliriz" diyor.

Tehdidi görebildik mi arkadaşlar?

Psiko-akustik...

Bakın, Sayın Cumhurbaşkanımız biliyor. Sadece Türkiye Cumhuriyeti tarihinde değil, dünya seçim tarihinde de hiç bu kadar kararsız seçmen yüzdesi olmadı. Psiko-akustik, psiko-nörotik, psiko-farmakolojik, psiko-linguistik, psiko-semiotik, psiko-semantik silahlar var. Siber uzayı kapsayan bütün araçlarını icra ediyor ve kararsız seçmen yüzdesini arttırıyor.

Gelelim ontolojiye.

Bilgisini elde etmek istediğimiz siber vatan nasıl bir gerçekliktir, olgudur? Ontoloji, siber vatan denilen bir olgu üzerinde nasıl bir şey yaratıyor. Tıpkı terör, terörizm, terörist de olduğu gibi. Terörizm bir fikirdir; fakat bataklığı kurutmazsanız sivri sinekler ürer. Terörist kim? Sivri sinek. Terörizm ne? Sıtma. Bunların hepsini bir arada düşünmek zorundayız. Mesela tıp. Evet, ortopedi var, kulak-burun-boğaz var, güzel de, hepsi aynı taksonomiyi... Karaciğerimiz mesela, karaciğer bir kimya fabrikasıdır. Peki, karaciğer... Bakın, üç tane kavramı iyi bilmemiz ve kavramamız lazım. Bu vücudu oluşturan bütün nesneler neyse, onların sahip olduğu ... nedir, direkt olarak tabiatına bağlı. ... sahip olduğu karakterdir. Bir de fiiliyatı vardır, orayı ileride göreceğiz.

Ontoloji, bu siber vatan denilen kavramı neler oluşturuyor, bunların arasındaki ilişkiler ne vesaire vesaire ve bunların hepsinin sonunda çeşitlerini ve yapılarını temsil etme, tanımlama, ilişkilendirme ve bütünleşik bir tarzda tüm boyutları, alanları ve aktörleri entegre etme disiplinidir.

Benim, siber vatan denilen, bilgisini elde etmek istediğim olguyu ne oluşturuyor, aralarındaki ilişki işte burada. Ondan sonra epistemoloji. Recep Şentürk, benim eski dostum, o da Columbia Üniversitesinde sosyolojide doktora yaptı, İbni Haldun Üniversitesinin eski rektörü, "Açık Medeniyet" kitabını okuyun. Multipleksi, ontoloji multipleksi, epistemoloji multipleksi diye kavramları var. Bunlara böyle bakmazsak elimizde patlar arkadaşlar. Bu bakış açısı çok önemli. Paradigmayı değiştirmek zorundayız. Tıpkı suyun üç halinin olması gibi.

John Lock, ontolojiyi dünyada ilk kullanmıştır. Bakın arkadaşlar, "atom bombası, batılı aklın şeytani aklın ürünüdür". John Lock, şu anda dünyadaki batılı akıl budur. Kendi çıkarları için. Yalnız batı'da değil, bizde de öyle. Nefs-i emmare ve nefs-i levvame. John Lock aldı, ontolojiyi öyle kullandı. 1700'lerde. Bakın, onların yarattığı insan modeli bütün dünyaya, tabiata zarar verdi. Dünya tarihinde insanoğlu hiç bu kadar tabiata zarar vermedi. Onun içinde, ontolojik baktığınız zaman, aynı kafayı görürsünüz. Ümmet nedir? Bütün kainattır. Benim için. Ümmet, bütün kainattır. Bu, insan olmanın, mümin olmanın bedelidir. Müslümanlığı geçelim, o ayrı.

Bilgisini elde etmek, bunu anlattık. Epistemoloji. Hangi bilgiyi istiyorum, ne tip bilgi istiyorum? Buldum ontolojisini. Hangi tip bilgiyi elde etmek istiyorum, metodolojim nasıl? Vahdette kesret, kesrette vahdet. Batı'da böyle bir şey yok. Göreceksiniz, tehdidi zihinsel alanda göreceksiniz arkadaşlar. Bildiğimi bilirim, bilmediğimi bilmem. Bazı konularda cahilimdir, ama bildiğimi bilirim.

Ontolojinin amacı: yeni bir müştereklik/ortak yaklaşımı ve bakış. Aynı resmi görebilme. Ortak akıl. Musalla sürüsü diyor, ortak akılla hareket edin. Ortak bir dil. Stratejik, operatif ve taktik seviyelerdeki planlamacılar ve idareciler için ortak sözlük. Göreceksiniz, bunu batı yapıyor; NATO yapıyor, Amerikan ordusu yapıyor, Güney Afrika yapıyor, İsveç-Norveç yapıyor. Ortak sözlük, ortak hareket resminin stratejik, operatif ve taktik seviyelerde oluşturulmasının temeli. Ortak anlam birliği. Ortak ve kontrol edilen terimler. Doktrin yazıcıları için. Ortak harekât resmi, operasyonu nasıl görüyoruz. Ve durumsal farkındalık. Hem askeriyede hem de iş dünyasında kullanılır. Ve durumsal anlama ve aynı zamanda semantik birlikte çalışabilirlik. Bunları yaratıyoruz. Kargaşa gidiyor, zamandan kazanıyorsun, hızlı akıl. Yapay zeka, diğer yeni bilgi teknolojileri dediğimiz, big data, big structure, veri analitiği vesairesi. Big data olmadan olmaz bu iş. Big structure, o büyük datayı ontolojik görürseniz, istihbaratta, terörde, iş dünyasında, finansta, o zaman hızlı bir şekilde çözüm üretirsiniz. İstihbarat da böyle düşünüyor,

terör de böyle düşünüyor, iş dünyası da böyle düşünüyor. Şimdi örneklerini vereceğim.

Modern orduların ve NATO'nun ontoloji kullanma örnekleri. Buyurun.

Bakın, Threat Assessment. Hepsine ontolojik bakış olmadan aklınızı alırlar arkadaşlar. Batı, Kur'an aklıyla düşünüyor, Kur'an algoritmasıyla düşünüyor. Kur'an nedir? Varlık ve ben ilişkisi. Gidin bakın. Umberto Eco delildir diye bakın, adamlar kullanıyor. Vebal altındayız. Tehdit büyük. Benim derslerim K'ye kadar gider; komuta kontrol, elektronik harp, bilgisayar korsan harbi, siber harp, ekonomik temelli bilgi harbi, istihbarat temelli harp, psikolojik harp. Sonra sosyal medya. Vebal altındayız. Vicdansız, ontolojiyi almış. Bakın, hocamla konuştum geçende bunu. Kur'an'da yazmıyor mu kâinat genişliyor diye; aldı adam, koydu, Nobel Fizik Ödülünü aldı. Vicdan yoksa, sen rahmani. İyi ile kötünün arasında bu savaş sürecek. Kötü bol. Ben Amerika'da mürekkep yaladım, iyi tanırım o batılı aklı. Arkasından İngiliz'in kendi çıkarı için tanrıcılık oynayan, Yunan felsefesine, Yunan mitolojisine yaslanan, batılı aklı, latin, grek, kilise ... kafayı anladık.

Buyurun, işte müşterek harekât ontolojisinin oluşturulması. Hocam, hani dedik ya, ontolojiyi kurarsak, tanımı yaparız. Bakın, hepsi burada. Bütün bu harekatların temeli. Amerika Birleşik Devletleri bunu her yerde kullanıyor. Aynı zamanda Harvard Business School'da anlatılıyor.

Buyurun. Kullanılan kaynakların ve personelin takibi için sıcak çatışmanın ontolojik olarak temsili. Lojistik paketi yolda tak buraya giderken oraya yolluyorsun, acil diyor, iş bitti. Böyle anlattık derslerde. Focus lojistik'te. Buyurun, bakın. Ontolojik.

Muharip ontolojisi. Buyurun, kaynak da burada.

Alın, durumsal anlama, durumsal farkındalık.

Alın, ortak doktrin hiyerarşisi.

Birlikte çalışabilirlik. Biraz önce operasyon merkezini, siber güvenliği gösterdiniz. Siz de kullanabilirsiniz. Herkese hitap ediyor.

Buyurun. Uzay operasyonları, siber. Ayaklanmaya karşı koyma doktrini dümeni altında, kurmaylara anlatıyor, ayaklanma nasıl yaratılır.

Buyurun, General Petreaus, ayaklanmaya karşı koyma ontoloji alanı. Daha çok başımıza çorap örerler, çuval geçirirler. Kur'an aklıyla bakıyor arkadaşlar, Kur'an algoritmasıyla düşünüyor. Zaman-mekân-kuvvet etkileşimini böyle gösteriyorlar. Ama batılı aklı.

Anlatabildim mi arkadaşlar?

İstihbarat ontolojisi. Gelsin bir istihbaratçı arkadaş, hiç kusura bakmayın, bazı konularda mütevazı olamayacağım, bir-iki iş gördüm tek başıma, iddia ediyorum ki daire başkanı yapamaz. İstihbarat paradigması değişti. Çok elimizde patlatırlar. Konvansiyonel anlamda yok. 15 Temmuz'u planlayanlar -çoğu öğrencimdi- ve ondan sonraki kişiler bildiğimiz konvansiyonel harekât planlaması paradigması dışında, özel eğitilmiş ve aynı zamanda istihbarat anlayışı verilmiştir. Onun için, işi çözerler, alttaki gariplere oldu olan. Deve dişlerini alamıyoruz, alamayız da. Çünkü onlar bizim konvansiyonel terör, konvansiyonel istihbarat ve konvansiyonel harekât planlama anlayışıyla değil, çok farklı bir anlayışla eğitildiler.

Bakın, istihbarat bilgi ontolojisi. Zamanında, anında.

Askeri planlama ontolojisi.

Biyolojik silahlar ontolojisi.

Buyurun, bir terörist de alıyor, ontolojisini kuruyor. Bakın. Koy buna yalanı ziyanı, yanına da Toyota'yı yapıştır, bak bakalım ne. Yoksa 34 kişiyi boşuna öldürmediler.

Anlatabildim mi arkadaşlar? Terörle mücadelede kullan, sosyal medyada kullan, sosyal medya teröründe kullan, psiko-sosyal gücümüzü etkileyen terörde kullan, iş dünyasında kullan.

Al işte NATO. Examples of ontological military models. Model ne demek? Gelir modeli vardı, iş modeli vardı, bir de operasyon modeli. Al, buyur. NATO modellemesi; komuta kontrol, istihbarat sistemlerinde. Eski bunlar arkadaşlar. Ben bunları 2014'ten önce anlatıyordum.

Alın, uzay gözetleme ontolojisi sensör görevlendirme şeması. Buyurun. Hava kuvvetleri. İHA-SİHA'larda. Yazılımda çok önemli. Yapay zekâ algoritmasıyla beraber big datayı öyle indirirsiniz. 15 senedir bu işi anlatıyorum.

Sivil, ticari ve istihbarat alanlarında ontolojinin kullanılması örnekleri.

Buyurun, siber güvenlik zafiyetleri yönetimi. Sosyal medya istihbaratı arkadaşlar, bir bakın, sosyal medyada büyük işler dönüyor. 2017 seçimlerinde Sayın Cumhurbaşkanımıza bu psiko-semantik, psiko-sosyal, psiko-nörotik temelli muharebe diye konuyu anlattık ve dedik ki, 2017 seçimlerinde.

Bakın, ben hiçbir partili falan değilim, değişik bir insanım, nevi şahsına münhasır biriyim. Vicdanım hür, fikrim hür, irfanım hür. Tevfik Fikret söylemiş. Bakın, bu ülkenin, bu devletin, bu insanın ve ümmetin sevdalısıyım ben, biraz da oradan gelen bir coşkuyla çalışıyorum.

Bakın, bunları toparlayamazsak... Bizde var bunlar. Algoritmayı kim bulmuştu?

SALONDAN- Harezmi.

Dr. HÜSEYİN BAYAZIT- Bravo. Harezmi. Eee? Senin ceddinde var. Horasan'dan, Semerkant'tan, Buhara'dan. Şah Muhammed Nakşibendi Hazretlerini yetiştirdi. Buruni. Bizde bu. Algoritmasız olmaz bu modeller. Ontoloji kuramadın mı? Bizim genlerimizde. Basit bir iş. Nereden buluyorum? Kafayı taktım, hemen, hemen anlıyorum. Benim genlerimde var, var bende. Batı'da yok bu, Batılı akılda yok.

Bakın, A Cognitive Approach to Detect Cybersecurity Events. Ve bakın, IBM kullanıyor bunu arkadaşlar, bir sürü şirket kullanıyor. Bakın, burada ne kadar büyük bir big data uzayı var. Google'da, orada burada yapıyor bunu istihbaratı.

Bakın, Güney Afrikalı yapıyor arkadaşlar. Ontolojisini kuruyor; model, hedefler, büyüklük, amaç, sınıflandırma. Buyurun, istihbaratta kullanın. Beyin yakarak. Beni niye yakmıyor? Yakacaksınız. Paradigma değişikliği zordur. Bakış açısı. Bitti. Bir sürü anlattık. İstihbaratta, terörde, iş dünyasında. İş dünyasında da var bu.

Bakın, bilgi güvenliğine yaklaşım diyor, hepsini anlatıyor. Böyle düşünüyor insanlar.

Bakın, güvenlik varlık tehdidi veya zafiyeti ontolojisi. Yani benim karaciğerim bundan bunu alıyor, buna veriyor, bundan bunu çatıyor, atıyor oradan. Tıpta da arttı bu. Geleneksel tıp var ya, bildiğimiz, onların hepsi epistemolojik. Esas önce ontolojisini kuracaksın.

Bu anlamda hocama teşekkür ederim, yırtındık şeyde. Bizim Türkiye'den 15 kişiydik, çatladım ontolojiyi anlatmaya, sonunda hocam anladı bir tek ve ilgilendi. TÜBİTAK falan vardı. Böyle. 2000'li yıllardan beri var.

Bakın, güvenlik algoritmasına kadar gidiyor. Çok verimli. Bunları bildiğiniz zaman gerisi geliyor zaten. O zaman, tık tık tık, biraz zorlanırsın, ama siber vatan için bu yaklaşım kaçınılmaz.

Bakın arkadaşlar, CIA bu algoritmayı sosyal ayaklanmalarda kullanıyor. Bizde Gezi'de niye hemen uygulanmadı? Ama biz uyanıyoruz artık. Yaptık da, bilen bilir. Bizim kafa ontolojik düşündüğü için. Bakın, bazı şeyler var. Mesela… Ben keçi çobanlığı yaptım. Bizim Burhaniye'de Septik Tepesi karardığı zaman, keçi kuyruğunu kaldırdığı zaman, 1 saat sonra yağmur yağar. Yağmur yağacak, keçi haber veriyor. Onun için milyarlarca dolarlık modellemeler falan değil, keçiye baktım, Septik Tepesi karardı, 1 saat sonra yağmur yağacak, hemen eve.

Bakın, open source, açık kaynaktan verileri topladıktan sonra… Bakın, kredi kartları, sizin yaptığınız Google'daki araştırmalar, Facebook'taki paylaşımlar falan, hepsini topluyor, kurmuş ontolojisini, 5 gün önceden toplumsal ayaklanmaları görüyor ve ona göre tedbir alıyor. Bizde de öyledir ha.

Siber vatan tanımına geldik. Buna dijital vatanı da koyabiliriz, bazı şeyler entegre oluyor. Biraz önce Mustafa Şenol hocamın da söylediği gibi, bütün o güçleri ilgilendiriyor siber vatan. O çok önemli, psiko-sosyal. Bunu anlatabildim mi; zihinlerin işgal edildiğini, zihnin hedef olduğunu, toplumsal değerlerimizin hedef olduğunu?

Siber vatan, çok boyutlu, çok alanlı, çok Kamanlı, çok aktörlü bir olgudur. Beş boyutu vardır; mavi vatan, kara vatan, gök vatan, uzay vatan, bilgisel ve teknolojik vatan. Altı, dijital vatanla da iç içedir bence. Kavramsallaştırma çok önemli arkadaşlar. Onun için paradigma, onun için ontolojik bakış, Kur'an aklıyla görüş. Kur'an'dan ayrı nizam anlamam. İş bitti. Tekvin yasaları okunsun. Tekvin kitabı vardır; Bunun da Batı'da karşılığı semiyotiktir. Her yerde kullanıyorlar. Hepimizi maymun ettiler.

Siber vatanın dört boyutu var; fiziki, bilgi/içerik, bilişsel ve toplum/millet. Psiko-sosyal da diyebiliriz.

Altı alanı var. Bir, toplumun karar vericileri. İki, toplumun organik altyapısı. Bireylerin yaşamı için elzem olan enerji ve gıda üretimi ve tedarik zincirleri, sağlık, ilaç, aşı, tıbbi cihazlar. Bunlar iç içe. Yani bizim toplumun organik altyapısı var. Üç, tüm alanlardaki kritik altyapı tesisleri. Dört, savunma, güvenlik, asayiş ve istihbarat birimleri. Bunlar da siber vatan için. Yani altı alan bu. Dört boyut, altı alan.

Toplum dedik; maddi ve manevi değerler sistemi, inanç sistemi, kullanılan

dil; masal, destan, efsane, hikaye ve fıkralar; metaforlar, ibadet biçimleri.

Tüm veriler, bilgiler ve içerikler. Ar-ge faaliyetleri. Bunların hepsi siber vatanın alanları içerisinde.

Özetle; siber vatan, "dört boyut ve altı alandaki ilişkileri, bağıntıları, süreçleri, olayları, karakteristik özellikleri ve nesnelerin türlerini, tiplerini, çeşitlerini ve yapılarını temsil eden, tanımlayan, ilişkilendiren ve bütünleşik bir tarzda tüm boyutları, alanları ve aktörleri entegre eden bir çatıdır."

İnsan-Fikirler (Bilgi/İçerik)-Teknoloji

Bir, insan. Ne oldu Endülüs'teki insan modeli? Gittim, gördüm. Evlad-ı Fatiha'mız Bosna'da yedi düvel üzerimize çullandı, aslan gibi durdurduk. İnsan. İnsan, insan, insan. Sonra fikirler. Bakın, bilgi/içerik üretiyoruz. Atatürk'ün bir sözü var, milli eğitimde maksat, orada burada kullanılan bir süs aracı vesaireden daha çok, "esas maksat, gerçek maksat bilgiyi cihaza dönüştürmektir" diyor. Teknoloji yapın diyor. İnsan, fikirler, ondan sonra teknoloji.

Teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Sağ olun hocam, çok teşekkür ederiz.

Vaktimiz kalmadığı için soru-cevap bölümünü yapmayacağız, öğlen arasında bunu yaparız.

Şimdi konuşmacılarımıza birer plaket takdimimiz olacak, ona geçiyoruz. Katıldığınız için teşekkür ederiz.

Kapatmadan önce Sayın Osman Coşkun hocamızın söylemek istediği birkaç husus var, sözü kendisine bırakıyorum.

Prof. Dr. OSMAN COŞKUN (Cumhurbaşkanlığı Bilim Teknoloji ve Yenilik Politikaları Kurulu Üyesi)- Teşekkür ederim hocam.

Öğleden sonra sizinle olamayacağım için birkaç bilgiyi sizinle paylaşmak istedim.

Öncelikle Şeref hocama ve arkadaşlarına çok teşekkür ederim, çok önemli bir konuyu gündeme almışlar.

Hüseyin hocam Endülüs'ten bahsetti. Müslümanlar İspanya'yı fethettiği zaman ilk üniversiteyi kuruyorlar ve bu üniversitenin kapısına da beş maddelik bir kitabe yazıyorlar. Bir devletin ayakta kalabilmesi için bu beş maddeyi sağlaması gerekir deniliyor.

İlk sıradaki madde: "Güvenlik kuvvetleri güçlü olmalıdır". Burada siber gü-

venliği gündemimize aldığımıza göre, eğer bir devlet ayakta kalacaksa, siber güvenlik anlamında güçlü olmak zorundayız. Dolayısıyla, bu program son derece önemli.

Diğer dört maddeyi de izninizle söyleyeyim.

İkincisi, "devleti yönetenler bilgili olmalı deniliyor". Yani birinci sırada silah var, ikinci sırada bilgi.

Üçüncü sıradaki madde: "Devletin hazinesi altınla dolu olmalı". Yani para. Üçüncü sırada para var.

Dördüncü sıradaki madde: "Devleti yönetenler adaletli olmalı diyor".

Bakın, o dönemde üniversiteyi kurmuşlar, ama batı'da ilkokul bile yok. Beşinci sırada da, o ülkede "ağzı dualı insanlar olmalı" deniliyor. İşte Akşemseddin'lerden, Şeyh Edebali'lerden, ecdadımızdan bunu görmüş durumdayız.

2000'li yıllarda, ... içerisinde olduğu bir fütürist grup, bir devletin ayakta kalması için ne gerekir diye bir çalışma yaptı. Üç madde tespit ettiler: Bir, silah. İki, bilgi. Üç, para. Tabii, kıymetli Hüseyin hocam hep bahsediyor ya, batı, evet, Kur'an aklını kullanıyor, ama Kur'an vicdanı yok. O yüzden işte binlerce insanın katledilmesi gündeme geliyor.

Tabii, cumhurbaşkanlığı başkanlık sisteminde politikayı kurullar belirliyor. Bu kurullardan bir tanesi de Bilim Teknoloji ve Yenilik Politikaları Kurulu. Bu kurulun başında Sayın Cumhurbaşkanımız var; kurulda, TÜBİTAK Başkanımız, ben, ASELSAN Genel Müdür Yardımcımız ve bir arkadaşımız daha var, beş kişi birlikte çalışma yapıyoruz. Yaklaşık 4 yıldır çalışan bu kurul bir çalışma yaptı. TÜBİTAK'ın tüm çalışanlarının, ASELSAN çalışanlarının, akademisyenlerimizin desteğiyle 27 teknoloji alanı tespit edildi. Yani kısa, orta ve uzun vadede odaklanılacak 27 teknoloji alanı. Bunun ilk sırasında siber güvenlik var. Dolayısıyla, siber güvenlik, hem çocuklarımız, hem gençlerimiz, hem bilim insanlarımızın yoğun bir şekilde odaklanması gereken bir alan. Bilim Teknoloji Yenilik Politikaları Kurulu olarak, bilgisi olan gençlerimiz ve bilim insanları ile finansı bir araya getirip, önlerini açıp, bunun çıktıya dönüşmesi, teknolojinin ortaya çıkması için çalışmalar yürütüyoruz. Bu konuyla ilgilenmek isteyenler bana ulaşabilir. Google'da Osman Coşkun telefon diye yazarsanız, telefon numaramı bulabilirsiniz. En kötü ihtimal, Milletvekili Osman Coşkun diye de yazsanız cep telefonumu bulabilirsiniz. "Benim bir projem var, finans ihtiyacım var" diyorsanız, finansör bulup onun çıktıya dönüşmesine katkı sağlıyoruz. Bununla ilgili yaşadığımız çok

acı, çok güzel örnekler var, ama zamanımız çok kısıtlı olduğu için burada paylaşamıyorum. Bunu DARPA Amerika Birleşik Devletleri'nde kurumsal olarak yapıyor. Ama şu anda bununla ilgili de kurumsal bir çalışmamız var, bir rapor hazırladık, Cumhurbaşkanımıza sundum. Yani bizde bilgi de var, sizler gibi çok güzel bilim insanlarımız var, finans da var; ama koordinasyon eksiğimiz var.

Şeref hocama çok çok teşekkür ediyorum. Kendisi aynı zamanda benim öğrencim olur. Bu güzel çalışmaları yaptığı için kendisiyle de gurur duyuyorum burada, huzurlarınızda. Cumhurbaşkanlığı Siber Güvenlik Politika Belgesinde de, kendisinin başkanlığında, akademisyenler, kamu temsilcileri ve özel sektör temsilcileriyle birlikte, çok güzel bir şekilde ülkemizin politikasını hazırladılar. Bu konuda da gerçekten çok teşekkür ediyorum. Sabrınız için sizlere de teşekkür ederim. (Alkışlar)

SİBER VATAN, SİBER GÜVENLİK ve SAVUNMA OTURUMU - 2

Oturum Başkanı:

Taha YÜCEL / Bilgi Güvenliği Derneği Başkanı- ASELSAN Genel Müdür Yardımcısı

Hatice Bİlge ALGIN / EMO Ankara Şubesi 26. Dönem Yönetim Kurulu Yazman Üyesi

SUNUCU- Değerli konuklar; etkinliğimizin öğleden sonraki oturumuna hepiniz tekrar hoş geldiniz.

"Siber Vatan, Siber Güvenlik ve Savunma" başlıklı ikinci oturumumuzu yönetmek üzere, Bilgi Güvenliği Derneği Başkanı ve aynı zamanda ASELSAN Genel Müdür Yardımcısı Sayın Taha Yücel'i Divandaki yerine davet ediyorum.

Buyurun.

OTURUM BAŞKANI- Sayın Başkanım, değerli katılımcılar; hepinizi saygıyla selamlıyorum.

Öncelikle böyle güzel bir mekânda bu kadar kritik bir toplantıyı için Elektrik Mühendisleri Odasını, değerli Başkanını tebrik ediyorum. İnşallah hayırlı bir toplantı olur.

Bugün 4 değerli konuşmacımız var. Daha önceki oturumlardan sarkmalar nedeniyle, biraz da süreyi doğru kullanma adına on beşer dakikalık 4 konuşma, 15 dakika soru-cevapla 15.00'e kadar inşallah konuyu toparlarız diye umuyorum. Hızlıca değerli konuşmacıları davet edeceğim.

Bu oturumumuzun ana konusu, Siber Vatan, Siber Güvenlik ve Savunma.

Burada en kritik olan konu -muhtemelen sabah da tartışılmıştır- bizim siber güvenliğimizin sağlanması, verilerimizin korunması. Konunun öneminin hepimiz farkındayız ve onun için de buradayız. Burada çok kritik, yani Türkiye'nin verilerinin bir şekilde ülkemizde muhafaza edilmesi, mümkün olduğu kadar kontrollü bir şekilde paylaşılması önemli. Yine savunma alanında siber güvenlik çalışmaları anlamında Milli Savunma Bakanlığımızın çok önemli bir yönergesi var. Bu yönergeden haberi vardır çoğu arkadaşımızın. Milli Savunma Bakanlığı Savunma Sanayi Güvenliği Yönergesi var, MSY 317-2C Yönergesi. Bunun da gizlilik bölümü var. Orada gerçekten aslında hepimiz için mesajı olacak bir tanımlama ve görevlendirme var, özellikle savunma sanayiinin siber güvenliğinin sağlanması için. Tabii, biraz zorlaştıran yönü var, ama orada özetle diyor ki, "Enerjideki iletim, iletişim ve veri hatlarında dışarıdan müdahale ve bilgi sızmasına engel olacak güvenlik tedbirlerinin alınması." Aslında biz bunu sağladığımız zaman zaten güvenli bir ortam oluşturacağız. Ama tabii, bu kadar güvenli bir ortam oluşturunca da bu sefer bazı çalışmaların dışarıdan yapılmasında zorluk oluyor, savunma sanayiinde uzaktan çalışma meselesinde ciddi zorluklarımız oluyor. Bunları çözebilecek mekanizmaları da oluşturmamız lazım. Yani çok aşırı korumacı olduğunuzda, bu sefer hayatın bize dayattığı ve gerçekten olması gereken uzaktan çalışma hepimiz kaybediyoruz ve belki de eleman kaybediyoruz bu nedenle. Yani sadece uzaktan çalışma yapamadığımız için kaybettiğimiz elemanlar var, savunma sanayi şirketlerinin. Bunların mekanizmalarını bulmamız lazım. Yani hem olabildiği kadar güvenli olacağız, hem de gerçekten hayatın getirdiği teknolojik avantajlardan istifade edeceğiz.

Sözü hemen Yusuf Bey'e veriyorum. Yusuf Tancan Bey, Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı Birim Müdürü.

Buyurun Yusuf Bey.

YUSUF TANCAN (Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Dairesi Başkanlığı Birim Müdürü)- Sayın başkanlarım, sektörümüzün kıymetli temsilcileri, saygıdeğer misafirler, değerli katılımcılar; öncelikle Siber Vatan ve Savunma Çalıştayının hazırlanmasında emeği geçen herkese teşekkür ederek başlamak istiyorum. Hepinize hoş geldiniz diyorum.

Teknolojinin hayatımızda meydana getirdiği dönüşüm hız kesmeden devam ediyor. Yenilikçi teknolojiler düşünme, davranma ve iş yapma şekillerimizi de hızlı bir şekilde dönüştürüyor. Ekonomide, yönetim anlayışında, eğitimde, medyada, sosyal hayatın birçok alanında köklü dönüşümleri hep

birlikte yaşıyoruz ve yaşamaya devam edeceğiz. Yakın bir zamana kadar bilimkurgu olarak kabul ettiğimiz, gördüğümüz, filmlerde izlediğimiz birçok şey hızla bilimsel gerçeğe dönüşmeye başladı. Fiziksel ve dijital ortam giderek iç içe geçiyor. Başlangıçta sadece kişisel bilgisayarlardan ibaret olan siber uzay, mobil telefonlarla akıllı cihazlardan sonra haberleşme yeteneği kazandırılmış milyarlarca nesneyi de dijital ikizleriyle insan dâhil gerçek dünyadaki her şeyi içine alarak, tıpkı fiziksel uzay gibi genişlemeye devam ediyor. Geleceğin teknolojileri hepimiz için harika imkânlar sunmakla birlikte, yeni riskleri de doğal olarak beraberinde getiriyor. Bu teknolojiler güvenlik bakış açılarını da kökten değiştirmiş durumda.

Teknolojiye en hızlı ayak uyduran grupların başında suç örgütleri geliyor. Bu durum düşünüldüğünde, önümüzdeki süreçte siber tehditlerin daha da çeşitleneceğini, kompleks bir hal alacağını, karmaşıklaşacağını ve sıklaşacağını öngörmek çok da zor değil. Teknolojinin insana faydalı olan yüzü yanında, suç örgütlerinin elinde etkili bir silaha dönüşen yüzü, mücadele edilmesi gereken bir tehdit olarak her zamankinden daha ciddi bir şekilde karşımıza çıkmakta. Siber saldırıların seyrine baktığımızda, geçmişte daha sade yöntemlerle, basit amaçlarla, belirli yetkinlikteki kişiler tarafından ve kısıtlı kaynaklarla gerçekleştirildiğini görüyoruz. Saldırganlar genel olarak kendini ispat veya propaganda gibi, artık masum diye niteleyebileceğimiz motivasyonlarla hareket ediyordu geçmişte. Günümüzde ise saldırılar artık devletler düzeyinde, yapay zekâ destekli otomatize araçlarla yıkıcı ve hedef odaklı olmaya başladı; saldırı motivasyonları da çıkar sağlamak, casusluk ve zarar vermek gibi amaçlara dönüştü. Boyut ve karakter değiştiren siber tehditler artık bir siber savaşa dönüşerek, kritik altyapı ve sistemleri birer hedef haline getirdi. ... teknolojilerle birlikte daha da karmaşıklaşan siber saldırılar kritik sistemlere kilometrelerce uzaktan ciddi hasarlar vermeye başladı. Bu saldırılar bazen tek başına, bazen de geleneksel savaş araçlarıyla birlikte simetrik, asimetrik veya hibrit savaş yöntemlerinin bir

unsuru olarak kullanılmakta, tarafların askeri ve siyasi hedeflerine ulaşmasında etkin rol oynamakta. Sonuçları ise sadece sanal ortamda değil, fiziksel ortamda da görülebilmekte; geleneksel savaşta olduğu gibi, can ve mal kaybına sebep olabilmekte.

Son 10 yılda siber saldırılarda meydana gelen artışın dijital ortamdan daha az kaynakla, daha az riskle, daha kısa zamanda daha fazla saldırı yapmak ve bir ülkeye karşı stratejik koz elde etmekle doğrudan ilişkisi var. Bu saldırılarla haberleşme sekteye uğratılabilmekte, bankalar çalışamaz hale gelebilmekte, şehirler elektriksiz kalabilmekte, sahte belgelerle itibar kayıpları yaşanabilmekte. Saldırıların birçoğunun sosyal medya ve diğer iletişim kanalları kullanılarak şekillendiğini görüyoruz. Sosyal mühendislik teknikleriyle kaos ortamı oluşturulması sağlanmakta, bu şekilde toplumsal düzenin bozulması hedeflenmekte.

Siber saldırıların artık bir savaşa dönüşmesi, ülkelerin tıpkı sınırları gibi dijital altyapılarını da korumasını giderek daha da zorunlu hale getirmeye başlamış durumdadır. Bu noktada, geçmişten bu yana süregelen bir soru, bir tartışma konusunu belki gündeme tekrardan getirmek lazım. "Siber güvenlik nasıl sağlanır, siber güvenlik sağlanabilir mi? Yasayla mı sağlanır, teknolojiyle mi sağlanır?" gibi geçmişten bu yana süregelen bir soru hâlâ gündemimizde. Esasen şunu peşinen kabul etmek lazım: Tıpkı gerçek dünyadaki gibi, burada nasıl yüzde yüz güvenli değilsek, siber uzayda da yüzde yüz güvenlikten bahsetmek teorik olarak mümkün değil. Peki, o zaman biz niye bu kadar uğraşıyoruz, bu kadar insan bu alanda niye kafa patlatıyor? Yasalar çıkıyor, yönetmelikler çıkıyor, genelgeler çıkıyor, teknolojiler geliştiriliyor, insan kaynakları yetiştirilmeye çalışılıyor. Bütün bunlar boşuna mı? Buna verilecek cevap şu olabilir: Siber saldırıların yıkıcı etkisinden uzak durmak. Yani saldırıyla karşılaşmamak değil, saldırıya muhatap olmamak değil; bu saldırıların yıkıcı etkisinden uzak durmak veya engellenebilenleri engellemek. Hep konuşulan bir örnek var; "Kurumlar ikiye ayrılır; siber saldırıya uğrayanlar veya siber saldırıya uğradığını veya uğrayacağını henüz bilmeyenler, henüz fark etmemiş olanlar" gibi. Siber güvenliği sağlamanın sadece bir boyutu olmadığını peşinen söylemek mümkün. Öğleden önceki oturumlarda zaten değerli konuşmacılarımız bu alanda ne kadar kompleks ve karmaşık bir yapının olduğunu üstüne basa basa anlattılar. Dolayısıyla böyle kompleks bir yapının içerisinde giderek genişleyen, büyüyen bir siber uzayın içerisinde, "Siber güvenliği sadece şunu yaparsanız sağlarsınız, yasal düzenlemeyi dörtdörtlük yaparsanız sağlarsınız" diyebilmek çok doğru bir yaklaşım değil. Genel itibarıyla ülkelerin siber güvenlikle ilgili olgunluk seviyelerini ekranda gördüğünüz şu 5 ana başlıktaki çalışmalarla

değerlendiriyor endeksle ilgilenen kuruluşlar: Bir, organizasyon yapısı. İki, yasal düzenleme. Üç, teknoloji. Dört, insan. Beş, ulusal ve uluslararası işbirliği. Bu unsurların her biriyle ilgili atılacak doğru ve bilinçli adımlarla ancak siber saldırıların yıkıcı etkisinden uzak durmak mümkün. Ülke olarak çeşitli kurumlarımız vasıtasıyla bu boyutların her birine yönelik çalışmaları yürütüyoruz. Bu boyutları bir zincirin halkaları gibi de düşündüğünüzde, burada teknolojinin en güçlü unsur olduğunu görüyoruz, organizasyon yapısının en etkili unsur olduğunu görüyoruz; ama bütün zincirler gibi, bu zincir en zayıf halkası kadar güçlü. Buradaki en zayıf halka da yine insan. Dolayısıyla insan hem bu zincirin müstakil bir halkası, hem de diğer halkaların yöneticisi veya kullanıcısı, bir şekilde hepsinin içerisinde ve odağında. Dolayısıyla siber saldırıların yıkıcı etkisinden uzak durması, esasen bu zincirin içerisinde insan faktörünü gerek kullanıcı olarak, gerek yönetici olarak, gerek geliştirici olarak ne kadar güçlendirdiğinizle doğru orantılı.

İstatistiklere baktığınızda, siber saldırıların yüzde 85'ini ortama saldırılar teşkil ediyor. Bu durum düşünülüğünde diyebiliriz ki, siber tehditlerden korunması gereken en kritik sistem insan, çünkü saldırı doğrudan insana yapılıyor. Saldırganlar, teknolojik önlemleri aşmaya çalışmak yerine, daha kolay ve maliyetsiz olan sosyal mühendislik yöntemleriyle insan bileşenini zafiyete uğratmayı tercih ediyor. Teknolojik önlemleriniz ne kadar güçlü olursa olsun, insan faktöründeki bir zafiyet... Çünkü saldırgan için tek bir zafiyet yeterli. Dolayısıyla onu en kolay bulacağı noktaya yöneliyor saldırgan. Dolayısıyla buradaki en zayıf noktamız insan. Bizim her alanda, yönetici, geliştirici, üretici, kullanıcı noktasında siber güvenliği bir kültür haline getirmemiz gerekiyor, bir yaşam biçimi haline getirmemiz gerekiyor. Dolayısıyla geçmişten bu yana gelen klasik soru, "Siber güvenlik yasal düzenlemeyle mi sağlanır, teknolojiyle mi sağlanır?" sorusunun cevabı, hiçbiriyle tek başına sağlanmaz; en kritik ve en zayıf

halkayı güçlendirerek, oradaki halkaların her birine yönelik doğru adımları atarak ve en zayıf halkayı da güçlendirerek, bunu bir yaşam kültürü haline getirerek... Sağlanır diyemeyeceğim, yüzde yüz sağlanamayacak. Bunu da zihinlerimize yerleştirmemiz lazım. Çünkü siber uzay sürekli genişliyor, milyarlarca nesne geliyor ve güvenlik temelli bir tasarım anlayışı olmadan bağlantılı hale getirilen bütün nesneler yeni zafiyetler ve yeni saldırı yüzeylerinin oluşmasına sebep oluyor.

Ülkelerin endekslerdeki durumuna bir göz attığımızda, Haziran 2021 tarihinde yayınlanan Ulusal Siber Güvenlik Endeksinde genel tablo bu şekilde. Türkiye burada 11. sırada, ama üzerinde 15 tane ülke var. Bu, esasen tek bir gösterge değil, aslında tek başına doğru bir gösterge de değil; çünkü farklı ölçüm kriterleriyle, farklı yaklaşımlarla farklı sonuçlar da çıkıyor. Bir sonraki slaytta onu da göstereceğim. Bu rapor 2 yılda bir yayınlanıyor. Bir önceki raporda Türkiye, dünya genelinde, 194 ülke arasında 20. sıradaydı, şu an 11. sırada görünüyor. Elbette bir gösterge, ama tek başına bir ölçü değil. Çünkü buradan, 1. sırada olan Amerika'nın siber saldırılara maruz kalmayacağı anlamı çıkmıyor. Belki de çok daha aşağılardaki bir ülkeden daha fazla siber saldırıya maruz kalma ihtimali var. Bu ölçüm yapılırken, az önce gösterdiğim 5 kategoride değerlendirme yapılmış ve Türkiye'nin gelişmeye açık tek unsuru organizasyon yapısı. Diğer unsurların hemen hemen tamamında tam puana yakın bir değerlendirme almışız, organizasyon yapımız.

YUSUF TANCAN- Aslında burada kapasite geliştirme şeklinde geçiyor, ben onu slayta alırken insan olarak aldım. Kapasite geliştirmenin içinde insan da var, teknolojik de var, eğitim ve farkındalık da var.

Esasen buradaki kapasite geliştirmenin içerisinde insan, unsurlardan sadece bir tanesi. Yani teknolojik kapasite geliştirme ve diğer unsurlar falan da var.

Bir başka endeks. Bu yeni yayınlandı, eylül ayında yayınlandı. 2022 yılındaki Siber Güç Endeksi Raporuna göre, Türkiye bu kez 30 ülke içerisinde 23. sırada gösterilmiş. Bu endeks hazırlanırkenki kriterler biraz daha farklı. 8 parametre göz önünde bulundurulmuş. Finansal parametreyi her ne kadar bu sene eklemiş olduklarını söyleseler de, puana etki etmediğini de belirtmişler. Aslında bu endeks şekil açısından değil, fonksiyon açısından bir değerlendirme yapmış. Finansal gözetim, istihbarat, ticaret, savunma, bilgi kontrolü, ofansif yeteneği veya standartlar açısından değerlendirmelere göre, Türkiye burada 23. sırada yer almış.

Burada hemen hızlıca aktarmak istediğim bir slayt var. Biz ofis olarak ulusal siber güvenlik yönetişim analiziyle ilgili bir çalışma başlattık. Türkiye incelemesini gerçekleştirdik. 30'a yakın kurumun 60'a yakın mevzuatını inceledik. Bununla birlikte, az önceki endeks sonuçlarında Türkiye'nin puan olarak üzerinde bulunan bazı ülkelerin de hem mevzuat, hem organizasyon yapısı açısından nasıl yapılandıklarıyla ilgili bir çalışma yaptık. Vakit az olduğu için çok hızlı bir şekilde özet bir bilgi aktaracağım. Bunlarla ilgili önümüzdeki Aralık ayının 14'ünde, kamu kurumlarımızla bir çalıştayımız olacak. Hem Türkiye'nin mevcut mevzuat yapısını, hem de organizasyon yapısını, dijital altyapılardaki siber saldırılara karşı mukavemeti arttırma noktasında nasıl bir yapılanma olması gerektiğiyle ilgili bütün kamu kurumlarımızda bir çalışma yapacağız ve ondan sonraki süreçlerde de gereken adımları atmayı planlıyoruz. Burada yaklaşık 14 tane ülkeyi inceledik. Bununla ilgili 4 tane özet bilgi aktaracağım. İncelediğimiz ülkelerin yüzde 73'ünde siber güvenlik için merkezi bir otorite var, merkezi bir kurum var ve doğrudan o ülkenin politik liderine, en üst yapısına bağlı. Dolayısıyla endekslerde evet, pek ölçü değil; ama üst sıralarda yer almalarının nedenlerinden bir tanesinin bu olduğunu düşünüyoruz. Kanada, Çin, İsrail, Birleşik Krallık, Almanya, Fransa, Hollanda, Avustralya, Güney Kore, Singapur ve Hindistan merkezi bir siber güvenlik kurumu olan ülkelerden bazıları. İncelediğimiz ülkelerin yüzde 60'ında, ilk veya ortaöğretimde siber güvenlik müfredatı var. Bu çok kritik. Onlarca bulgu var, kritik 4 tanesini buraya taşıdım. Konuşmamın az önceki bölümünde, siber güvenliği bir yaşam kültürü haline getirmemiz gerektiğinden bahsetmiştim. Bu, aslında tam olarak onu karşılıyor. Bizde, Siber Güvenlik Lisesi açıldı İstanbul'da. YÖK'le bir protokol imzaladık, siber güvenlik meslek yüksekokulları geliyor önümüzdeki seneden itibaren. Yüksek lisans ve doktora düzeyinde bazı programlar var. Ama bunlar akademik müfredatın içerisinde olan şeyler. Onun dışında, toplum genelinde de bunun bir yaşam kültürü, bir bakış açısı olması gerekiyor. İncelediğimiz ülkelerin yüzde 67'sinde siber güvenlik oluşumu var ve yüzde 53'ünde de ulusal siber kriz yönetim planları var. Türkiye'de bu plan henüz yok.

Ülkelerin siber güvenlik organizasyon yapıları dünya genelindeki eğilimlere ve teknolojik gelişmelere göre sürekli bir değişim gerektirmekte. Son yıllarda hem ölçek, hem de çeşitlilik itibarıyla artan siber saldırılar, siber tehditler, verinin kıymetlenmesi ve mahremiyeti, yüksek veri yoğunluğu, yeni nesil teknolojilerle birlikte saldırı yüzeyinin genişlemesi, kritik altyapıların hedef alınması, siber saldırıların hibrit savaşın bir unsuru olarak kullanılması, ülkeleri siber güvenlikle ilgili politika, strateji ve yönetişim yapısını bütüncül bir bakış açısıyla yeniden değerlendirmeye sevk ediyor. Bu

noktada, ülkemizde de siber güvenlik alanında odaklı hazırlanmış dağıtık yapıdaki mevzuatın yeni hükümet sisteminin yapısına uygun olarak rol ve sorumlulukları netleştiren, teknolojik gelişmelere ve yeni nesil siber tehditlere karşı ulusal mukavemeti arttırıcı bütüncül bir yaklaşımla yeniden düzenlenmesi atılacak en doğru adımlardan biri olacaktır.

Önümüzdeki süreçte ulusal siber güvenlik yönetişiminin klasik anlamdaki savunmanın yanında; yani reaksiyon vermeye dayalı, bir saldırı olmasını bekleyip, o saldırıyı tespit edip gereken adımların atılmasına dayalı bir savunma anlayışının yanında, ofansif güvenlik... Burada ofansif güvenliğin çeşitli tanımları var. Kısaca şöyle özetleyeyim: Proaktif savunma diyebiliriz veya siber etki diye tanımlayanlar da var. Dijital altyapılarımızın saldırılara karşı mukavemetini arttırabilmek için, yıkıcı etkilerden korunabilmek için, "Kapasite geliştirme, denetim ve siber suçlarla mücadele" başlıklarında, kamu, akademi, özel sektör, hatta bireyleri de kapsayacak yeni bir yapıya kavuşturulmasını elzem görüyoruz.

Bu vesileyle Çalıştayın düzenlenmesinde emeği geçenlere tekrar teşekkür ediyorum. Hepinize saygılar sunuyorum.

OTURUM BAŞKANI- Biz teşekkür ediyoruz.

Şimdi sözü Yusuf Tulgar Bey'e vereceğim. Yusuf Bey, gerçekten ülkemiz için önemli bir çalışmaya imza atan önemli bir ürünün belki kurucularından, organize edenlerden biri. Aynı zamanda güvenli bir bulut nasıl oluşturulur ve nasıl veri korunur, o anlamda ciddi bir deneyime sahip.

Buyurun Yusuf Bey.

YUSUF TULGAR (Divvy Drive A.Ş. Genel Müdürü)- Sayın Başkanım, saygıdeğer katılımcılar, hocalarım; hepinizi saygıyla selamlıyorum.

"Siber Vatan Varlıklarını Koruma ve Güncel Çözümler" konulu konferansı düzenleyen herkese teşekkürlerimi sunuyorum.

Tabii ki siber vatanı nasıl koruyacağımızı 15 dakikada anlatmak, detaylandırmak imkânsız aslında. Dolayısıyla ortalama 1 dakikada 2 slayt konuşmam gerekiyor.

Ülkemizi savunmak için alınacak tedbirler aslında çok fazla. Kategori inanılmaz geniş. Fakat ben, özellikle bir noktaya dikkat çekmek istiyorum. Hocalarımız çok değişik konularda fikirlerini ve teorilerini ortaya koydular. Burada siber saldırganların hedeflerinden bir tanesi... Bir tanesi diyorum; çünkü bazen kritik altyapıları aşağı indirmek olabiliyor, bazen veriyi değiştirmek olabiliyor, bazen veriyi çalmak olabiliyor, bazen hizmeti durdurmak

oluyor. Dolayısıyla ben bu konuşmada sizlerin verinin güvenliği konusunda dikkatinizi çekmek istiyorum.

Bu rakamları hızlıca geçiyorum, çünkü bol bol söylendi ve artık herkes biliyor Maliyetler, saldırıların hızları, Türkiye'nin durumu vesaire. Bunları geçiyorum.

Siber terörizm denilen bir kavram var artık ve maalesef siber terörizm her geçen gün siber güvenlik şirketlerinden daha hızlı büyüyor, kendilerini daha güncel tutabiliyorlar ve tabiri caizse onların güdümlü füzeleri her zaman için etkili oluyor gerçekten. Burada dikkatinizi çekmek istediğim kamu kurumları değil sadece. Siber vatan dediğimiz zaman, aslında bireysel kullanıcının elindeki telefondaki veri de kritik ve kıymetli. Yani ben bir kullanıcının telefonundaki verinin mahremiyetini sağlayamıyorsam eğer, eğer bir şekilde o telefona sızdım ve oradaki bilgiyi değiştiriyorsam, bir hastaneye sızdıysam ve hastanedeki analiz sonuçlarını değiştirebiliyorsam; Allah korusun, ileride bir doktor ameliyata girerken, belki hastanın önceki hastanın tetkiklerine güvenmekte bile problem yaşamaya başlayacak. Yani belki bir komplikasyon gelişecek ve ameliyat anında baktığı veri değişmiş olacak, bu da insanın ölmesine neden olacak. Dolayısıyla tamamen güvenlik sistemlerinin bolca yatırımlar aldığı Milli Savunma Bakanlığı, diğer bakanlıklarımız, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, böyle kritik noktaların yanında, son kullanıcı ve bu ameliyatı yapan doktorun elindeki telefonun da güvenliğinin sağlanması, verinin mahremiyetinin sağlanması çok önemli olmaya başlayacak.

Tabii, bu tür sistemlerin tamamını birden güvenlik altına almak, yüzde yüz güvenlikten bahsetmek imkânsız. Burada çok ciddi bir bilgi seviyesine ihtiyacımız var, alınması gereken önlemler var; ama en kritik konu bence sahip olduğumuz verinin merkezileştirilmesi. Yani bizler, son kullanıcılar elimizdeki parayı ya da altını korumak için evimizdeki kasada tutmuyoruz artık; çünkü hırsızlar çok gelişti. 1 milyon dolarınız varsa evde tutmazsınız, gidip bunu bankaya koyarsınız. Neden? Bankanın fiziksel koruması var, daha fazla önlem alınıyor, her geçen gün kendini iyileştiriyor ve en önemlisi, arkada devlet güvencesi var, paranıza bir şey olmaz. Fakat biz ne yapmaya çalışıyoruz? Son kullanıcılar olarak, bazen de kamunun bazı birimleri kendi verisini kendi korumaya kalkıyor. Bu çok yanlış bir yaklaşım, özellikle son kullanıcılar için. Çünkü siber terörizmin bir kuralı yok, size zarar vermek için her türlü saldırıyor, çekineceği veya geri adım atacağı bir kurgusu yok. Dolayısıyla her türlü sizin elinizdeki veriyi ele geçirmeye, onu yok etmeye, onu karıştırmaya, onu değiştirmeye çalışıyor.

O yüzden, kesinlikle şu farkındalığı oturtmakta çok büyük fayda görüyorum: Kişisel kullanıcılar kendi verilerini kendileri kontrol altında tutmaya çalışmamalı. Artık eskiden olduğu gibi PC'mizde ya da şirketimizdeki bir ofis ortamındaki bilgisayarda verileri tutamayız. Nerede tutmalıyız; bütün veri bulut (cloud) sistemlerde durmak zorunda. Yani baktığınız zaman, Google Drive, OneDrive, Microsoft, tamamının artık çok ciddi veri merkezleri var. Artık Microsoft, Windows işletim sisteminde veri yedekleyeceğiniz bir ortama izin vermeyecek, "Bu işletim sistemini kullanıyorsan, kusura bakma, az oda tutacaksın" diyecek. Şu anda bunu yapmıyor mu? Size telefon satıyor, kapasitesi dolduğu zaman diyor. Hiç çaktırmadan, yavaş yavaş bütün veriyi ... getiriyoruz. Aynı şeyi Samsung yapacak, aynı şeyi Microsoft yapacak. İşte, bizim burada çok hızlı bir şekilde bütün ülkemizdeki vatandaşlarımızın veya kamu kurumlarındaki bütün birimlerin gerçekten verilerini güvenli olarak depolayabilecekleri bir ortam sağlamamız gerekiyor. Eğer bunu sağlamakta, bunun kurallarını ortaya koymakta, bu altyapıyı oluşturmakta geri kalırsak, zaten veri yurtdışına gitmiş olacak ve bunun için de bir siber atak gerekmiyor, biz kendi elimizle götürüp bırakıyoruz. Buranın da biraz dikkatini çekmek istiyorum. Çünkü kullanıcı hayatını kolaylaştırmak istiyor, Wetransfer'le bir dosyayı transfer edebilmek istiyor, mail alıp vermek istiyor, video izlemek istiyor. Bunun için, bu altyapı milli midir, değil midir, bunu düşünmüyor; en kolay, en ucuz, en pratik olanı alıyor ve kullanıyor. Aslında ne yapıyor; aslında siber güvenlikte kocaman bir gedik açıyor. Bunun önüne geçmemiz gerekiyor. Tabii ki biz Çin değiliz, yani bütün Türkiye'yi kapatıp dışarıdan bütün komünikasyonu kesemeyiz. Öyle bir yapımız da yok, tavrımız da yok. Kamu tabii ki bu konuda çok daha bilinçli; ama bir Wetransfer'i kullanmak, bir Google Drive'ı kullanmak, bir OneDrive'ı kullanmak gerçekten çok büyük problem. İnsanlar şunu söylüyor: "Benim alışveriş yaptığım faturanın bilgisinin Amerika'da ne önemi var? Oraya koysam ne olur, koymasam ne olur?" Bunun gibi düşünen milyonlarca vatandaşımızın sliplerini değerlen-

direrek big data analizi yaparak, big data biliminden habersiz oldukları için insanlar, bizim ekonomik durumumuzu, neye eğilimli olduğumuzu, her şeyi çıkarabiliyor. Biliyorsunuz, artık 1 gigabaytlık verinin karşılığı 2.5-3 dolar, petrolden daha pahalı yani. Biz mavi vatanda petrol arıyoruz, öyle değil mi? Aslında verimize sahip çıksak ve bu veriyi işleyip katma değerli hale getirsek, petrolden çok daha değerli bir şey. Baktığımız zaman, dünyadaki bu sosyal medya sistemlerine altlık sağlayan verinin büyük bir kısmını da maalesef biz oluşturuyoruz ülke olarak, çünkü farkındalığımız yoktu bu konuda.

O yüzden, mutlaka verinin artık ülkemizde kalması gerekiyor. Ülkemizin verisi ülkemizde kalmalı. Peki, nasıl olmalı bu? Eskiden verileri biz file sistemlerde tutuyorduk, dosya sistemlerinde. Yani baktığınızda, her işletim sisteminin bir dosya sistemi var. Artık verileri dosya sistemine koyup da 3-5 dolarlık, 10 dolarlık bir antivirüs satın alarak, onun mahremiyetini sağlamasını bekleyemezsiniz. Son kullanıcıya veya KOBİ'ye indiğinizde -ki, 5 milyon KOBİ var- hangi birisi milyon dolarlık mühendislik sistemleri satın alabilir veya böyle konferanslara katılabilir? Dolayısıyla onları da bu işlerin içerisine katacak, onlardaki verinin de mahremiyetini sağlayacak yapılar kurgulamak gerekiyor.

Tabii, işletim sistemlerindeki bu verilerin mahremiyetinin sağlanmasının zorunluluğundan sonra hayatımıza veritabanı sistemleri girdi. Veritabanı sistemleri, dünyada birkaç marka var ve biliyorsunuz, biz bu trendi kaçırdık ülke olarak, yani bir işletim sistemimiz olmadı. Pardus bizim değil, bizim bir veritabanımız olmadı. Selçuk Bey'in de, Selçuk Bayraktar'ın da söylediği gibi, SİHA ve İHA'larda biz aslında çok iyi bir şey yakaladık, elektrikli araçlarda da çok iyi bir şey yakaladık, TOGG'la beraber. Neden? Biz alüminyum gövde bir motor, verimli bir motor geliştiremedik veya içerisinde insan olan bir savaş uçağını dizayn edemedik; ama tam bu teknoloji geçişinde aslında güzel bir şey yakaladık. Tam bu noktada, micro cloud servislerinin olduğu, tamamen yerli ve milli hizmetler veren bir bulut sistemi hayata geçirebiliriz. Bu, aslında teknolojinin tam bir geçiş noktası. Çünkü benim için data veya dosyanın bir anlamı yok. Her şey daha, bir IP cihazından gelen veri de bir data, benim bir kullanıcımın elindeki bir video da data, her şey data. Eğer ben bu datayı Azure'a, Amazon'a, Google Cloud'a ihtiyaç duymadan, yüzde yüz yerli ve milli, ülkemizde barındırılan, güvenliği alınan, servisleri eksiksiz olan bir yapıyla vatandaşa, kamuya veya KOBİ'ye sunmayı başarırsam ülke olarak, o zaman gerçekten ülkemiz için güzel olacak. O zaman big data analizi yapabiliriz, o zaman veriyi anlamlandırabiliriz.

Konuşmacılarımız çok haklılar, kesinlikle siber vatanı ülkenin dışında da kabul edebiliriz; ama unutmamamız gereken bir konu var. Bir saldırıda, fiziksel bir saldırıda, bir savaşa girdiğimizde çok rahatlıkla bizim ülkemizin dışındaki altyapılara erişimimizi kesebilirler. Dolayısıyla biz bütün hayatımızdaki veriyi yurtdışına koyarsak, orada güvenliğini sağlamayı başarsak dahi, kritik bir anda oraya erişimimiz kesilecek, tam ihtiyacımız olduğunda o veriyi aktif edemeyeceğiz. O yüzden siber vatanın içinde kalmak zorunda. Gerçekten çok kritik bir konu. Dikkatinizi çekmek istiyorum.

Tabii, her zaman dışarıdan gelmiyor bu saldırılar. İnsanların aklına şu geliyor: "Ben bütün ülkenin verisini tek bir noktada birleştirirsem, o zaman devlet benim her şeyimi mi görecek?" ya da "Bu kullanıcının verisini bu görebilecek mi?" gibi. Aslında bunu teknolojik olarak ispatlamak, veriye erişildiğini ya da erişilmediğini kanıtlamak çok kolay. Dolayısıyla böyle bir yaklaşımla, aslında milli bir çözümle insanların bu kaygılarını da giderip insanlarımız gerçekten yerli ve milli sistemleri kullanabilirler ya da her bakanlığa bir sistem odası kurmak yerine, belki de üniversitelerin denetlediği, Cumhurbaşkanlığının denetlediği, çok ciddi ulusal seviyede veri merkezi, yani aslında bir cloud sistemi kurup bütün Türkiye'ye hizmet verebilecek micro cloud servisleri hayata geçirilebilir ve buradaki verilerin de mahremiyeti sağlanabilir. Dediğim gibi, son kullanıcının bilgisayarında kurulu 10 dolarlık, 20 dolarlık bir antivirüsle bu güvenliği sağlayamazsınız; ama bunları da tamamen yok sayamayız. Yani veri farklı farklı noktalarda depolanırsa... Örneğin bir kamu kurumuna gidiyorum, ERT sistemleri var, ... sistemleri var, o sistem, bu sistem, 50 tane sistem var ve veri 50 yerde duruyor. Birisi 10 yıl önce kurgulanmış, birisi son teknoloji, birisi dışarıdan erişilmeye çalışılıyor vesaire. Bu kadar karışık bir yapıda tutulan verinin mahremiyetini sağlamak da çok büyük problem; çünkü saldırı her zaman dışarıdan gelmiyor, içeride de kötü niyetli insanlar olabilir. Dolayısıyla bizim teorimiz, fikrimiz, kamu kurumlarındaki veri -ki,

veri, data- merkezi bir noktada depolanmalı, merkezi bir noktada backup'a alınmalı ve merkezi bir noktada antivirüs vesaire denetimleri sağlanmalı. Yani aslında söylemeye çalıştığım şu: Divvy Drive olarak bizim geliştirmiş olduğumuz bir konsept var. Artık yeni trend, ... sistemde dosya durmamalı, veritabanına da sığmıyor artık, o zaman content management olmalı, bunu da buluta açabileceğimiz bir bulut ...olarak hayata geçirebiliriz. Verinin sınıflandırılması, merkezileştirildikten sonra bunun üzerine bir analizin yapılması da belli kurallara tâbi tutulmadı.

Kurumsal arşiv konusuna değinmek istiyorum. Aslında şöyle bir yapı var: Kamu kurumlarında, atıyorum, doküman sistemi çok kullanılan bir yapı. Bir belge oluşturuluyor ve bir yaşam döngüsünden geçiyor ve depolanıyor. O kadar fazla veri depolanıyor ki, her kurum kendi verisine sahip olmak istiyor haklı olarak. Hiçbir bürokrat kendi kurum verisini açmak istemiyor veya dışarıda depolanmasını istemiyor. Bu, aslında tekrara ve çok ciddi masraflara da neden olabilir. Yani aslında biz hepimiz bir araya gelsek, hepimiz bütün bilgi ve tecrübelerimizi ortaya koyup bu ülkede aktif çalışacak gerçek manada iki veri merkezi kurabilsek, bütün kamu da bu sistemlere micro cloud sistemleriyle hizmet alabilse, hem dışarıdan gelebilecek saldırılara karşı koymak inanılmaz kolay olacak, hem her türlü güvenlik sistemlerini bu tür yapılara entegre etmek çok kolay olacak. Çok basit bir örnek vereyim. TC kimlik numarası içeren bir verinin dışarı paylaşılmasını istemiyorsunuz; ama bu dokümanın üstünde var, dosya sisteminde var ya da personel sisteminde var. Birkaç yerde bu kuralı yazmanız gerekiyor. Bazen satın aldığımız güvenlik sistemleri kullanmış olduğunuz sisteme entegre olamıyor; yani böyle bir yeteneği yok, böyle bir yetkinliği yok. O zaman ne olmak zorunda kalıyor; ya o hizmeti vermiyorsunuz ya da göz ardı edip o hizmeti devam ettiriyorsunuz, ama bir güvenlik açığına neden oluyorsunuz. Fakat bütün veri denetlenen gerçek bir bulut (cloud) sistemde dursaydı ve kuralı tek noktadan yapıyor olsaydık, o zaman hiçbir zafiyet ortaya koymadan verinin mahremiyetini sağlamış olabilecektik.

Buyurun.

YUSUF TULGAR- Donanımın üstüne zaten yaklaşık 10 yıldır, yaklaşık 45 ayrı noktaya çözüm üreten micro cloud servisler geliştiriyoruz. Şu anda yaklaşık 15 bakanlık, Savunma Bakanlığımız, BTK, İş Bankası, Vakıfbank, 3 operatör, bu sistemimizi geliştirdik. Tamamen yerli ve milli. Başkanımızın da söylediği gibi, her şeyi kapatıp, fişleri çekip siber güvenlikten bahsedemeyiz. Artık mobilite var hayatımızda, giyilebilir teknolojiler var. Dolayısıyla veriye her yerden 7/24 aktif etmek zorundayız. Bu veriyi access etmek için

de bir yol açmanız gerekiyor, bir kanal açmanız gerekiyor. Mesela Merkez Bankasındaki yapımız tamamen kapalı bir network'ta çalışırken, dışarıdan da access edilen yapılar var. Bu tür sistemlerde biz file sistemlere güvenemeyiz, bir veritabanına güvenemeyiz, satın aldığımız antivirüse güvenemeyiz. Biz Divvy Drive olarak yüzde yüz yerli ve milli, veriyi ... tutan ve dünyadaki bütün işletim sistemleri üzerine entegre çalışabilen bir mekanizma geliştirdik. Yatayda ve dikeyde büyüyebilen ve şu ana kadar yaklaşık 780 katrilyon dosyayı yönetiyoruz. Buradan şunu söylemek istiyorum: Biz Türkiye Cumhuriyeti verilerini yönetebilecek güçteyiz, bu teknik tecrübeye ve altyapıya sahibiz artık. Buradaki birçok arkadaşımız Divvy Drive kullanıyor zaten. Zaten bütün bakanlıklar neredeyse Divvy Drive kullanıyor. Dolayısıyla bizim ülkemizdeki verinin ülkemizde kalması için, işletim sisteminden bağımsız, datanın tipinden ve boyutundan bağımsız bir hizmet vermek için, biz şirket olarak, Divvy Drive A.Ş. olarak böyle bir şeye hazırız.

Veri güvenliği ve mahremiyetiyle ilgili, eğer ki herkesin bildiği bir sistemde veriyi yönetirseniz hack'lenmeniz daha kolay olur. Biz, klasik bir file sistemde verinin nasıl yönetildiği kurgusuyla yönetmiyoruz ya da bir ... tutmuyoruz; tamamen bize özgü yerli ve milli bir algoritmayla datayı kriptolu bir şekilde yönetiyoruz. Yani çok kabaca, "Dünyanın hiçbir ülkesi bize ulaşamaz" dediğimizde herkes şunu söylüyor: "Sen kimsin, siz kimsiniz?" "Siz kimsiniz?"dediler bize. Çok basit bir teknik açıklaması var. Biz veriyi, yani dosyayı data olarak ... parçalayıp kriptolu olarak tutuyoruz. Yani içeri girecek olan bir arkadaş, elinde silah var; Allah korusun, bizi tarayacak; biz, onu atomik parçalarına bölüyoruz, elindeki silah dâhil olmak üzere ve her bir parçasını ... kriptolayıp arka tarafta base blockchain mantığında yedekli aktif yönetiyoruz. Buraya kadar problem yok, herkes parçalara bölebilir insanları; fakat geri çıkarken, ölmeden, bunu tekrar hücrelerine kadar birleşip bir hücresi de eksik olmadan geri gönderebiliyoruz. O yüzden aslında bu yüksek güvenlikten bahsediyoruz. Ayrıca da dünyadaki bütün antivirüs sistemleri, her türlü tarama ve virüs sistemleriyle de entegre çalışabiliyoruz. Dünyada olmayan bir özelliğini söyleyeyim. Örneğin Divvy Drive'ın arkasında 10 tane antivirüsü entegre edersiniz. Bir dosya attığınızda, 10 antivirüs ayrı ayrı sistemden geçirir ve stabilize edilmiştir artık o. Dünyada en azından yetkinliği ispatlanmış, bilinen antivirüs sistemlerinin tamamını analiz etmiş, "Bulguya rastlandı" veya "Rastlanmadı" raporunu verebilir size. Ama son kullanıcı buna antivirüs satın almaz. Parası olmadığı için değil, çünkü aynı makinede aynı anda çalışmaz.

Dolayısıyla yakın gelecekte zaten kişisel bilgisayarlarınızda bir disk alanı olmayacağı için, sıkıştığımız anda bizi cloud'a yönlendirecekleri için, biz

bugünden eğer bu cloud sistemlerini kurmazsak, verimizi zaten kendi elimizle götürüp teslim ediyor olacağız; yani bir siber saldırıya gerek kalmadan, bu işi maalesef kendimiz yapmış olacağız.

8,5 milyon satır kod geliştirdik bu iş için. Yaklaşık 45 tane ayrı modül var. Wetransfer'den Drive'a kadar ya da bir arşive kadar ya da bir mail ekinin yönetimine kadar ya da Google'daki bir formdan Word, Excel ya da PowerPoint açmaya kadar o kadar fazla servisimiz var ki, "Sörf yapayım, ofis belgeleriyle ilgileneyim, yazılarımı yazayım" gibi son kullanıcının bütün ihtiyaçlarını gören ürünleri yükleyip yerli ve milli geliştiriyoruz. Açık kaynağa karşı değiliz, ama açık kaynak kullanmıyoruz. Neden kullanmıyoruz? Ben kendim yıllardır kod yazıyorum, 15 sene HAVELSAN'da çalıştım, 10 yıldır da bu sistemin geliştirme aşamasında çalışıyorum. Başkasının yazmış olduğu milyonlarca koda yüzde 100 hâkim olmak gerçekten imkânsız. O yüzden biz her şeyi sıfırdan yazdık. Büyük bir ekip tarafından bu 8.5 milyon satır geliştirildi ve geliştirilmeye de devam ediyor.

Özetle biz, yerli ve milli cloud sistemlerini kurmak zorundayız. Verinin mahremiyetini sağlamak için backup discord yapıyoruz ya, veri o kadar büyüdü ki, artık böyle bir teknoloji yok. Verinin backup'ını alamıyorsunuz artık; alsanız da, verinin başına bir iş geldiğinde discord edemeyeceksiniz. O yüzden ne olmalı; verinin birden fazla nokta yedeğinin sağlanması gerek. Yeni teknolojik altyapılarla bunları geliştiriyoruz. Tabii, bunlarla ilgili sorular için her zaman bizimle iletişime geçebileceksiniz.

Referanslardan bazıları. Yani biz bu noktaya gelmek için gerçekten inanılmaz bir efor sarf ettik. Çünkü bunların her biri gerçekten çok kritik müşteriler. Örneğin Vodafone bir İngiliz markası aslında. Bütün verisinin güvenliğini sağlıyoruz. Sayıştay, Kültür Bakanlığı ve bizim için çok kritik Bilgi Teknolojileri ve İletişim Başkanlığı olmak üzere... Neden? Çünkü 4.5 ay boyunca BTK bizim ürünümüzü aldı, sızma testlerinden, performans testlerinden geçirdi. Ömer Başkanımız sağ olsun. İnanılmaz bir efor sarf ederek, "Bu insanlar doğru mu söylüyor, ne kadar yetkinler, gerçekten böyle bir durum var mı?" diye bizi denetledi ve bize resmi bir denetim rapor belgesi sundu BTK.

Hepinize saygılar sunuyorum. Teşekkür ediyorum.

OTURUM BAŞKANI- Teşekkür ediyoruz.

Emniyet Genel Müdürlüğü Terörle Mücadele Dairesi Başkanlığından değerli konuşmacımız Hüseyin Akarslan Bey'i davet ediyoruz. Buyurun.

HÜSEYİN AKARSLAN (EGM Terörle Mücadele Daire Başkanlığı)- Sayın Başkanım, sayın hocalarım, değerli katılımcılar; hepiniz hoş geldiniz.

4. Sınıf Emniyet Müdürü Hüseyin Akarslan. Terörle Mücadele Daire Başkanlığında görev yapıyorum. Bugün size siber terörizm ve açık kaynak istihbarından bahsedeceğim biraz. Açık kaynak istihbaratı nedir, neden önemlidir, nasıl kullanılır; güvenlik bürokrasisi dışında, özel sektörde kullanılmalı mıdır ve tehditler, teknikler, trendler nelerdir, bunlardan bahsetmeye çalışacağım.

Öncelikle kavramlardan biraz bahsetmek istiyorum. Organize suç ve terörizm en çok birbirine karıştırılan kavramlardan. O yüzden, organize suçtan biraz bahsetmek istiyorum. Organize suç, birçok ülkede örgütlü suçları ifade eden suç; yani tek başına insanın işleyemediği, belli bir grup halinde işlemesi gerektiği ve temel amaçları genelde maddi çıkar olan, hiyerarşik bir yapısı olan, literatüre göre en az 3 kişinin olması gereken gruplardan bahsediyoruz. Terörizm ise, cebir ve şiddet kullanarak, baskı, korkutma, yıldırma, sindirme veya tehdit gibi yöntemleri kullanarak bir devletin siyasi yapılanmasına yönelik suçlar olarak tanımlıyoruz. Arasında benzerlik olmakla birlikte, ciddi farklılıklar da var. Bir kere, terör suçlarında amaç ideolojik, organize suçlarda ise finansal. Terör suçlarında genelde siyasi bir örgütlenme, yapılanma varken; organize suç örgütlerinde daha adi bir yapılanma var, daha basit düşünebilirsiniz. Birinde hedef doğrudan rejim ve devlet iken, diğerinde hedef güç ve itibar ve en sonunda maddi çıkar elde etmek. Organize suç örgütlerinin ve terör örgütlerinin ortak paydaları, tehdit, şiddet, silah, uyuşturucu ve kaçakçılık gibi fenomenlerdir.

Siber terörizm dediğimiz şeyi ise, az önce bahsettiğimiz terörizm kavramını, yani devletin idari yapılanmasını, anayasal düzenini hedef alan suçun aslında siber alanda işlenmesi veya bu suçun işlenmesi için siber alanın bir araç olarak kullanılması olarak çok basit bir şekilde tanımlayabiliriz. Yani günün sonunda, yapılan iş siber alanda olsa da amaç, gerçek hayattaki siyasi yapılanmayı, bir devletin yönetimini etkileyecek, bunu yıkacak, bunu

farklı bir şekle evirecek eylemlerdir aslında.

Bunun dışında, bir de terörizmin finansmanı kavramı var; burada özellikle değinmek istiyorum. Bu da yine önemli bir kavram. Yurtdışında, ülkemizde ve birçok ülkede de ayrı bir kanunla ayrı bir suç olarak tanımlanmış bir şeydir terörün finansmanı; çünkü terörizmin gerçekleşmesi için aslında en önemli şeydir. Bir terör eyleminin veya en basit terör örgütünün yapılanması için ilk ihtiyaç duyacağı şey bir fondur, yani maddi destek. O yüzden, ülkemizde de bu terörizmin finansmanı, terör örgütlerine para sağlamak, eylemlerini desteklemek maddi olarak tamamen ayrı bir suç olarak tanımlanmıştır ve cezası normal terör örgütü üyeliğinden veya sempatizanlığından çok daha fazladır.

Peki, açık kaynak istihbaratı nedir? Açık kaynak istihbaratından önce, istihbaratın ne olduğunu düşünürsek, TDK'da, yeni öğrenilen bilgiler, haberler, duyumlar şeklinde tanımlanırken; Güvenlik Terimleri Sözlüğünde, kullanıcıların talep ve ihtiyaçlarına yönelik olarak değişik kaynaklardan bilgilerin toplanması ve bu bilgilerin bir dizi işlemden geçirilerek yorumlanması sonucu elde edilen nihai ürün; kısaca, üretilmiş, genellikle gizli ve daha çok eyleme/aksiyona yönelik zamanlı bilgidir. Bunda dikkat edilmesi gereken birkaç tane husus var. Bir, anlamlı bilginin dışında, istihbarat dediğimiz şey, anlamsız bilgiden, anlamsız veriden belirli işlemler işleme sonucu üretilmiş ve belli bir zamanda belli bir geçerliliği olan anlamlı bir bilgi olarak düşünülebilir.

Bizim bilgi değer zinciri dediğimiz şey, ham veriden karar alma süreçlerine kadar bilginin istihbarata dönüştürülmesi ve sonrasında kurumların, şirketlerin ya da organizasyonların karar verme süreçlerinde bu bilgiyi kullanmasıdır. Aslında bir dizi işlemden geçiyor yani. İstihbarat dediğimiz şey hiçbir zaman hazır bir şekilde alınıp kullanılan bir şey değildir veya birisine göre anlamlı bilgi olan bir şey birisine göre veya bir kuruma göre istihbarat olabilir ya da olmayabilir.

Yine şunu ifade etmek lazım: İstihbarat, normal anlamlı bir bilgi veya işlenmiş veri dışında, belli bir sorunun cevabını verir aslında. Yani bir kurum için ya da bir organizasyon için eğer çözülmesi gereken bir sorun varsa ya da merak ettiğiniz bir şey varsa, bunun cevabını veriyorsa ve bu cevap sizin organizasyon yapınızda veya organizasyonel karar alma süreçlerinizde sizin işinize yarıyorsa, o zaman istihbarattır diyebiliriz. Tabii, istihbaratı aldıktan sonra da karar alma süreçlerinde kullanmanız, bir eyleme geçmeniz ve bundan kurumsal bir değer üretmeniz gerekir. Açık kaynak istihbaratı bugün her ne kadar modern öncesi istihbaratta da varmış gibi kabul edilse

de, aslında modern istihbaratın ortaya çıkarttığı bir şey. Çünkü modern öncesi istihbaratla, yani bundan 100 yıl öncenin istihbarat yapısıyla son 100 yıldaki istihbarat tamamen değişmiş durumda, özellikle kurumsal yapılanma olarak. Bundan 100 yıl öncesine gittiğinizde, aslında ciddi istihbarat kurumları görmüyorsunuz. İstihbarat çok daha küçük, mikro ölçekte, ajanlar üzerinden, kralların ya da padişahların birkaç kişi üzerinden ürettiği bir süreçken, son yüzyılda özellikle kurumsal yapılanmaya dönüşmüştür. Açık kaynak istihbaratının tarihi herhalde son 50 yıla dayanır. İlk adımları yine İngilizler tarafından atılmıştır. 1940'ta uygulandığından itibaren özellikle BBC tarafından... BBC'yi biz normalde nasıl biliyoruz; İngiltere'nin bir kanalı ve yayın organı diye düşünüyoruz. Ama tam tersine, İkinci Dünya Savaşı'ndan itibaren tam bir istihbarat ajansıdır BBC. 2016 yılındaydı galiba, adını değiştirerek farklı bir yapılanmaya geçti. Bugünkü bildiğimiz açık kaynak istihbaratı, verilerin takibi gibi işler İngilizler tarafından başlatılmıştır.

Açık kaynak istihbaratı dediğimiz şey aslında kamunun erişimine açık her türlü basılı ve elektronik ortamdaki bilgilerden elde edilen istihbarat şeklinde tanımlanmaktadır. Bu erişim tamamen herkese açık olduğu gibi, gri literatür dediğimiz bir ... diye tanımlayabiliriz. Bu da şudur: Kolaylıkla erişemeyeceğimiz, ancak bir-iki metotla erişebileceğimiz, belli bir kişiye açılmış alan olsa da, girebileceğimiz alanı ifade eder.

Açık kaynak istihbaratıyla ilgili yine birkaç tane terim var; bunlardan birisi açık kaynak verisi. Açık kaynaktan elde edilen ham veriyi ifade eder. Açık kaynak bilgi, açık kaynaktan elde edilen anlamlandırılmış veridir. Açık kaynak istihbarat ise açık kaynaktan elde edilen doğrudan istihbari değeri olan kıymetli bilgiyi ifade eder. Doğrulanmış açık kaynak istihbaratı ise, açık kaynaklardan elde ettiğimiz istihbaratla gizli istihbaratımızı birbiriyle çakıştırarak doğruladığımız, artık tamamen yüzde yüz doğrulanmış ve karar alma süreçlerinde kullanabileceğimiz istihbarattır aslında. Açık kaynak istihbaratın bugünkü anlamına baktığımızda, tamamen siber alanı ifade ediyor. Çünkü bugünkü veri miktarına baktığımızda, verinin artık çok büyük bir kısmı dijitalde olduğu için, açık kaynak istihbaratı deyince, tamamen dijital dünyayı, siber alanı anlıyoruz. Bugün artık bir gazete veya basılı yayın açık kaynak istihbaratının pek de süjesi değil. İstihbarat toplama türü olarak sinyal istihbaratın altına giriyor ve kaynak olarak da açık kaynak diye ifade ediliyor.

Tabii, açık kaynak istihbarat döngüsünden bahsetmeden önce, açık kaynak istihbaratıyla ilgili birkaç eski komutan ve yöneticinin sözünden bahsetmek istiyorum. Bizim MİT Müsteşarımız Hakan Fidan'ın da yüksek lisans

tezi var, şu anda internette yer alıyor, okuyabilirsiniz. Kendisi de bizzat şöyle der: "Hiçbir analist, elindeki gizli bilgilerle tam bir istihbarat analizi yapamaz, açık kaynaklarla doğruluğuna bakmalı ve iki bilgiyi birleştirerek yorum yapmalıdır." Yine 60lı yaşlarda bir generalin bir sözü var. O da şöyle der: "Aslında istihbaratın büyük bir kısmı açık kaynaklardadır, çok küçük bir kısmı, yani yüzde 10'u kadarı gizli bilgilerdir; ancak, bu daha magazinsel ve popüler olduğu için. Ancak, asıl veri açık kaynaklardadır ve bu nedenle de asıl istihbarat kahramanı Sherlock Holmes'tur, James Bond değil" der. Çünkü biliyorsunuz, James Bond, onun için hazırlanmış hazır aletleri kullanır ve tık tık tek bir şeylere basar, şeyi çözer. Ama Sherlock Holmes öyle değil, yaşadığı bir sürü olayları analiz ederek bir sonuca varır.

Yine eski bir Amerikan Özel Kuvvetler Komutanının bir sözü var. Yine o da 60-70'li yaşlarında bir general, normalde sahada çalışmış ve şöyle bir söz söyler: "Biz artık sosyal medyayı, bu mecrayı tamamen yeni muharebe alanı olarak tanımlamak zorundayız." Şöyle düşünebilirsiniz: "65 yaşındaki bir general, Özel Kuvvetlerde çalışmış, sahada çalışmış, sosyal medyayla ne işi olabilir" diye düşünebilirsiniz; ama böyle önemli sözleri var.

Açık kaynak istihbaratı döngüsü dediğimiz olay, devam eden 6 basamaktan ve sonrasındaki döngüden oluşmakta. Hızlıca bunlardan bahsetmek istiyorum. Birinci aşama planlama aşaması; yani siz istihbarat toplayacaksanız neyi toplayacaksın, neye ihtiyacınız var, onun tartışıldığı aşamadır. İkinci aşama bilgi toplama; bu hedeflediğiniz alana göre bilgi toplamaya başlarsınız. Üçüncü aşama topladığınız bilginin işlenmesidir. Dördüncü aşama, topladığınız bilginin analiz edilmesidir. Beşinci aşamada artık burada bir ürün ortaya çıkar; yani bir rapor, bir görsel ya da resmi belge şeklinde dönüştürülür. Altıncı aşamada da artık bu istihbarat sürecini başlatan kişilere ya da makama verilmesi ve sonrasında diğer ilgili birimlere dağıtılmasıdır.

Açık kaynak istihbarat süreci takip edilirken üç yöntem uygulanır. Birincisi, tamamen pasif bilgi toplama. Bu pasif bilgi toplama, kaynakla hedef arasında herhangi bir doğrulama gerektirmez ve açık kaynak istihbarat toplama teknikleri içinde en güvenilir olarak kabul edilir. Bunu şöyle düşünebilirsiniz: İnternetten bir haber gazetesi okuyorsunuz, bunu okurken bir doğrulama gerektirmez; kendi kimliğimizi proxy'inizi falan gizleyerek de o habere erişebilirsiniz. İkincisi, yarı pasif bilgi toplama. Burada, hedefle kaynak arasında tam bir doğrulama olmasa da, kaynak hedeften verilecek bazı doğrulamaları ister. Yine bazı web sitelerine girerken ... falan gibi bazı şeyleri ister. Bu da yarı pasif bilgi toplamadır. Burada da tam bir güvenlik

olmasa da, kısmen karşı tarafa karşı kendinizi gizleme şansınız var. Aktif bilgi toplama yönteminde ise, evet, kaynak açıktır; ancak, o açık kaynaktaki hedef sizin tamamen kendinizi doğrulamanızı ister. Burada ne yazık ki kendi bilgilerimizi gizlememiz çok kolay olmaz. Nedir mesela; kendi TC kimlik numarasını girdiğini bir portalı düşünün. Artık orada kendi kimliğinizi doğrulamanız lazım. Evet, yine açık bir kaynaktır, herkes oraya erişebilir; ancak, kimin girdiği, kimin baktığı kontrol edilebilir ve manipüle edebilir bir durumdur.

OSINT araç ve teknikleri. Birincisi, hazır uygulamalar. İnternette çok fazla hazır uygulama var, bunları edinebilirsiniz. İkincisi, ücretli ve ücretsiz paket programlar. Üçüncüsü, eğer bir yazılım geliştirme yeteneğiniz varsa sıfırdan bir yazılım geliştirebilirsiniz. Dördüncüsü, doğrudan ücretli servisler alınabilir. İşte, ne bileyim, Ajans Pres gibi ya da medya takip servisleri var, onlardan alabiliyorsun. Ama tabii, dört farklı araç ve servisi kullanıyorsanız, bunu doğru bir şekilde entegre etmeniz gerekiyor.

En çok kullanılan OSINT tekniklerinden biri halen metin madenciliği. Çünkü internet ortamında veya siber alandaki en ciddi veri halen metin ve bu metni analiz ederek, veri madenciliği gibi metin madenciliği yöntemini kullanarak istihbarat toplama şansınız var.

En çok kullanılan tekniklerden birisi de sosyal ağ analizi. Normal sosyal yaşamda nasıl insanlar arasında bir sosyal diyagram varsa, aynı şekilde, sizin siber alandaki hareketleriniz, davranışlarınız da sizin o sosyal bağlantınızı, çizginizi veya ilişkilerinizi oraya koymaktadır. Yine en çok kullanılan araçlardan birisi.

Üçüncüsü mekânsal analiz. Bugün artık internette, siber alanda en çok paylaştığımız verilerden birisi maalesef coğrafi bilgiler. Fotoğraf çekerken, internette bir twit atarken birçok kullanıcı yine coğrafi bilgisini paylaşıyor. Normalde sizi yabancı birisi sorsa, "Şu an neredesin?" diye telefonunuzu arasa, hayatta söylemezsiniz. Bu çok gizli bir bilgiyken, aslında son kullanıcı bu bilgiyi maalesef isteyerek paylaşıyor. Mesela şu slaytta üsttekine bakarsanız, DEAŞ'lı bir terörist, çatışma bölgesinde, twit atarken telefondaki konum paylaşma özelliğini açık unutuyor. Norveç'ten kalkmış, Kuzey Irak'a, Suriye'ye, çatışma bölgelerine gitmiş birisi. Ancak, attığı twitlerden yeri tespit edilip yakalandı.

Alttaki örneğe bakarsanız, orada da aslında bir video görüntüsü var. Biliyorsunuz, DEAŞ'lı teröristler çok fazla video yayınlarlar YouTube'ta. Burada, videonun arkasında görünen binalardan, binaların gölgelerinden, Go-

ogle Maps'teki görüntüler eşleştirilerek, tam olarak videoyu nerede çektiği rahatlıkla tespit edilebiliyor. İnterneti iyi araştırırsanız görürsünüz, gündüz çekilen fotoğraflarda güneş ve gölge boyları çok önemli ve açık kaynak istihbaratında kullanılan yöntemlerden birisi. Bununla ilgili web siteleri de var. Bir cisim var, cismin gölgesi ne kadar, onu tarih ve saatiyle fotoğrafı biliyorsanız, o portallara bu bilgiyi girdiğiniz zaman size fotoğrafın nerede çekildiğini şak diye söyleyebiliyor.

Güncel trendler ve tehditleri konuşalım şimdi de.

Şu an dünya nüfusu 7.9 milyar. Bunun 5.4 milyarı şu anda internet kullanıyor. Yani artık dünya nüfusunun yüzde 69'u internete erişebiliyor ve kullanabiliyor. Son kullanıcı bu manada artık inanılmaz bir veri üreticisi haline geldi. Son 10 yıldaki paradigma değişimi tamamen bu yüzden. İnternetin ilk yaygınlaştığı yılları düşünürsek, veriyi üreten daha çok kurumlar ve şirketlerken, akademik birimlerken, bugün artık internet ortamında verilerin ciddi bir kısmını son kullanıcı üretiyor. Bu, açık kaynak istihbaratı açısından, verinin çok ciddi büyümesi nedeniyle ciddi bir sıkıntı olarak görülebilir.

Diğer bir problem siber alan. İnternet ilk çıktığında yüzeysel bir internet varken, bugün artık üç ayrı katmana ayrılmış durumda. Birincisi, yüzeysel alan. İkincisi, derin web dediğimiz alan. Bu alan aslında verinin çok ciddi bir kısmını tutuyor ve kolayca erişemeyeceğiniz bir alan. En altta da tamamen farklı protokolleri ve yöntemleri kullanarak erişebileceğiniz, karanlık web dediğimiz dark web var. Yani eskiye nazaran artık üç farklı katman var. Eğer açık kaynak istihbarat sistemini yürütecekseniz veya açık kaynak bilgisine ihtiyacınız varsa, bu üç katmanı da dikkate almanız gerekiyor. Sadece yüzeysel yapıyla yetinemezsiniz. Sosyal medya dediğimiz şey en üstteki yüzeysel yapı aslında. Evet, verinin ciddi bir kısmı olduğunu düşünüyoruz, ama diğer katmanlarda da çok ciddi bir veri havuzu var.

Büyük veri yaklaşımı artık açık kaynak istihbaratında zorunlu hale gelmiş gibi bir durum var. Çünkü açık kaynaklardan elde edeceğiniz verileri artık

klasik yöntemlerle toplamanız, analiz etmeniz çok mümkün değil.

İkincisi, yapay zekâ. Bırakın topladığınız verinin analiz edilmesini, hangi veriyi nasıl toplayacağınızı, neye öncelik vereceğinizi bile artık yapay zekâ algoritmalarını kullanarak belirlemek zorundasınız. Diğer türlü bu kadar verinin klasik metodolojiyle analiz edilmesi mümkün değil. Tabii, internet teknolojisindeki değişimle açık kaynak istihbaratın metodolojisi de tamamen değişmiş ve yenilenmiş durumda.

Şu anda biz üçüncü nesil açık kaynak istihbaratından bahsediyoruz. Yani makine öğrenmesine, yapay zekâya dayalı, manuel yöntemle veya insani usulle kesinlikle analiz edemeyeceğimiz, çözemeyeceğimiz bir noktaya vardık. OSINT'te ise artık semantik web denilen, Blokzincir teknolojisi ile sanal gerçekliğin giderek arttığı, farklı bir yapılanmaya geçtik. Metaverse çok popüler durumda. Önümüzdeki belki 5-10 yıl sonra artık bu sanal gerçeklik dünyası içinde OSINT yapmak, burada istihbarat toplamak sıradan bir durum haline gelecek.

Trendler dedik. Açık kaynaklarda çok ciddi bir veri var, sizin de bu verilerden bir şeyler yapmanız lazım, kurumsal ihtiyaçlarınız var. Ama nereye nasıl bakacaksınız? Bugün aslında en büyük problem bu. Evet, veriye erişiminiz var, ama hangi veriyi ne yapacaksınız, bunu kurum olarak bilmeniz gerekiyor. Özellikle siber terörizm ve diğer bilişim suçlarını düşündüğümüzde, bununla ilgili trendleri devamlı takip etmek gerekiyor. Örneğin Birleşmiş Milletler bununla ilgili bir rapor yayınladı. Bizim radikalleşme dediğimiz veya aşırıcılık dediğimiz; teröristin normal bir insanken bir anda belli bir radikal çizgiye kayması, sempatizan olması, daha sonrasında da örgüt üyesi olması dediğimiz bu süreçte, mesela oyun konsollarının ve oyun platformlarındaki sohbet (chat) odalarının bunu çok etkilediğiyle ilgili bir rapor yayınladı Birleşmiş Milletler. Eğer böyle bir raporu görürseniz, nereye odaklanmanız gerektiğini de bilirsiniz. Bugün siz teröristleri takip edecekseniz, bu oyun platformlarına girip bir hesap açmanız lazım, bu oyunları belki oynamanız lazım, belki bu oyunlardaki insanlarla konuşmanız lazım, oradaki verileri kendinize çekmeniz lazım gibi.

Yine benzer şekilde Europol'ün her yıl yayınladığı bir terörizm trend raporu var. Burada da yine terörizmin finansmanında kullanılan dijital varlıklar veya siber terörizmdeki güncel trendlerle ilgili detaylı bilgiler paylaşılıyor, bunlara da düzenli olarak bakmak gerekiyor.

Üçüncüsü, yine Europol'ün yayınladığı bir İnternet Organize Suç Tehdit Değerlendirmesi raporu var, bu raporda da yine siber suçların nasıl değiş-

tiği, yaşadığımız dönemde neler yaşanmış, önümüzdeki dönemde neler yaşanabilir gibi beklentiler yer alıyor, bu raporu da düzenli olarak takip etmek faydalı olabilir.

Sunumum bu kadar. Dinlediğiniz için teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Çok teşekkür ediyoruz. Son konuşmacımız, Mahmut Esat Yıldırım, USOM İleri Güvenlik Operasyon Koordinatörü. Buyurun.

MAHMUT ESAT YILDIRIM (USOM İleri Güvenlik Operasyon Koordinatörü)- Öncelikle hoş geldiniz. Bize bu konuşma fırsatını veren herkese teşekkür ederim.

İsmim Mahmut Esat Yıldırım, USOM, Ulusal Siber Olayları Önleme Merkezinde ileri siber güvenlik operasyonları koordinatörü olarak görev yapıyorum. Yaklaşık 7 senedir orada çalışıyorum.

Az önceki sunumlarla da çakışan, benzer içerikte bir sunum benimki de, benzer şeylerden ben de bahsetmiş olacağım.

Bildiğiniz gibi, 2012'de Bakanlar Kurulu kararıyla ulusal siber güvenlik çalışmalarının yürütülmesi, yönetilmesi, koordinasyonu konusu ele alındı. Sonrasında, 2012'de Siber Güvenlik Kurulu ve ilerleyen yıllarda da siber güvenlik stratejisi eylem planları yayınlanmaya başlandı. Bu stratejilerden ilkinde de 2013 tarihinde USOM kâğıt üzerinde kurulmuş oldu aslında. Neden kâğıt üzerinde diyorum? O zamanki yetkinliği ve görev, faaliyet, sorumlulukları günümüzdekiyle çok farklıydı, sadece isim olarak Türkiye'de olması gerektiğine karar verilmişti. Sonrasında, 2016'da yeni gelen kanunla, 5809 sayılı Elektronik Haberleşme Kanunuyla USOM'a belli başlı görev, yetki ve sorumluluklar verildi. İlkin, caydırıcılığı sağlamak için her türlü tedbiri alır ve aldırır şeklinde bir sorumluluk verildi. Sonrasında, "Kurum, görevi kapsamında ilgili yerlerden bilgi, belge, veri ve kayıtları alabilir ve değerlendirmesini yapabilir" şeklinde bir yetki verildi. Bu bizim olay müdahale faaliyetleri yapmamıza ve orada adli bilişim çalışmaları gerçekleştirmemize olanak sağladı. Ve son olarak da "Para cezası uygulayabilir" şeklinde bir yetki verildi.

USOM'un genel olarak yapısından bahsetmek gerekirse, şu şekilde bir yapıdan bahsedebiliriz. Bir ülkede CERT kurdunuz. CERT dediğimiz, computer emergency response team. Bütün ülkenin kapsamı aslında bizim sorumluluğumuzda oluyor. Yani bütün ülkenin IP adlarından, domain'lerinden tutun da, vatandaşların, şirketlerin falan siber saldırılardan korunması yönünde biz sahada ön planda oluyoruz CERT olarak. Bunun için de aslında

bizim birçok farklı kaynaktan, birçok farklı noktadan veri/istihbarat toplamamız gerekiyor. Ki anlık olarak ülkemizde neler oluyor, yurtdışında neler oluyor, onları görebilelim.

Burada, kısaca bahsetmek gerekirse, bizim ihbar olarak adlandırdığımız bir sürecimiz var. Dışarıdan bize gelen tüm bilgileri biz ihbar olarak kabul ediyoruz. Bu şu şekilde oluyor: Vatandaşlar olsun, diğer ülkelerin CERT'leri olsun veya diğer kamu kurumlarında yer alan siber olaylara müdahale ekipleri olsun, bize sürekli bilgi akışı sağlıyorlar. Şu anda siz bile telefonunuza gelen bir dolandırıcılık SMS'ini gördüğünüz zaman, hemen bizim ihbar hattımıza mail'le ya da telefonla ulaştırabiliyorsunuz. Buradan gelen verileri biz ortak merkezimizde topluyoruz. Tabii, kendi geliştirdiğimiz, birazdan bahsedeceğim projelerimiz var, bu projelerden de çok farklı istihbaratlar, veriler topluyoruz. Ayrıca bizim bağlı bulunduğumuz bazı uluslararası işbirliği organizasyonları mevcut. Bunların başlıcaları; FIRST, Türk Devletleri Teşkilatı, NATO gibi birçok farklı organizasyondan siber istihbarat, siber güvenlik tehdit istihbaratı anlamında bilgiler akıyor. Onun yanı sıra diğer CERT'ler, yani diğer ülkelerin USOM'larından bize gelen çeşitli bilgiler-belgeler oluyor. Onun yanı sıra, belki duymuşsunuzdur, çeşitli yarışmalar, tatbikatlar düzenliyoruz, oralardan çok farklı kaynaklar ediniyoruz. Bu şekilde USOM'un genel veri akış şeması var.

Peki, bu toplanan verilerle ne yapıyoruz? Önceki sunumlarda da bahsedildi, big data olarak adlandırabileceğimiz bir veri mevcut burada. Bunları birçok farklı ekibe bölmek durumunda kalıyoruz.

Ben size biraz da operasyonel faaliyetlerimizden bahsetmek istiyorum. Önce USOM'un organizasyon şemasını bir anlatayım, sonrasında bu operasyonu biz nasıl ilerletiyoruz, onu anlatmak istiyorum.

İhbar ekibimiz gelen bütün verileri analiz ediyor. Daha sonrasında, bu gelen istihbarat, bu gelen bilgi neyle ilgili, neyle alakalıysa, onunla ilgili ekibe bunu gönderiyoruz.

Zafiyet tarama ekibimiz var. Bu zafiyet tarama ekibimiz şunu yapıyor: Sabah Oğuz Başkanımız da sunumunda bahsetti, Kasırga diye tanımladığımız, kendi geliştirdiğimiz bir projemiz var, bir yazılımımız. Dağıtık bir ... çalışan ve tamamını bizim kendi fonladığımız bir sistem olduğunu düşünün, Türkiye'deki 17 milyon IP adresini sürekli olarak, günde birkaç sefer açık portlarla tarıyoruz ve bu portlardan elde ettiğimiz verileri bir veri ambarına aktarıyoruz ve bunun üzerinde de zafiyet taramaları gerçekleştiriyoruz. Örneğin şunu yapabiliyoruz günümüzde: Dün bir zaaf çıktı, bütün dünyayı kasıp kavuruyor; hemen, 1 saat içerisinde, Türkiye'de bu zafiyet hangi kurumların hangi IP adreslerinde var, onları tespit edip, yine ihbar ekibimiz aracılığıyla resmi yazıyla bunu gönderebiliyoruz. Bu anlamda, ülkenin varlık yönetimini ve siber zafiyet/saldırı yüzeyini güzel bir şekilde çıkartabiliyoruz.

Sızma testi ekibimiz var. Bunlar da çeşitli kurum ve kuruluşlara düzenli olarak sızma testi icra ediyorlar.

Zararlı yazılım ekibimiz var. Bildiğiniz gibi, ülkemiz de birçok ülke gibi sürekli olarak siber saldırıya maruz kalıyor. Ancak, bizim genel olarak farklılığımız, asıl öncelik verdiğimiz saldırılar, APT dediğimiz, daha çok devlet destekli saldırılar oluyor. Bunların da kullandıkları, siber silah olarak niteleyebileceğimiz çeşitli zararlı yazılımlar bulunuyor. Bu ekibimiz bunları inceliyor, gerekli indikatörleri çıkartıyor ve sonrasında tüm diğer kurumlarla bu bilgileri paylaşarak, bu indikatörler hangi kurumlarda varsa onları tespit etme noktasında çalışıyorlar.

SALONDAN- Sadece kamu kurumlarına mı yapıyorsunuz bu testleri?

MAHMUT ESAT YILDIRIM- Kamu kurumu, şirketler, gerçek kişilere kadar inebiliyoruz. Bunu yapmak için de, yine birazdan bahsedeceğim, SOME olarak adlandırdığımız, siber olaylara müdahale ekiplerimiz mevcut tüm Türkiye'de. Şu an sayısı 2500'ü geçti sanırım. Her SOME'de, bazılarında 2-3 kişi var, bazılarında 15-20 kişi var, neredeyse tüm kamu kurumlarında bir siber olaylara müdahale ekibi var ve direkt olarak bizimle koordineli çalışıyorlar.

Olay müdahale ekibimiz var. Olay müdahale aslında USOM'da en kritik işlerden birisi. Benim tabirimle bir itfaiyecilik oluyor bu. Tam polislik değil ne yazık ki, ama itfaiyecilik. Şöyle: Bizim elde ettiğimiz istihbaratla olsun, SOME'lerden gelen bilgilerle olsun, bir kurumda veya bir şirkette bir siber saldırı tespit edildiği zaman, hemen, bazen yerine giderek olay müdahale faaliyeti gerçekleştiriyoruz, bazen uzaktan gerçekleştiriyoruz ve o saldırıyı

nasıl bertaraf edebiliriz, tekrar olmaması için neler yapabiliriz, gerekirse eğitim verelim, gerekirse biz yazılım süreçlerine dahil olalım gibi birçok farklı önlemde bulunuyoruz. Burada itfaiye dememin sebebi de şu aslında: Tecrübelerimize dayanarak söylüyorum, herhangi bir siber saldırı durumunda biz olay müdahaleye gittiğimiz zaman, ne yazık ki bunun en az 7-8 ay başladığını tespit ediyoruz. Bazı yerlerde çok daha geriye gidiyor; bazı yerlerde kayıt hiç tutulmadığı için inceleme, o sürecin ne zaman başladığını tespit etme şansımız da olmuyor. Ama zaten dünya genelinde yapılan araştırmalarda, bunun günümüzde yaklaşık 6 ay gibi bir süresi olduğu söyleniyor. Bir siber saldırı tespit edildiği zaman, geriye dönük incelediğimiz zaman, o saldırının en az 6 aydır içeride olup, belki de sizin bilgi işlem personelinizden daha iyi o sistemi bilir hale geldiğini görüyoruz.

Tehdit istihbarat ekibimiz var. Yine bizim en çok önem verdiğimiz ve en güçlü kaslarımızın olduğu ekiplerimizden birisi. Bu ekibimiz de... Hepinizin bildiği çeşitli siber teknik istihbarat faaliyetleri zaten gerçekleştiriliyor; açık kaynaklar olsun, diğer faaliyetler olsun. Ama burada bizim yaptığımız bir diğer faaliyet; hem caydırıcılığı sağlamak, hem de asıl yerinde o bilgiyi toplamak için yaptığımız faaliyet siber operasyonlar oluyor. Bu, tam da isminden anlayacağınız gibi, bir hack back diye düşünebilirsiniz. Örneğin bir komuta kontrol adresini bizim zararlı yazılım ekibimiz tespit ediyor ve APT'yi inceliyor, bakıyor. Normalde USOM olarak bize verilen kanuni yetki ve sorumluluk çerçevesinde bu adresi USOM web sitesinde yer alan zararlı bağlantılar listesine ekliyoruz; eklediğimiz zaman hiçbir mahkeme kararı olmadan, otomatik olarak, yaklaşık 5 dakika içerisinde tüm ISP'ler seviyesinde engelleniyor bu adresler. Bu şekilde yapıp geçiştirebiliriz, engelleyebiliriz. Ama o zaman saldırının arka planını tespit edemiyoruz. Bunun için bir adım ileriye gitmemiz gerekiyor. Çünkü mevcutta bulunduğumuz, gördüğümüz savaş, bu siber savaş dediğimiz şey nizami bir harp değil, gayrinizami çalışıyor ve bizim de ona adapte olmamız gerekiyor. Biz çeşitli operasyonlarla komuta kontrol merkezine sızabiliyoruz; sızdığımız zaman, içeriden elde ettiğimiz birçok farklı veri çıkıyor ve bunlarla ilgili çeşitli raporlar oluşturup ilgili birimlere, kurumlara iletiyoruz. Bu konuda özellikle İstihbarat Teşkilatımız olsun, Emniyet olsun, çok sırt sırta çalıştığımız durumlar oluyor.

DevOPs ekibimiz var. Bizim USOM'da kullandığımız yazılımların tamamını geliştiren ekip bu. Aslında iyi bir şey mi, kötü bir şey mi bilemiyorum, ama şu ana kadar biz USOM olarak hiçbir paralı ürün kullanmadık, para vererek bir ürün satın almadık; tamamını, ihtiyacımız neyse hepsini sıfırdan kendimiz geliştirdik ve tamamını bu ekip geliştirdi.

Bunun yanı sıra bir regülasyon ekibimiz var. Onlar da ülkemizdeki bu siber güvenlik alanındaki faaliyetleri geliştirmek için çeşitli mevzuatlar, regülasyonlar çıkarmak için çalışmalar yürütüyorlar.

Son olarak da ağ ve sistem ekibimiz var. Bizim hem kendi iç kaynaklarımızın ağ ve sistemlerinin yönetimini yürütüyorlar, hem de USOM'un tüm operatörlerle olan işbirliğini yürütüp yönetiyorlar. Bu şu şekilde oluyor aslında: Basit bir örnek vereyim. Az önce bahsettim, bizim web sitemizde herhangi bir zararlı adresi engelliyor demiştim. Black list'e yazdığımız zaman, o adres engelleniyor. Aslında sadece engellemeyle bırakmıyoruz onları, operatörlerle otomatik yürütülen bu çalışmada o komuta kontrol adresine giden, gitmeye çalışan istekler, müdahale edilerek, USOM ... sunucularına yönlendiriliyor. Buradan müthiş bir tehdit istihbaratı çıkartabiliyoruz. Günün sonunda şu oluyor: Örneğin elimizde bir zararlı yazılım var ve bunun komuta kontrol merkezi var. Bu komuta kontrol merkezini engellediğim zaman, tüm oraya gelen istekleri yönlendirildiği zaman bana, tüm Türkiye'de o zararlı yazılım kimlere bulaşmış, hangi kurumlara, hangi şirketlere, hangi IP'lere ulaşmış, bir anda görebiliyorsunuz. Milyonlarca, milyarlarca satırdan bahsediyoruz burada. Onların incelemesini de düzenli olarak bizim teknik ekiplerimiz yürütüyor.

USOM olarak her gün karşılaştığımız saldırı çeşitleri var. Hepinizin bildiği gibi, fidye (ransomware) saldırıları var, virüsleri çokça arttı günümüzde. Ne yazık ki bu tarz saldırılara günümüz teknolojisiyle genellikle bir şey yapılamıyor. Bir kısmı zayıf algoritmalardan kaynaklı olarak kırılabiliyor, çözülebiliyor; ancak, bu saldırı başarılı bir şekilde gerçekleştirildikten sonra ne yazık ki artık bizim de yapabileceğimiz pek bir şey kalmıyor.

Bunun yanı sıra IoT botnetler var ve android botnetler var. IoT botnetler ve android botnetler özelinde birçok farklı çalışma yürütüyoruz. Vaktimiz kısıtlı olduğu için teknik detaylarına çok giremiyorum.

Asıl uğraştığımız, genellikle yoğunlaştığımız taraf da APT saldırılar oluyor, advanced persistent threat saldırıları. Çünkü kapsam tüm Türkiye olduğu

için, sürekli olarak, günde binlerce, on binlerce saldırıyla çarpışmak zorunda kalıyoruz. Bu saldırıların içerisinden de mecburen kritiklik derecesine göre seçim yapmamız gerekebiliyor bazen. Burada önceliğimiz APT'ler oluyor.

Son olarak da oltalama saldırıları tabii ki. Bizim zararlı bağlantılar sitemizde, web sitemizdeki engellediğimiz adreslerin yüzde 90'ı kadarı şu an oltalama içerikli alan adları ve IP'lerden oluşuyor. Günümüzde saldırganların en çok para kazandığı, en kolay para kazandığı yerlerden birisi bu. Şu şekilde bir istatistik verebilirim: Bugüne kadar yaklaşık 170 bin tane alan adı veya IP adresini engellemişiz. Bunların 119 bin tanesi oltalama. Tamam, biz kamu kurumlarımızı bir şekilde APT'ler ve diğer zararlı (malware) yazılım saldırılarından korumaya çalışıyoruz; başarılı olduğumuz da oluyor, olamadığımız da oluyor. Ancak, asıl buradaki büyük tehdit bana göre bu taraf. Çünkü vatandaşların her birini ayrı ayrı koruma şansımız olmuyor. Bunun için de yapmamız gereken şeyin şu olduğuna inanıyorum: Farkındalık çalışmaları. Gerekirse filmler, diziler, reklamlar, kamu spotları, halkı bilinçlendirecek çeşitli etkinlikler gibi çalışmaların ülkemiz genelinde yürütülmesi gerekiyor. Çünkü diyelim biz bir bakanlığı bu gece kurtardık. Ancak, o bakanlığı kullanan, o bakanlığın sistemlerini kullanan yüz binlerce, milyonlarca vatandaş kendi cep telefonlarından ayrı ayrı birçok saldırıya maruz kalıyorlar. Onları bu konuda bilinçlendirerek ancak bunu bertaraf edebiliriz.

Örneğin şöyle bir panel var, gördüğünüz. Bu, Anulis olarak adlandırılan android botnet zararlı yazılımına ait bir komuta kontrol merkezinin paneli. Az önce bahsettiğim bir siber operasyon sonucu biz bu paneli ele geçirdik ve içerisinde şunları gördük. Binlerce telefona bu zararlı yazılımı bulaştırmışlar, yedirmişler ve bu telefonlarda tam yetkiye sahipler. Şuradan butona tıklayarak kamerasını açabiliyor, mikrofonunu açabiliyor, içerisindeki bütün dosyaları çekebiliyor, hatta bunların üzerinde kurulu olan mobil bankacılık uygulamalarına girerek oradaki kullanacağınız şifreleri çekiyor. Diyeceksiniz ki, iki faktör var, SMS var, nasıl gelecek? Telefonda tam yetkiye sahip olduğu için, o gelen iki faktör SMS'ini de silebiliyor ve bankadaki tüm parayı boşaltıyor. Bununla da kalmıyor, yine panellerde, başka arka plan sayfalarında gördüğümüz şey, eğer banka hesabında yeteri kadar para yoksa, üzerine kredi çekiyor adamın ve o krediyi çalıyor. Bazı botlar düşünün, şu şekilde notlar almış: "Emekli, 5 gün sonra maaşı yatacak." "Memur, şu kadar borcu var." "Krediye başvuruldu, cevap bekleniyor." Bunun gibi birçok yorum eklenmiş. Dediğim gibi, bu tarz saldırılar çokça arttı. Şimdiye kadar 18 bin tane böyle komuta kontrol merkezini tespit edip engelledik. Bir tanesinde en az 5-10 bin tane kullanıcı var, telefon,

böyle düşünün. Bazılarında 20-30 bin tane.

Peki, bunları ne yapıyoruz? Yine SOME'lerimiz aracılığıyla, siber olaylara müdahale ekiplerimiz aracılığıyla ve kanunun verdiği yetkiler çerçevesinde hemen resmi yazıyla buradaki bilgileri ilgili kurumlarla paylaşıyoruz. Bu case'de, BDDK ... bankacılık sektörüyle ilişkili bu kurumlarla hem telefonların bilgilerini, hem kredi kartı bilgilerini paylaşıyoruz, hemen o kartların, o bankacılık kullanıcı hesaplarının pasife alınması noktasında telkinde bulunuyoruz.

Gördüğünüz gibi, bu şekilde bir oltalama sayfası yapıyorlar. Birçok farklı özellikleri bu panel içerisinde görebiliyorsunuz.

Benim sunumum bu kadar. Dinlediğiniz için teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- USOM İleri Güvenlik Operasyon Koordinatörü Mahmut Esat Yıldırım'a kıymetli sunumlarından dolayı çok teşekkür ediyoruz.

Bu arada, ASELSAN Genel Müdür Yardımcımız, Bilgi Güvenliği Derneği Başkanımız Sayın Taha Yücel, acil bir toplantısı olduğu için, özürlerini ileterek çıkmak durumunda kaldı. Kendilerine çok teşekkür ediyoruz.

Evet, soru-cevap bölümüne geçebiliriz.

Buyurun lütfen.

SALONDAN- USOM Koordinatörü Mahmut Esat Yıldırım Bey'e bir sorum olacak.

Acaba USOM bünyesinde ... ...

MAHMUT ESAT YILDIRIM- USOM bünyesinde kurduğumuz bir "security operations" merkezimiz var, orada birçok farklı şekilde çalışabiliyoruz, takip ediyoruz. Az önce bahsettiğim Kasırga haricinde 12 tane daha farklı projemiz var, onların da ekranlarını incelediğimiz ve çeşitli operatörlerden gelen verileri de izlediğimiz bir merkezimiz bulunuyor. Burada şunu bile görebiliyoruz: Herhangi bir şehrin bir ilçesinde anlık bir baz istasyonu kesintisi var mı, buna görebiliyoruz. Mesela 3G Ankara'nın Yenimahalle ilçesinde bir anda kesildi, 4.5G İstanbul'un Kadıköy ilçesinde kesildi. Bunda bile alarm oluşturabilecek sistemleri izliyoruz.

OTURUM BAŞKANI- Çok teşekkür ederiz. Vaktimiz biraz kısıtlı olduğu için daha fazla soru alamayacağız. Şimdi konuşmacılarımıza teşekkür belgelerini takdim etmek istiyorum. Katılımlarınız için teşekkür ederiz.


Ankara
Ticaret Odası

SİBER VATAN, SİBER GÜVENLİK ve SAVUNMA OTURUMU - 3

Oturum Başkanı: Prof. Dr. Mustafa ALKAN / Gazi Üniversitesi Adli Bilişim Anabilim Dalı Başkanı

OTURUM BAŞKANI- Sayın Başkan, kıymetli konuklar; öncelikle Elektrik Mühendisleri Odası Ankara Şubemize ve ATO'ya bu güzel etkinlikten dolayı teşekkür ederek bu oturumu başlatıyorum.

Otururumuz siber vatan, siber güvenlik ve savunma konusunda olacak. Çok kıymetli konuşmacılarımız, panelistlerimiz var. Zaman da ilerlediği için ben sözü fazla uzatmadan hızlıca kıymetli konuşmacılarımıza söz vermek istiyorum.

İlk konuşmacımız, Doç. Dr. Murat Dener hocamız, Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Anabilim Dalı Başkanı. Kendisini konuşmasını yapmak üzere kürsüye davet ediyorum.

Gazi Üniversitesi Fen Bilimleri Enstitüsü Bilgi Güvenliği Anabilim Dalı Başkanlığı konusunda kısaca birkaç bilgi vermek istiyorum.

Biliyorsunuz, siber güvenlik denildiğinde, Gazi Üniversitesi, Türkiye'deki üniversiteler içerisinde en başta gelen, en öncü üniversitelerimizden bir tanesi. Nitekim araştırma üniversiteleri içerisinde siber güvenlik konusunda YÖK tarafından yetkilendirilmiş, görevlendirilmiş üniversitelerimizin başında geliyor. Bilgi Güvenliği Anabilim Dalı Başkanlığı da Türkiye'de ilk defa Gazi Üniversitesinde açıldı ve lisansüstü seviyede eğitim veriyor. Murat hocamız da siber güvenlik konusunda Bilgi Güvenliği Anabilim Dalının başkanlığını yürütüyor, bu konuda çok kıymetli çalışmaları olan, çok yetkin bir hocamız.

Buyurun hocam.

Doç. Dr. MURAT DEĞER (Gazi Üniversitesi FBE Bilgi Güvenliği Anabilim Dalı Başkanı)- Teşekkürler hocam.

Sayın Başkanım, değerli hocalarım, kıymetli misafirler; hepinizi saygıyla selamlıyorum. Bu etkinliği düzenleyen Elektrik Mühendisleri Odası Ankara Şube Başkanı Şeref Sağıroğlu hocama ve değerli ekibine teşekkür ediyorum.

Ben de sizlere üniversitelerde siber güvenlikle ilgili ülkemiz ve dünya analizini sunacağım ve ülkemizin siber güvenlik alanında bir haritasını çıkarmaya çalışacağım.

Öncelikle kısa bir siber vatan tanımından sonra, WoS dünya ve ülkemiz analizlerinden, daha sonra ülkemizde bulunan siber güvenlik programlarından, araştırma tezlerinden, YÖK tez analizinden ve sunumun sonunda da anabilim dalımızda neler yapıyoruz, bunlardan bahsedeceğim.

İçinde bulunduğumuz devrin adı dijital çağdır. Sanayi devriminin hammaddeleri petrol, altın, demirken; dijital çağın hammaddesi ise veridir. Veriyi elinde tutanlar, demokrasiyi de, hukuku da, kişisel hak ve özgürlükleri de hiçe sayarak, kendi dijital diktatörlüklerini kurabilmektedirler. Siber dünyanın insanlığı tehdit eder hale gelmesi tesadüf değil, bilinçli bir tercihtir. Kontrolü elinde tutanlar, bu kaosu istedikleri gibi yönlendirebilme, sosyal, siyasi ve ekonomik olarak farklı ve kötü sonuçlara bunları dönüştürme imkanına sahiptir. Bu, hiçbirimizin görmezden gelemeyeceği kadar büyük bir tehdittir. Çünkü artık ülkelerin egemenlik hakları fiziki sınırlardan ziyade dijital dünyada saldırı altında bulunmaktadır. Onun için, karada ve havada yürütülen vatan savunmamızı, denizde, mavi vatanda olduğu gibi, dijital dünyada da siber vatanı içine alacak şekilde genişletmek gerektiğini hepimiz biliyoruz. Bu kapsamda siber güvenlikle ilgili bilimsel olarak dünyada neredeyiz, ülkemizdeki üniversitelerimiz ne durumda, bununla ilgili analizlerimi sizlerle paylaşacağım.

Web of Science dünya indeksi; tüm dünyadaki yapılan bilimsel akademik çalışmalar bu veri tabanında yayınlanmaktadır. Cyber security olarak başlık ve anahtar kelimelerin geçtiği şekilde Web of Science'ta analiz ettiğimizde, 1. sırada Amerika Birleşik Devletleri'nin olduğunu görüyoruz. Daha sonra Çin, Hindistan geliyor, bu şekilde devam ediyor. Avrupa'dan İngiltere, İtalya, Almanya gibi ülkeler var. Türkiye olarak ilk 10'da olmadığımızı tablodan görebiliyoruz.

Amerika Birleşik Devletleri neden 1. sırada diye kısa bir analiz yaptığımızda şunu görüyoruz: Dünyanın ilk 20 üniversitesinde yer alan tüm Amerikan

üniversitelerinin hepsinde siber güvenlik programları mevcut. Buradan da bu bilgiyi verelim.

Bu sıralamada ülkemizi 18. sırada görmekteyiz. Bizim önümüzde Avrupa'dan Fransa, İspanya, İsveç gibi ülkeler mevcut. Geçen hafta yaptığımız bir analiz bu, 314 çalışmayla 18. sırada bulunmaktayız.

Buradaki 314 çalışmayı irdelediğimizde; yıllara göre baktığımızda, 2008'de tek tük başlayan çalışmalar, 2014 yılında 10'lu sayılara, 2018 yılında 40'lı sayılara ve 2020 yılından itibaren de 50'li sayılara ulaşmış durumda.

Bu 314 çalışmayı üniversitelere göre analiz ettiğimizde, burada üniversite olarak bizleri gururlandıran bir tablo ortaya çıkmakta. Üniversitemiz 38 çalışmayla 1. sırada. 2. sırada olan ODTÜ'yle iki kat fark var arasında. Devam ettiğimizde, Ankara'dan ODTÜ'yle birlikte Hacettepe Üniversitesi de var, İstanbul'dan ise İstanbul Teknik Üniversitesi, İstanbul Kültür Üniversitesi, Boğaziçi Üniversitesi ve Yıldız Teknik Üniversitesi mevcut. Ankara ve İstanbul dışında da Fırat Üniversitesi ve Sakarya Üniversitesini görüyoruz. Burada 10'a kadar olan sayıları aldık.

Ülkemizdeki siber güvenlik programlarına önlisans, lisans ve lisansüstü seviyesinde baktığımızda şunu görüyoruz: Solda yer alanlar devlet üniversiteleri, sağda yer alanlar vakıf üniversiteleri. Sol tarafa, yani devlet üniversitelerine baktığımızda; Bandırma, Balıkesir, Akdeniz bölgesinde Burdur, Isparta, İç Anadolu'da bir tek Selçuk Üniversitesi var, Doğu Anadolu'da Erzincan ve Karadeniz'de de Giresun, Karabük, Samsun ve Zonguldak üniversiteleri mevcut. Vakıf üniversitelerinden çoğu İstanbul. Sadece OSTİM Teknik Üniversitesi Ankara, diğer üniversiteler İstanbul'da yer almakta.

Burada şöyle bir şey ortaya çıkıyor: Bu 2 yıllık önlisans bölümü İstanbul'da herhangi bir devlet üniversitesinde yok, sadece vakıf üniversitelerinde var. Bununla beraber Ege bölgesinde ve Güneydoğu Anadolu bölgesinde yine bu 2 yıllık bölümümüz yok. Ek olarak, bir önceki sonuçlarla bu çalışmayı analiz ettiğimizde, yani Web of Science'ta bu ilk 10'da yer alan üniversitelerden burada sadece Gazi Üniversitesinde mevcut, orada yer alan diğer üniversitelerde yine bu önlisans bölümleri yok.

Tabii, bu yeni bir haber ve bu haberden dolayı da mutluluk duyduk. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile YÖK arasında siber güvenlik meslek yüksekokulları açılmasına ilişkin protokol yapılmış. Daha bilgili, becerili, uygulama yetkinliği yüksek kişiler bu şekilde sektöre bu okullarla kazandırılabilecek.

Lisansa baktığımız zaman, bilgi güvenliği teknolojisi bölümü Türkiye'de 1 tane var, o da Yeditepe Üniversitesinde ve 2019 yılında kurulmuş.

Lisansüstü olarak bakalım. Yine sol tarafta devlet üniversiteleri, sağ tarafta vakıf üniversiteleri mevcut. Ahmet Yesevi Üniversitesi buna uzaktan olarak destek vermekte. Akdeniz bölgesinde Adana Bilim Teknoloji Üniversitesi mevcut, Karadeniz'de ... Üniversitesi var; Ankara'ya baktığımızda, Gazi, Hacettepe, ODTÜ var. İstanbul'da da Milli Savunma, İstanbul Teknik, Marmara, Yıldız Teknik üniversiteleri var. Yine Marmara bölgesinde Gebze Teknik ve Sakarya üniversitelerinin lisansüstü programları var. Vakıf üniversitelerinde de yine çoğu İstanbul. Bahçeşehir ve Işık üniversiteleri devam etmekte. Ankara'da TOBB ve Akdeniz tarafında da Antalya vakıf üniversiteleri bu lisansüstü programlarına devam etmekte.

Burada kırmızıyla işaretlediğimiz bölümler var, o da şöyle: Buradaki bütün bölümlerin yüksek lisans puanları var; fakat sadece kırmızıyla işaretlenenlerin doktora programları var. Bu da çok önemli. Çünkü bilimsel düzeyde siber güvenlik alanında daha iyi konumlara ulaşabilmemiz için kesinlikle bu doktora programlarının sayısının da artması lazım.

YÖKTEZ'de özet anahtar kelime ve başlık şeklinde siber güvenliği analiz ettiğimizde 125 tane tez karşımıza çıkmakta; 18'i doktora, 107'si yüksek lisans tamamlanmış tez olarak. Burada da lider olarak yine Gazi Üniversitesi var. Yüksek lisansta da yine ilk sırada Gazi Üniversitesi mevcut. Çoğunlukla Ankara ve İstanbul'daki üniversitelerde bu sayılar yüksek.

Siber güvenlik araştırma merkezlerine baktığımızda şöyle bir tablo ortaya çıkıyor: Demin saydığım önlisans programı, lisans programı ya da lisansüstü programlarda hiç yer almayan 6 üniversitenin siber güvenlik araştırma merkezleri var. Batman'da, Nevşehir'de, Yalova'da, Kayseri'de, Van'da ve İstanbul Boğaziçi Üniversitesinde bu merkezler mevcut. Yine üniversitemiz de mevcut. Ankara'da ODTÜ de var. Isparta, Samsun 19 Mayıs ve Zonguldak üniversitelerinde de bu merkezler var. Sağ tarafta da vakıf üniversitelerini görüyorsunuz; yine hepsi İstanbul, bunların siber güvenlik araştırma merkezleri var.

Bu programların da, merkezlerin de bütün üniversitelerimize yaygınlaştırılması gerekmekte.

Tabii, biz bu sunumu hazırlarken sayılardan dolayı çok gururlandık. Çünkü Gazi Üniversitesi olarak hem siber güvenlik alanında bütün programlarımız mevcut, hem de bilimsel çalışma olarak da öncüyüz ve birinciyiz.

Bunu destekleyen programlarımız; 2014 yılında kuruculuğunu Prof. Dr. Şeref Sağıroğlu hocamın yaptığı Bilgi Güvenliği Mühendisliği Anabilim Dalımız, Akıllı Şebekeler Anabilim Dalımız, yine şu an başkanlığını Prof. Dr. Mustafa Alkan hocamızın yürüttüğü Adli Bilişim Anabilim Dalımız, Mühendislik Fakültesinde bulunan Büyük Veri Analitiği Güvenliği ve Mahremiyeti Anabilim Dalımız ve Fen Fakültesinde bulunan Veri Bilimi Anabilim Dalımızla biz siber güvenlikle ilgili bilimsel çalışmalara katkılar sunuyoruz.

Bundan sonrasında Bilgi Güvenliği Mühendisliği Anabilim Dalımızı ve kısaca burada neler yapıyoruz, sizlere onu aktaracağım.

2014 yılında ilk kurulan program, siber güvenlik alanında ilk kurulan programımız. Yüksek lisans ve doktora programları mevcut.

Programımız açılırken; bilgi güvenliği mühendisleri yetiştirmek, akademik personel yetiştirmek, eğitim-araştırma kalitesini arttırmak, yarışmalar yapmak, açık kaynak içerik üretmek, katma değeri yüksek projelerin daha çok üretilmesinin önünü açmak, Avrupa Birliği güvenlik projelerinden daha fazla faydalanmak, bilişim sektörüne katkıda bulunmak; uluslararası konferanslar, sempozyumlar, çalıştaylar yapmak; işbirliği yaparken ulusal çözümler üretmek, hem de uluslararası bilgi akışını sağlamak; bilimsel birikimi arttırmak, problemleri çözebilmek, bilimsel olarak ülkemizin gelişimine katkıda bulunmak ve üniversitemizi de bu alandaki bir numaralı üniversite yapmak amaçlarımızdı.

Bu amaçlara ulaşmak için çok çeşitli ve donanımlı derslerimiz var. Siber güvenliğin temel olarak anlatıldığı, siber güvenliğin temelleri; siber savaş, savunma, güvenlik gibi, kriptolojinin anlatıldığı, bu alandaki politikaların anlatıldığı temel derslerimiz var. Ağ güvenliği, web güvenliği, gömülü sistem güvenliği, kablosuz cihaz güvenliği gibi derslerimizi yetkin hocalar vermekte. Yine bu güvenliği sağlamak için gerekli olan teknikler; yapay zekâ teknikleri, veri madenciliği, makine öğrenmesi, büyük veri analitiği gibi, tüm bunlar da derslerimiz arasında. Kritik altyapılar, blok zincir, etik hackleme, akıllı şebekelerde siber güvenlik, hibrit savaş, siber terör gibi, yine mobil yazılım analizi, görüntü ve video işleme bilgi güvenliği uygulamaları, biyometrik kimlik doğrulama, bilgi güvenliği hukuku, bilişim suçları

ve adli bilişim gibi derslerimiz mevcut ve her zaman güncel literatürü takip ediyoruz. Örneğin, siber güvenlikte derin öğrenme teknikleri ve uygulamaları, enformasyon savaşları, dijital dezenformasyon ve derin sahtecilik uygulamaları gibi derslerimiz de akademik kurulumuzda kabul edildi ve yakın zamanda, bir-iki dönem içerisinde anabilim dalımızda açılacak.

Şu ana kadar 1 doktora mezunumuz var ve bu mezunumuz da şu an İstanbul Bilişim Üniversitesinde siber güvenlik araştırma merkezi müdürü. Tabii, biz bu sayıların daha fazla olmasını ve mezun olan öğrencilerimizin bu tarz kurumlara öğrendiklerini anlatmalarını, uygulamalarını ve bunun dağılmasını istiyoruz.

Yaklaşık 2 yıl içerisinde de doktoradan mezun olacak birçok öğrencimiz var, son aşamalarına gelen.

Öğrencilerimizin çalıştığı konular arasında; blok zincir, kötücül yazılım analizleri gibi konular var. Yine saldırı tespit önleme, gerçek zamanlı veri akış analizleri, sınıflandırılması, yeni model oluşturulması gibi farklı alanlarda tezleri mevcut ve bunların üzerinde çalışıyorlar.

Şu ana kadar mezun olan 27 yüksek lisans öğrencimiz var. Bu öğrencilerimizin bu tezlerinin hepsine YÖKTEZ'den ulaşılabilir ve tezin içeriği, metni okunabilir.

Zararlı yazılım tespitleri, güvenli yönlendirme protokolü, politikalar, siber tehdit istihbaratı, bilgi paylaşım modelleri, özel ataklara karşı savunma yöntemleri, kritik altyapılarla ilgili çalışmalar, yeni siber güvenlik araçlarının geliştirilmesi, bütünleşik tehdit yönetimleri, yine kötü yazılımların analizleri, SCADA sistemlerinin güvenliği gibi birçok farklı konuda da öğrencilerimiz tez çalışıyorlar.

Tabii, biz bu yapmış olduğumuz çalışmaları hemen hızlıca yayına dönüştürüp, Web of Science'ın veri tabanında indekslenmesi için çalışıyoruz.

Burada son 2 yılda anabilim dalımızdaki öğretim üyelerinin siber güvenlikle ilgili yaptığı çalışmaların bir kısmını görüyorsunuz. Bu çalışmaların yayınlandığı dergilerin hepsi niteliği yüksek kalitede dergiler.

YÖK'ün araştırma üniversiteleri toplantısında, fen/mühendislik alanlarında siber güvenlikle ilgili üniversite seçimi konusunda yapılan toplantıda Gazi Üniversitesiyle birlikte Gebze Üniversitesi, Sabancı Üniversitesi ve İstanbul Üniversitesi Cerrahpaşa seçildi. Biz de bu kapsamda, Araştırma Üniversiteleri Destek Programı Projeleri kapsamında, anabilim dalımız bünyesinde bir proje oluşturduk, Akıllı Şebekeler İçin Zeki Siber Güvenlik Çözümleri

Geliştirme şeklinde. Projeye başlandı. Proje yaklaşık 2 yıl sürecek.

Bu proje 5 modül içermekte. Güvenli iletişim protokolü tasarımı geliştirilmesi, saldırı tespit sistemi geliştirilmesi, enerji etkin veri trafiğini yönlendirme, elektromanyetik parmak iziyle cihazları kimliklendirme ve açıklanabilir yapay zekâ yaklaşımları kullanarak bu alanda çözümler geliştirilmesi şeklinde 5 modülden oluşmakta. 2 yıl içerisinde projeyi tamamlayacağız. Yine projeyle ilgili gelişmeler hakkında anabilim dalı sayfamızda peyderpey bilgi vereceğiz.

EÜAŞ'la, Elektrik Üretim Anonim Şirketi'yle ortak bir proje için şu an görüşmeler devam ediyor. Yakın zamanda, bir-iki hafta içerisinde bunun da onaylanmasını bekliyoruz. SCADA sistemlerinde meydana gelebilecek siber atak olaylarının, önceden kesinti olmamasını içeren, saldırıları tespit edecek, makine öğrenme, yapay zekâ temelli milli yazılım modellemeleri kapsamında bir proje gerçekleştireceğiz. Bununla ilgili olarak bilgi işlem daire başkanı ve oradaki siber güvenlik müdürüyle toplantılarımız tamamlandı, kısa bir süre sonra da resmi olarak bunun da sözleşmesi imzalanacak.

Tabii, bundan önce birçok alanla ilgili proje de tamamladık.

Anabilim dalı olarak Gazi Siber Güvenlik Zirvesini düzenledik. Akıllı Ulaşımda Siber Güvenlik konulu bir seminer düzenledik. Bu, tüm belediyelerin bilgi işlem daire başkanlarının katıldığı bir seminerdi. Daha sonra Azerbaycan'daki iki üniversiteyle ortaklaşa, Uluslararası Bilgi Güvenliği Günü düzenledik. Bunlar doğrudan anabilim dalımız tarafından düzenlenenler. Fakat daha aşağıda yazdıklarımız üniversitemiz ve diğer birimleri tarafından gerçekleştirilenler. Bu alanda Şeref hocamın katkısı çok fazladır. Düzenledikleri bilgi güvenliği proje konferansları 16 yıldır düzenleniyor. Bunun gibi birçok konferans, çalıştay düzenlenmektedir.

Açık kaynak kitaplarımız var. Yine Şeref hocamın editörlük yaptığı 6 tane siber güvenlik ve savunmayla ilgili çok kıymetli kitap var. Bu kitaplar açık

kaynak, bağlantı linkleri web sayfamızda mevcut, herkes tarafından indirilebilir. Yine Uluslararası Bilgi Güvenliği Mühendisliği ile International Journal of Security Science dergilerimiz mevcut, çalışmalarımızı yayınlamak için.

Sonuçta, bizler, büyük ve güçlü Türkiye için, yurtdışı destekli, katma değeri yüksek projelerle işbirliği içerisinde, bu tezlerimizi yerli-milli ürünlere dönüştürme şeklinde ve ülkemizdeki ulaştırma, iletişim, bilişim, tarım ve sağlık benzeri bu alanlarda güvenliğin sağlanmasına bütüncül bir bakış açısıyla bakarak, bunları yapmaya çalışıyoruz.

Sunumum bu kadar. Dinlediğiniz için teşekkür ederim. (Alkışlar)

İkinci konuşmacımız, Sayın Kadir Kağan İnanoğlu, Siber Vatan Program Koordinatörü. Sunumunun konusu, "Kalkınma Ajansları Siber Vatan Programı."

Buyurun.

KADİR KAĞAN İNANOĞLU (Siber Vatan Program Koordinatörü)- Sayın Başkanım, değerli konuklar; hepinizi saygıyla selamlıyorum.

Ben Kadir Kağan İnanoğlu; Zonguldak, Karabük, Bartın illerinde faaliyet gösteren Batı Karadeniz Kalkınma ajansında uzman olarak görev yapıyorum, aynı zamanda da siber vatan programını yürütüyoruz.

Kalkınma ajansları siber vatan programına değinmeden önce biraz kalkınma ajanslarından söz etmek istiyorum.

Kalkınma ajansları, bildiğiniz üzere, Türkiye'de 26 adet bulunmakta. Bölgedeki kaynakları etkin ve verimli kullanmak, potansiyeli harekete geçirmek için araştırmalar, analizler ve raporlar hazırlamakta; müdahale etmeyi uygun gördüğü alanlarda da çeşitli destek mekanizmalarıyla harekete geçebilmektedir.

Gün boyu bütün konuşmacıların değindiği siber güvenlik konusu kapsamında Batı Karadeniz Kalkınma Ajansı olarak biz de ekosistemin ihtiyaç duyduğu nitelikli insan kaynağının geliştirilmesi amacıyla bir program geliştirdik; siber vatan programı. Bu programla amacımız, bölgemizde siber güvenlik alanında istihdam edilecek nitelikli insan kaynağının geliştirilmesi ve dijital teknolojiler alanında girişimlerin arttırılması.

Bölgemiz, maalesef, girişimcilik kültürünün çok gelişmediği bir bölge. Biz, siber vatan programıyla, teknik eğitimler veriyoruz, teknik eğitimlerden sonra girişimcilik programları düzenlemeye çalışıyoruz.

Biraz programın bugüne kadar gelmiş olduğu önemli merhalelerden bahsetmek istiyorum.

Aslında 2014 yılında sadece kamu kurumlarının bilgi işlem sorumlularına teknik destek projeleri kapsamında birtakım eğitimler verdik. Sonrasında, Zonguldak Bülent Ecevit Üniversitesinde Karaelmas Uygulama ve Araştırma Merkezi kuruldu. 2018 yılında biz üniversitelerle daha fazla işbirliği geliştirmeye başladık. Çünkü bizim hedef kitlemiz üniversite öğrencileri. Üniversitelerle gidip toplantılar yaptık, görüşmeler yaptık, "Böyle bir fikrimiz var, bunu hayata geçirmek istiyoruz, bunun en önemli paydaşları olarak bizlere yardımcı olabilir misiniz?" dedik. Üniversitelerle temasımız 2018 yılından itibaren başladı ve 2019 yılında da programın ilk eğitimlerini başlatmış olduk. Öğrencilerin moral ve motivasyonlarını arttırmak için de çeşitli yarışmalara katıldık, bu yarışmalarda da önemli dereceler elde ettik. 2020 yılında ise yaptığımız çalışmaların tanıtımını biraz daha arttırabilmek için siber vatan isminin marka tescilini aldık.

Programın modüllerinden kısaca bahsedeyim.

Bir müfredatımız var, AB kapsamında oluşturduğumuz bir müfredatımız var. 13 tane eğitimimiz var müfredatta. Biz, Batı Karadeniz Kalkınma Ajansı olarak bu programı uyguluyoruz, 13 tane eğitimi öğrencilere vermek istiyoruz. Süre olarak yaklaşık 3 yıla yaygın bir şekilde programı yürütmeye çalışıyoruz. Burada çeşitli farkındalık eğitimlerimiz de oluyor, etkinliklerimiz de oluyor; birazdan detaylarından bahsedeceğim.

2019 yılında başlattığımız siber vatan programında bugüne kadar 60 eğitim gerçekleştirdik. Bu eğitimleri yıl olarak bölersek, 2019 yılında 110 öğrenciyle başladık, 2020'de sadece Karabük ve Bartın'ı içerecek şekilde 70 öğrenciyle ilerledik, 2022 yılında ise tekrar 120 öğrenciyle eğitimlerimize devam ettik. 2021 yılında pandemiden dolayı yeni bir program başlangıcı yapmadık.

Geldiğimiz noktada siber güvenliğin bazı konularında belli bir seviyeye

geldiğimizi düşünüyorum. Bunlar; web güvenliği, zararlı yazılımlar ve tersine mühendislik, yapay zekâ, blok zincir, mobil uygulama, oyun geliştirme. Öğrencilerimiz belirli eğitimlerden sonra takımlara ayrılıyorlar ve bu takımlara girmeye çalışıyorlar.

18 yarışmaya katıldık, bu yarışmalardan önemli dereceler elde ettik. Yapmış olduğumuz çalışmalar neticesinde insan kaynağını daha ekonomik bir şekilde kullanabilmek için 3 tane firma Zonguldak Teknopark'ta ofis açtılar ve bütün 3 yılı baz alırsak da yaklaşık 85 öğrencinin istihdamına katkıda bulunmuş olduk.

Bizim en çok üzerinde durduğumuz konu ise genç girişimcilik. Eğitimlere aldığımız 3 öğrencimiz ortak bir şirket kurdular, Cyrops Siber Güvenlik A.Ş. adında. Zonguldak'ta böyle bir şirket kurdular ve giderek de büyüyorlar, epey de önemli çalışmalar yapmaya başladı bu arkadaşlarımız.

Teknofest Hack Karadeniz. Yine bizim yapmış olduğumuz çalışmalar neticesinde, Teknofest'in en önemli yarışmalarından bir tanesi olan bu yarışmayı Dijital Dönüşüm Ofisi Zonguldak'ta yapmaya karar verdi. Bu yarışmanın gerçekleştirilmesi faaliyetini de. Batı Karadeniz Kalkınma Ajansı ve siber vatan ekibi yürütüyor. Bize güvendikleri için buradan bir kez daha kendilerine teşekkür ediyorum.

Az önce bahsetmiş olduğum istatistiklerin yıllara göre dağılımı yer alıyor burada.

Bizim siber güvenlik alanında yapmış olduğumuz çalışmaların olumlu sonuçlarından dolayı Bakanlığımız siber güvenlik alanında koordinatör ajans görevini bize tevdi etti, 2021 yılının ortalarında. Biz hemen bu koordinatör ajans görev ve sorumluluğu kapsamında ajanslarla bir toplantı yaptık, onlara yaptığımız çalışmaları anlattık, sektörün insan kaynağı açısından duymuş olduğu ihtiyacı, beklentiyi belirttik ve daha rafine, daha istihdam odaklı bir programı nasıl geliştirebiliriz şeklinde görüşmeler yaptık. Sonrasında Savunma Sanayi Başkanlığımızla birlikte toplantılar yaptık. Çünkü biraz da istihdam odaklı bir program olmasını istiyorduk. "Biz eğitimleri verelim, belli bir seviyeye getirelim, bu getirdiğimiz seviyeden sonrası artık top sizde olsun" dedik. Yaklaşımımız buydu. Onlar da çok olumlu yaklaştılar, Türkiye Siber Güvenlik Kümelenmesi vasıtasıyla bu programın içerisinde yer alabileceklerini söylediler ve programın başlangıcını 2021 yılının Ocak ayında yapmış olduk.

Program, Sanayi Teknoloji Bakanlığı ve Savunma Sanayi Başkanlığı işbirliğiyle, Kalkınma Ajansları Genel Müdürlüğü koordinasyonunda, kalkınma

ajansları, Türkiye Siber Güvenlik Kümelenmesi ve üniversiteler tarafından uygulanmakta. Daha da büyütmek istiyoruz açıkçası.

Temel olarak programın faaliyetleri şunlar: Siber güvenlik eğitimleri, eğitimlerin olmadığı dönemde usta-çırak buluşmaları ve saha gezileri, konferanslar ve staj desteği.

Program uygulama sürecinden kısaca bahsetmek istiyorum.

Bu programı kendi bölgesinde uygulamak isteyen ajans, üniversitelerle görüşmeler gerçekleştiriyor, üniversitelerden eğer bu işbirliğine olumlu yanıt alırsa bir protokol imzalıyorlar ve bu protokol çerçevesinde üniversiteler çağrıya çıkıyor, yani öğrencilere duyuruyor, böyle bir eğitim programı gerçekleştirilecek diye. Ve başlık topluyor. Bu başlıkları da yine sibervatan.org internet sitemizden topluyoruz. Gelen başlıkları kalkınma ajansının temsilcisi, üniversitenin bu program kapsamında belirlemiş olduğu formatta değerlendiriyor ve belirlemiş oldukları kontenjan dahilinde öğrencileri seçiyor ve eğitime dair öğrencilere geri bildirimde bulunuyor, yine öğrencilerin detaylı bilgileri de sisteme yükleniyor. Daha sonra eğitimler gerçekleşiyor. Gerçekleştirilen eğitimlerden sonra biraz daha yetenekli öğrencileri stajyer aday havuzuna alacağız. Daha henüz kimseyi staja göndermedik. Çünkü henüz daha üçüncü eğitimdeyiz, üç tane daha eğitimimiz var, daha yolun yarısındayız.

Birazdan bahsedeceğim, 2022 Temmuz ayında Antalya'da Kalkınma Ajansları Siber Vatan Bootcamp gerçekleştirdik. Burada 7 farklı üniversiteden öğrenci vardı, yaklaşık 90 öğrenciyle 10 gün boyunca Antalya'da teknik eğitim gerçekleştirdik. Burada hiçbir hizmet alımı gerçekleştirmedik; doğrudan bizim önceki programlardan mezun olan, halihazırda çeşitli kamu kurumlarında ve özel sektörde çalışan öğrencilerimiz kendileri teknik eğitim verdiler yeni öğrencilerimize. Böyle sıkı bir kamp gerçekleştirmiş olduk

Antalya'da ve o eğitim sonucunda az önce bahsetmiş olduğumuz takımlara öğrencilerin dağılımını gerçekleştirdik.

Programın son durumu bu şekilde. Halihazırda programı uygulayan KUSKA'yla birlikte 5 ajansa ulaşmış olduk. Toplamda 280 öğrenciye ulaşmış oluyoruz ve ilk eğitimimizi de geçen hafta Kuzey Anadolu Kalkınma Ajansı gerçekleştirmiş oldu. 13 eğitim gerçekleştirdi. 280 öğrenciyle programa devam ediyoruz.

Bu eğitimleri gerçekleştiriyoruz, öğrencilere teknik eğitimler veriyoruz, çeşitli programlarla öğrencilerin donanımlarını arttırmaya çalışıyoruz; ama sürdürülebilirlik konusunda bir soru işareti vardı bizde. Bunu gidermek için bir projemiz vardı. Bakanlığın kendi içerisinde farklı destek mekanizmalarından yararlanmak istiyorduk. Bakanlığa siber güvenlik kuluçka merkezi adında bir proje sunmuştuk. İlk etapta kabul edilmedi bu; ama sonra, bizim ısrarlı çalışmalarımız sonucunda Bakanlığımız kabul etti. Önümüzdeki dönemde, muhtemelen 2023 yılında Zonguldak Bülent Ecevit Üniversitesinde, Karabük Üniversitesinde ve Bartın Üniversitesinde siber vatan yetkinlik merkezlerini kurmuş olacağız. Buradaki amacımız şu: Öğrenci nereden eğitim alacağını bilsin. Yani teknik eğitimlerin verileceği bir salon olmasını planlıyoruz. Sonrasında yine siber vatanın altyapılarında öğrencilerin 7/24 istedikleri zaman çalışma programı yapabilecekleri alanları oluşturmayı planlıyoruz. Ve sadece ekosisteme bir insan kaynağı olarak dahil edilmekten ziyade, kendi şirketini kurarak ekosistemden bir pay almak amacıyla öğrencilere çeşitli hızlandırıcı programlar uygulamak istiyoruz bu merkezlerde.

Bu, Zonguldak Bülent Ecevit Üniversitesinin bize tahsis etmiş olduğu yer. Bu binanın alt katını, yaklaşık 500 metrekarelik bir alan, bize tahsis etmiş durumda. Bunlar da içeriden görüntüleri.

En hazır alanı bize Bartın Üniversitesi tahsis etti. Yeni kurulan, çok modern bir kütüphanede bir alan bize tahsis etti Sayın Rektörümüz. Orada sadece tefrişatı yapıp, eğitime başlayabilecek durumdayız.

Benim kalkınma ajansları siber vatan programı kapsamında anlatabileceklerim şimdilik bu kadar. Çok teşekkür ediyorum. (Alkışlar)

OTURUM BAŞKANI- Biz teşekkür ederiz.

Evet, gerçekten de kalkınma ajansları çok ciddi bir rol üstlendiler ve çok ciddi faaliyetler, çalışmalar yürütüyorlar. Umarım bu şekilde devam ederler. Kadir Bey'e de bu güzel sunumu için teşekkür ediyoruz.

Bir sonraki konuşmacımız, yine bu siber vatan kapsamında bir başarı hikayesi olan bir arkadaşımız. "Başarı Hikayesi: Bartın Siber Vatan Projesi" başlıklı sunumunu yapmak üzere Dr. Öğretim Üyesi Eyüp Burak Ceyhan'ı kürsüye davet ediyorum.

Buyurun Eyüp Bey. (Alkışlar)

Dr. Öğretim Üyesi EYÜP BURAK CEYHAN (Bartın Siber Vatan Proje Koordinatörü)- Sayın Başkanım, değerli katılımcılar; ben Dr. Öğretim Üyesi Eyüp Burak Ceyhan, Bartın Üniversitesinde bilgisayar mühendisliği öğretim üyesiyim. Aynı zamanda Bartın Siber Vatan Projesinin koordinatörlüğünü yürütüyorum.

Siber vatan projesiyle ilgili detaylı bilgileri zaten Kadir Bey çok güzel bir şekilde anlattı, o yüzden ona çok girmeyeceğim. Ama bu siber vatan projesi kapsamında neler yapıyoruz, ona değinmek istiyorum. Ben aynı zamanda Siber Güvenlik ve Akıllı Sistemler Kulübü danışmanı olarak görev yapıyorum Bartın Üniversitesinde. İkisinin birlikte olmasının verdiği avantajlar neler oluyor, bunlardan biraz bahsetmek istiyorum. Çünkü öğrenci kulüplerinin burada diğer arkadaşlarını motive etme açısından çok verimli olduğunu bizzat yaşadım, gördüm. Bu siber vatan projesinde de yine bu arkadaşların ciddi katkısı oldu. Bu kulüpteki arkadaşlarımız, siber güvenlikle hiç ilgisi olmayan arkadaşları da bu programa dahil ederek, sonrasında bu ekosisteme çok güzel bir şekilde fayda sağladılar. Elde ettiğimiz başarılardan bahsedeceğim zaten. Bu ikisini belirtmemin sebebi, bu ikisi arasındaki ilişki de çok büyük bir katkı sağlıyor. Kadir Bey'in dediği gibi, birçok kalkınma ajansında yeni başlayacak bu program, oralara da faydası olur diye düşünüyorum.

Bunlardan bahsetmeyeceğim, çünkü siber vatan programıyla ilgili bilgi verildi.

Faaliyetlerin ücretsiz olduğunu, öğrencilere ücretsiz verildiğini söylemek istiyorum öncelikle.

Kazanımlar neler? Belki şunu söylemek lazım: Katılım sertifikası her eğitimden sonra veriliyor, bir de sene sonunda genel bir katılım sertifikası, yani bu projeye katılım sertifikası veriliyor.

Biz Bartın Üniversitesi olarak bu projeye 2020 yılında, tam pandemi başlarken dahil olduk. Ama bu süreçte eğitimleri planlamıştık zaten; dolayısıyla eğitimlerin yarıda kalmaması için, o pandemi şartlarında, dışarı çıkma yasakları olmasına rağmen, öğrenci arkadaşlarımıza özel izin alarak, yurtlar-

da özel odalarda birer kişi kalmalarını sağlayarak, o şartlarda bu eğitimlere başladık. 2021 yılında yeni öğrenciler kattık ekibimize. 2022 yılında da aynı şekilde. Bundan sonrasında da eğitim ekibimize yeni öğrencileri katmayı planlıyoruz.

Biraz sonra anlatacağım faaliyetler, az önce bahsettiğim Siber Güvenlik ve Akıllı Sistemler Kulübümüz ile Siber Vatan Projesinin ortak faaliyetleri. Birbirlerini aslında besliyor bunlar. Çünkü bu kulüp faaliyetleri bir farkındalık oluşturmuş. Biz 2018 yılında kurduk bu kulübü ve 2018'den 2020 yılına kadar bir altyapı oluşturmuştuk. Sabah sunumlarını gerçekleştiren Mustafa Şenol Bey de HAVELSAN ekibi olarak katılmışlardı bizim faaliyetlerimize. Hatta Ahmet Hamdi Bey de katılmıştı. Yani bir altyapı oluşturmuştuk; eğitimler, konferanslar, çalıştaylar düzenliyorduk zaten. Bu Siber Vatan Projesiyle birlikte bu daha üst seviyeye taşındı.

2018 yılında, kulübümüzün ilk kurulduğu zamanlarda Siber Kulüpler Birliğine üye olduk. Bunu zaten hepimiz biliyoruzdur, Türkiye Siber Güvenlik Kümelenmesinin de desteklediği bir birlik aslında bu. Buraya üye olarak kulübümüzü buraya kaydettirmiş olduk. Bunun çok büyük faydaları oldu. Çünkü düzenlemek istediğimiz faaliyetlerde bu birlik bize eğitimci sağladı. Yani biz hiçbir masraf yapmadan, para ödemeden bu eğitimleri bitirebilmiş olduk bu birlik sayesinde. Mesela bunlardan bir tanesi, "Siber Tehdit İstihbaratında Büyük Veri Analitiğinin Önemi" konulu seminerdi. Yine onlar sağlamıştı bize bu etkinliğimizi. Burada da SwordSec'ten Seyfullah Kılıç bu eğitimi verdi.

Şeref hocanın benim üzerimde emeği büyüktür, bunu söylemeden geçemeyeceğim. Ben Gazi Üniversitesinde yüksek lisans ve doktora yaptım, Şeref hocamın danışmanlığında. Bütün bu vizyonu aslında orada kazandım. Yani bu yaptığımız faaliyetlerin hepsini biraz da ona borçluyuz. Onun bu aktifliğini gördüğümüz zaman zaten biz de aktif olmaya gayret ediyorduk. Bartın Üniversitesine gittiğimiz zaman da biz aslında onu sadece sürdürmüş olduk, yeni bir şey yoktu aslında.

Yine arkadaşlarımızın 2021 yılında ISCTurkey'e katılımını sağladık. Siber güvenlik farkındalığını aslında burada kazanmaları için tekrar bir teşvik oldu onlar için.

Yine Teknofest Hack İstanbul'a katıldık; yanlış hatırlamıyorsam, 2019 veya 2020'ydi. Daha yeni yeni aslında bu kulüp faaliyetlerini gerçekleştiriyorduk. 6 tane takım oluşturduk; bu 6 takımdan birisi İstanbul'da beşinci oldu, birisi altıncı, diğerleri yedi, sekiz, dokuz ve altmış birinci oldular. Bu aslında bizim ilk yaptığımız faaliyetlerden biri olduğu için ve beşincilik, altıncılık gibi yüksek dereceler aldığımız için güzel bir başarıydı bizim için.

Başka bir faaliyetimiz de şu: Siber vatan öğrencilerimiz, o Siber Vatan Projesi kapsamında öğrendiklerini kulüp çalışmaları kapsamında kendi arkadaşlarına da aktardılar. Bu da yine kulübün bir avantajı şeklinde ortaya çıkmış oldu. Elde ettikleri bilgileri kendi kulüpteki arkadaşlarına da öğreterek farkındalık sağlamış oldular.

Bu da yine büyük bir projeydi; Bartın'daki ortaokul ve lise öğrencilerine siber güvenlik ve kodlama eğitimi. Aslında farkındalık eğitimi verdik biz burada, siber güvenlikle alakalı farkındalık kazandırmak amaçlı verdik bu eğitimi. 16 ortaokul ve liseden 850 öğrenciye biz bunu vermiş olduk. Bu, yanlış hatırlamıyorsam 2018 yılındaydı. Burada da yine kulüp öğrencilerimiz bizzat eğitim veren konumunda oldular, biz de katılım sağladık, biz de eğitim verdik ve hep birlikte, hem hocalar, hem öğrenciler olarak okula giderek bu eğitimleri gerçekleştirdik. Bazılarını kendi üniversitemizin laboratuarlarında yaptık, bazı eğitimleri bizzat kendimiz okullara giderek yaptık. 4 haftalık yoğun bir süreç geçti, yani 4 haftada tamamladık bu eğitimleri.

Bunlar da o eğitimden kareler.

Siber güvenlikte kariyer ve uygulamalı IP sızma testi eğitimi düzenledik. Bunu da yine Türkiye Siber Güvenlik Kümelenmesinin desteğiyle gerçekleştirdik, eğitimcimizi onlar sağladı.

Siber Güvenlik ve Bilgi Güvenliği Panelini düzenledik. Burada sunum yapan hocaları bu sefer kendimiz bulduk.

Siber Güvenlik Zirvesine katılım sağladık. Batı Karadeniz Kalkınma Ajansı BAKKA'nın düzenlediği bir zirveydi bu. Dijital Dönüşüm Ofisi Başkanı Dr. Ali Taha Koç Bey'in ve Savunma Sanayi Başkan Yardımcısı Murat Şeker'in katıldığı bir zirve oldu bu. Öğrencilerimiz buradan çok bilgiler elde etti. Bu etkinliğin sonunda bir yarışma düzenlendi, orada da Start-Up Weekend diye bir etkinlik düzenlendi bu zirvenin peşinden, o etkinlikte de yine arka-

daşlarımız üçüncülük elde ettiler.

Siber Vatan Projesi kapsamında Certified Ethical Hacker (CEH) ve Linux eğitimleri verildi. Bu yine pandeminin başlangıcında veya belki ortalarına doğru verdiğimiz bir eğitimdi.

Sonra Teknofest Hack Karadeniz Yarışmasına katıldık. Daha doğrusu şöyle oldu: Teknofest Hack Karadeniz Yarışmasının düzenlenmesinde bizim siber vatan öğrencilerimizden de destek sağlandı. Dolayısıyla, Bartın siber vatan ekibi olarak bu Hack Karadeniz'de de katkımızın olduğunu görmek bizi memnun etti.

Yine biraz önce bahsetmiştim, Siber Vatan Projesi kapsamında bir yaz kampı yapıldı. 10 günlük bir etkinlikti bu, güzel bir etkinlikti. Mustafa Varank ve Ali Taha Koç da buraya katılım sağlamışlardı, ziyaret etmişlerdi ve öğrencilerimizi motive etmişlerdi.

Hacktrick Yarışması. En önemli başarımızı Mayıs 2022'de burada elde ettik. Hacktrick yarışmasında birincilik ödülünü aldık. Bu yarışmaya aslında birçok üniversiteden; Gazi, Hacettepe, Marmara gibi birçok büyük üniversitelerden de katılım olmuştu. Bizden de bu yarışmaya bizim hem Siber Vatan Projesi, hem de Siber Güvenlik ve Akıllı Sistemler Kulübümüzün öğrencileri olan 4 öğrencimiz katıldı. Onlardan biri de şu an aramızda, Sefa arkadaşımız, kendisini de buraya davet ettik. Arkadaşlarımız bu yarışmada güzel bir başarı elde ettiler. Bu başarı öğrencilerimizi çok motive etti. Çünkü Bartın Üniversitesi yeni kurulmuş bir üniversite, "Biz bir şey yapamayız; biz düşük puanla girdik buraya, başaramayız" gibi düşünüyorlardı, derslerde de hep bunu söylüyorlardı. Ama bunun böyle olmadığını hissettirmiş olduk onlara. Yani Sefa ve diğer arkadaşları, bu fotoğraftaki diğer arkadaşları -şu an zaten çeşitli kurumlarda, firmalarda işler de yapıyorlar- bunun böyle olmadığını, Bartın Üniversitesi veya benzeri yeni kurulan bir üniversitenin de bu ligde

yer alabileceğini aslında göstermiş oldular, kanıtlamış oldular. Bu güzel bir başarıydı.

Yine az önce bahsettiğim zirvenin sonunda yapılan etkinlikte de Bartın Üniversitesi üçüncü oldu. Kendi fikirleriyle yarışmış oldular bu yarışmada.

Yaklaşık 1 ay önce de STM'nin yaptığı bir yarışma vardı, CTF yarışması. Burada 156 takım, 813 yarışmacı katılmıştı ön elemeye. Ön elemeyi geçen 200 yarışmacı ve 50 takımla Yıldız Teknik Üniversitesi Davutpaşa Kampüsünde yüz yüze bir yarışma gerçekleştirildi ve bu yarışmada da... Burada firma temsilcilerimiz de var, belki şöyle bir önerim olabilir: Bir CTF yapıldığında öğrenciler ile sektörde uzun zamandır çalışan kişileri ayırmak gerekiyor sanki veya öğrencileri farklı kategorilerde değerlendirmek lazım. Mesela orada çok başarılı öğrenciler vardı, ilk yarışmaya katılan öğrencilerimiz yine buraya katıldı, ama şöyle oldu: Sektörde uzun yıllardır çalışan, çok tecrübeli, 10 yıllık tecrübesi olan kişilerle aynı kategoride değerlendirilince bu sefer on dördüncü oldular burada. Belki çok daha başarılı olabilecekleri şey açısından ve belki kendilerini ilerideki yarışmalar için daha iyi motive edebileceklerdi. Yeri gelmişken bu önerimi de söylemek istedim. Kulüplerden arkadaşlarımın da buna destek verdiklerini şu an görebiliyorum. Umarım değerlendirilir.

Dinlediğiniz için çok teşekkür ediyorum. (Alkışlar)

OTURUM BAŞKANI- Biz teşekkür ediyoruz hocam, sağ olun.

Evet arkadaşlar, her başarı öyküsünün arkasında böyle isimsiz kahramanlarımız var, fikir liderleri, düşünce liderleri var. Önce bir kıvılcımla başlayan çalışmalar, sağ olsun, böyle yetkin öğretim hocalarımız sayesinde buralara kadar geliyor, birçok başarı öyküsü ortaya çıkıyor. Emekleri için herkese teşekkür ediyoruz, Sefa kardeşimize de başarılar diliyoruz, bu güzel başarısından dolayı tebrik ediyoruz. Bartın Üniversitesine de teşekkür ediyor, başarılarının devamını diliyoruz.

Son konuşmacımız, yine bir başarı öyküsü, Gazi Üniversitesinden genç arkadaşların oluşturduğu Gazi Cyber Öğrenci Topluluğu Başkanı Mustafa Öztürk'ü davet ediyorum. (Alkışlar)

Buyurun.

MUSTAFA ÖZTÜRK (Gazi Cyber Öğrenci Topluluğu Başkanı)- Merhabalar. Ben Mustafa Öztürk, Gazi Cyber Öğrenci Topluluğu Başkanıyım. Aynı zamanda toplulukta 3. yılım. Aslında topluluğa başlama hikayem, kendi yazdığım yazılımların siber güvenlik yönünden zaaflarını fark edip,

bunları nasıl daha iyi hale getirebilirim diye araştırmamla başladı. Sonrasında kendi yazdığım ... ne kadar başarısız olduğunu zamanla gördüm ve sonrasında Gazi Cyber ekibine girdim ve bu şekilde devam ettim.

Az önce Burak hocamın bahsettiği her şey beni aslında çok gururlandırdı ve sektöre yeni atılmış bir insan olarak doğru yolda olduğumu bana hissettirdi. Çünkü ben aynı zamanda Burak hocamın bahsettiği Kulüpler Birliği Yönetim Kurulu üyesiyim, yine Gazi Üniversitesi Bilgisayar Mühendisliği Bölümü öğrenci temsilciyim. Az önce STF'deki etkinlikten bahsedildi, topluluk olarak da organizasyon ekibinde yine biz vardık ve Burak hocamın bahsettiği noktaya geldik.

Burak hocamın STF yarışmalarına ilişkin yaptığı eleştiriyi haklı buluyorum; gerçekten de öğrenciler ile sektörde çalışanların ayrılması gerektiğini ben de düşünüyorum. O STF'in hazırlandığı dönemde ben STF'i yapan kurumda stajyerdim ve dolayısıyla STF'e sorular hazırlamamız da gerekiyordu ve bazı arkadaşlardan aldığım uyarılarda soruların gerçekten güzel olduğunu öğrenmiş oldum.

Benim bugün buraya gelme amacım, siber tehdit istihbaratı ve dark web hakkında bir derleme yapmak ve kendi yaptığım araştırmalarla öğrendiklerimi sizlere aktarmak ve global ölçekte ülkemizin nerede olduğuna ilişkin bir bakış açısı sunmak.

Öncelikle siber tehdidin ne olduğuyla başlamak istiyorum.

Siber tehdit, teorik anlamda üç farklı bileşenden oluşur. Bunlardan birincisi niyettir, diğeri kabiliyet ve üçüncüsü de fırsattır. Eğer bu üç bileşen aynı anda bir araya gelirse bir siber tehdidimiz var demektir.

Siber tehdit, sözlük tanımı olarak, kötü niyetli kişi veya kişilerin, kurumların, sistemlere yetkisiz erişimleri veyahut da sistemleri kısmen ya da tamamen kullanılamaz hale getirme girişimleri olarak ifade edilebilir. Fakat bizim için en önemli etken bu üç bileşenin, niyet, kabiliyet ve fırsat üçgeninin tamamlanması. Aksi takdirde tehdit sürekli yarım kalacak ve ciddi olarak kaygı duyabileceğimiz bir siber tehditle karşı karşıya olmayacağız.

Dark web, bu bahsettiğimiz siber tehditlerin sürekli meydana geldiği, buradaki aktörlerin kendi aralarında haberleştiği veyahut da kendi paydaşlarına haberler gönderdiği karanlık bir mecra. Burada envai çeşit suç trafikleri var, uyuşturucu da var, kaçak da var vesaire gibi bileşenleri içeren belalı ve pis bir internet.

Peki, madem bu kadar pis bir mecra, bunu biliyoruz, bizim dark web'te, deep web'te ne işimiz var?

Biz aslında normal internete çıktığımızda, Google'den herhangi bir arama yapıp eriştiğimiz bir web sitesinde sadece o koskoca internetin yüzde 4'ünü görebiliyoruz. Kalan yüzde 96'lık kısım bizim erişemediğimiz kısımda kalıyor. Dolayısıyla, bizler de dark web'te bu tehdit aktörlerinin neler yaptığını, bu tehdit aktörlerinin tekniklerini, taktiklerini, prosedürlerini keşfetmeye ve aslında siber tehdit istihbaratın temelini atmaya çalışıyoruz. Çünkü siber tehdit istihbaratı dediğimiz şey aslında bir siber güvenlik olayı; herhangi bir tehditle karşılaşmadan veya saldırıya uğramadan önce, gelebilecek olan tüm saldırıları ve tehditleri öncesinde tespit edip, bunlara öncesinde önlem alarak, bu saldırıların gerçekleşmeden engellenmesini sağlamaktır. Siber tehdit istihbaratın temeli budur.

Siber tehdit istihbaratın çok çeşitli adımları ve basamakları var, farklı farklı bileşenleri de bünyesinde barındırıyor. Fakat kurumlar özelinde düşündüğümüzde, ki Siber Vatan Çalıştayında kurumlardan bağımsız tüzel kişilere ya da bireysel bir şeye değinmekten ziyade kurumlar üzerinden bu süreci götürmek daha mantıklı.

Kendimizi kurum yerine koyduğumuzda ilk soracağımız soru: Saldırıyı tahmin edebilir miyim? Siber tehdit istihbaratın … model diye bir kavramı var ve bu … model kavramının bize bazı önermeleri var. Bu modelin bize verdiği önermelerden bir tanesi şu: Dışarıda her zaman senin açığını kollayan ve sana zarar vermek isteyen hacker'lar, APT grupları, … grupları var ve bunların varlığını asla yadsıyamazsın. Dolayısıyla, biz de sistemimize her zaman bir saldırı gelebileceğini tahmin etmemiz gerekir. Bu tahmini yapabilmek için en önemli bileşenimiz, atak yüzey analizlerimiz ve atak yüzeyinin yönetilmesi.

Diyelim ki saldırıyı tahmin edemedik. Sonraki soru: Saldırıya karşı erken önlem alabilir miyim? Saldırının geleceğini tahmin edemiyoruz; ancak, olası bir saldırıda erkenden buna reaksiyon göstermem mümkün mü? İkinci sorumuz bu.

Bunu da geçtik, üçüncü soru: Saldırıyı önleyebilir miyim? Artık sistemimize

saldırı geldi ve saldırı altındayız, her yer alarm veriyor, bu saldırıya karşı bir çözümümüz var mı, herhangi bir yaklaşımımız var mı, bunu irdeleriz.

Bunu da önleyemedik diyelim, sistemimiz zarar gördü, saldırı gerçekleşti vesaire. Dördüncü soru: Sonraki saldırı için hazır mıyım? Çünkü istatistiksel olarak, eğer bir saldırı geldiyse sisteme, mutlaka bir diğer saldırı da gelecektir ve bunun için bizim mutlaka önlem almamız gerekmektedir.

IBM'in 2022 yılında yaptığı, ... Faaliyeti isimli bir araştırması var. Burada bazı dikkat çeken istatistikler var. Bu çalışma kapsamında 550 tane firma değerlendiriliyor ve bunların 20 tanesi Türkiye'den. Çalışmada yer alan kurumlardan yüzde 83'ü daha önce bir siber saldırıya maruz kalmışlar. Dolayısıyla, az önce sorduğumuz soruyu birebir doğrulayan, destekleyen bir istatistik. Çünkü bir saldırı aldıysanız, sıradaki tekrar gelecektir. Kritik altyapı sistemleri dediğimiz, enerji üretimi, enerji dağıtımı, su ve kanalizasyon sistemleri, hastaneler, barajlar vesaire gibi kuruluşların ise yüzde 79'u mevcut siber güvenlik protokollerinde sıfır güven politikası dediğimiz politikayı uygulamıyor. Sıfır güven politikası da, elimizden geldiğince erişimleri kısıtlayıp, her ne kadar güvensek de önce doğrulama anlayışıyla yaklaştığımız bir politika. Ki büyük kurum ve kuruluşların ciddi manada güvenliğini arttıracak unsurlardan bir tanesi. İlginç şekilde, yaşanan ihlallerin yüzde 45'i bulut teknolojilerinden kaynaklanıyor. Ki geçtiğimiz sene bu oran çok daha fazlaydı. Bunun nedeni ise şu: Halihazırda buraya katılanların yüzde 43'ü bulut teknolojilerine yeni adapte olmaya başlamışlar ve daha yeni yeni bu sisteme geçiyorlar. Ki bulut teknolojileri dediğimiz kavram da ülkemiz ve dünya açısından çok eski bir kavram olmadığı için, ilk çıktığında ve ilk duymaya başladığımızda ... kavramıyla gündemimize girdi. Sonrasında yeni yeni ... title'ına dönüştü. Bu title'lar bulut teknolojisinin hazır sistemlere entegrasyonu ve bunların güvenliğini sağlama adına çalışan title'lar. Dolayısıyla, işgücünün de teknolojiye yeni girişinin getirdiği yüzde 45'lik bir veri ihlali durumu söz konusu. Buradaki ihlallerin yüzde 19'u da şirketlerin doğrudan kendilerinden değil de birlikte çalıştığı, iş ortaklığı yaptığı firmalar tarafından, onların güvenliğinin ihlali sonucu gerçekleşen ihlaller. Bu da aslında sadece kendi güvenliğimizin değil, komşumuzun da, iş ortağımızın da, arkadaşımızın da güvenliğinin ne kadar önemli olduğunu gösteriyor. Yani bütün sistemleri aslında siber vatan kapsamında değerlendirebileceğimiz bir durum söz konusu. Bütün kurum ve kuruluşların güvenli olduğundan emin olmalıyız ki, yarın bir gün iş ortaklığına girdiğimiz zaman biz de bu yüzde 19'luk kesimin içinde yer almayalım.

Bulut tabanlı ihlal maliyetlerine baktığımız zaman, 4.24 milyon dolar olan

kısım, şirketlerin kendi içerisinde, yani ... ... adı verdiğimiz, özel bulut servisi kullanımından kaynaklanan maliyet. 5.02 milyon dolarlık kısmı, genel bulut servisi kullanan firmaların ortalama veri ihlali maliyeti. 3.80 milyon dolarlık kısım ise hibrit bulut servisi kullanan firmaların ortalama veri ihlali maliyeti.

Dikkat çeken istatistiklerden bir tanesi de şu: Fidye (ransomware) saldırıların hepimiz duyduk ve aslında pandemiden bu yana ne gibi problemler yarattığını biliyoruz. Fidye saldırılarının tespiti ve bunlara müdahale, diğer saldırılara nazaran 49 gün daha uzun sürüyor.

Supply chain adı verdiğimiz tedarik zinciri ihlallerinde ise, bu ihlallerin algılanması, tespiti ve müdahale ortalama 26 gün içerisinde gerçekleştiriliyor. Ki daha öncesinde veri ihlaliyle karşılaşan herhangi bir kurum-kuruluştansanız, bahsedilen sürenin ne kadar büyük ve bize zarar verebilecek zaman dilimleri olduğunu biliyorsunuzdur.

Esas bizim için en önemli kısımlardan bir tanesi, ülkelerin ortalama veri ihlali maliyetleri. Buna baktığımızda, ilk sırada Amerika Birleşik Devletleri, sonra Uzak Doğu ülkeleri, Çin vesaire gibi ülkeler, Kanada, İngiltere, Almanya diye devam ediyor. Burada bizi ilgilendiren esas grafik, 17 farklı ülke ve bölge arasında Türkiye'nin 1.19 milyon dolar gibi bir veri ihlali maliyetiyle bu sıralamanın en sonunda, yani en az veri ihlali maliyetiyle karşılaşan ülke olması. Dikkatimizi çeken bir başka nokta da, Türkiye'de veri ihlali maliyetlerinin geçen seneye oranla yüzde 42'lik bir azalışın olması. Dolayısıyla, kurumlarımızın siber güvenlik çözümlerine istihbarat yaklaşımlarını entegre etmeleri sonucu global çapta da bir ilerleme kaydettiğimizi görebiliyoruz.

Bu saldırılar, çeşitli vektörler kullanılarak yapılan saldırılardır. Tespit uzun yıllar boyu asla 200 günün altına düşmüyor. 200 gün çok çok uzun bir zaman dilimi. Tespit ve müdahale kısmında geçen seneye oranla 11 gün gibi bir düşüş var. Eğer biz bu müdahale ve tespit sürecini 200 günün altına

düşürebilirsek, yüzde 26.5 çok daha az bir ihlal maliyetiyle karşılaşacağız demektir.

Son olarak, üzerinde çok fazla düşündüğüm, ama bir türlü en geniş perspektifi ve çerçeveyi yakalayamadığım siber vatan kavramına geleyim.

Siber vatan, ülkemizin akla gelebilecek bütün dijital varlıklarını vatan toprağı olarak görüp, bu varlıkların ürettiği verilerin kendi denetimimiz dışına çıkmaması amacıyla yerli-milli teknolojiyi destekleyen ve global siber uzayda var olan tehditlere karşı proatif bir anlayışla savunma stratejileri geliştiren global siber uzayın milli parçasıdır.

Teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Mustafa arkadaşımıza teşekkür ediyoruz.

Onun bıraktığı yerden devam edecek olan, yine Gazi Cyber Öğrenci Topluluğundan öğrenci arkadaşımız Burak Özlü'yü kürsüye davet ediyorum.

Buyurun.

BURAK ÖZLÜ (Gazi Cyber Öğrenci Topluluğu Başkan Yardımcısı)- Merhabalar. Ben Burak Özlü, Gazi Üniversitesi Bilgisayar Mühendisliği öğrencisiyim. Aynı zamanda özel bir şirkette siber güvenlik görevlisi olarak çalışıyorum.

Dark web üzerinde sıklıkla karşılaştığımız siber tehdit vektörlerinden bahsedeceğim.

Dark web üzerinde sıklıkla illegal ürün satışları, fidye aktiviteleri, panel satışları, erişim satışları, fiziki tehditler, DDOS aktiviteleri ve illegal marketler gibi içeriklerle karşılaşıyoruz.

Dark web'de genellikle insanlar arasında illegal ürün satışları oluyor. Bu illegal ürün satışlarına yönelik bazı örnekler ekledim slaydıma.

Sol altta gördüğünüz gibi, biri silah satıyor, silahın modeli belirtilmiş, kalibresi, kapasitesi belirtilmiş ve fiyatı belirtilmiş. Ancak, burada dikkat etmemiz gereken asıl nokta, elinde bu silahtan 50 adet bulunması. 50 adet silah kimsenin eline tesadüfen geçmeyeceği için, bu satıcının bir terör kolu veya bir suç örgütüne mensup olduğunu düşünebiliriz. Bu tehditler kapsamında emniyet güçlerimiz aktif olarak çalışmakta ve bu platformları takip etmekteler.

Burada da anahtarlık görünümlü bir silah satışı görüyoruz. Bu ürünler Türkiye'deki kritik isimlere düzenlenebilecek saldırılarda kullanılarak ülke gü-

venliğimiz için tehdit oluşturabilir.

Burada da jammer satışı görüyoruz. Jammer satışları ülkemizde yasak. Bu ürünler ancak Türk Silahlı Kuvvetleri, Milli İstihbarat Teşkilatı ve Emniyet güçleri tarafından kullanılabiliyor. Bu ürünleri illegal bulanlar veya emniyet güçlerinden bir şekilde çalarak elde etmiş olabilirler ve bunların satışını yapıyorlar. Yine emniyet güçleri bu konuları da dikkatle takip ediyordur.

Dark web'te illegal ürün satışları arasında uyuşturucu ve kaçak sigara olduğunu da görüyoruz. Bu uyuşturucular ülkemize kaçak yollarla sokularak tehdit aktörleri tarafından satışa çıkartılmakta. Yine bu ürünler kaçak yollarla ülkemize getirildiği için, bu ürünlerden elde edilen gelirlerin nereye gittiğini biz bilmiyoruz, muhtemelen suç örgütleri veya terör örgütleri bu satışlardan nemalanıyorlar diye düşünüyoruz. Kaçak sigara gibi ürünler de dark web'te sıklıkla satılmakta.

Bunun dışında, sahte belge ve doküman satışlarını da dark web platformlarında sıklıkla görüyoruz. Örneğin fiziksel kart basım servisi adıyla bir aktörün yaptığı paylaşımı görüyoruz. Bu tehdit aktörü, vatandaşlık kimlik kartları, ehliyet gibi kimlik kartlarını basmasının yanında, polis, asker, basın kartı ve baro kartları gibi kartlar basmakta ve bu kartların kullanımı ülke güvenliğimiz için bir tehdit oluşturabilir. Tehdit aktörünün iki türde ürün sattığını görüyoruz. Birinci kalite olarak sattığı polikarbon kartlar ve ikinci kalite olarak sattığı PVC kartların fiyatlarını görebiliyoruz.

Bunun dışında dark web'te panel satışlarıyla da sıklıkla karşılaşıyoruz. Motorlu taşıtlar sürü kurslarıyla ilgili bir modül satışı görüyoruz. Bu erişim muhtemelen bir motorlu taşıtlar sürücü kursunda çalışan birinin hesap bilgileri. Bu hesaplar oltalama (fishing) saldırıları veya zararlı yazılımlarla elde edilerek bir şekilde farklı platformlarda satışa çıkartılıyor.

Bunun dışında otel kayıt hizmeti görüyoruz. Bu otel kayıt hizmetini detaylarıyla ekranda da görebiliyorsunuz. Bu panel muhtemelen güvenlik güçlerine ait bir panel. Fiyatların arasındaki farkı görebiliyorsunuz. Muhtemelen daha az bulunan bir panel. Panellerin bulunma sıklığı fiyatlarını etkileyebiliyor.

Bunun dışında, dark web üzerinde erişim satışlarını görüyoruz. Sağ üst tarafta havaalanına ait erişim satışını görüyoruz. Dark web'teki bu havaalanına erişim kullanılarak, havaalanında bir şok oluşturulabilir, bir panik oluşturulabilir. Çünkü acil durum sistemine erişim var.

Bunun dışında, bir yakıt dağıtım şirketine ait bir erişim satışı görüyoruz. Bu erişim satışları fidye gruplarınca satın alınarak, fidye aktiviteleri gerçekleştirilebilir.

Bunun dışında, erişim satışlarının çalışanlar tarafından gerçekleştirilebileceğini de görüyoruz. ... Show adı altında düzenlenen bir etkinlik var Amerika Birleşik Devletleri'nde. Bu etkinliğe katılanların listesinin, database'inin içeride çalışan bir kişi sayesinde erişilerek satışa sunulduğunu görüyoruz.

Geçtiğimiz kurban bayramındaydı sanırım. Türkiye'de bir kurum çalışanının bilgileri sızdırıldı. Bu olayı araştırdığımızda, aslında fidye gruplarının bu kişiye birlikte çalışma teklifinde bulunduğunu, ama bu kişi teklifi kabul etmediği için bilgilerinin sızdırıldığını görüyoruz.

Bunun dışında, veri sızıntılarıyla karşılaşıyoruz. "TEDAŞ hacklendi, binlerce vatandaşın bilgileri hacklendi." Bu başlığı bir haber sitesinden aldık. KVKK tarafından doğrulanmıştı bu veri sızıntısı. Ancak, bu veri sızıntısı KVKK tarafından doğrulanmadan önce benim kontrolümde keşfedilmişti. Gece sanırım 24.00 civarıydı, biz bu erişime dair bilgileri aktörden bir şekilde aldık, onunla iletişime geçerek. Bu şekilde verileri doğruladık. Bunun dışında, aktörün yaptığı paylaşımları sürekli olarak izlediğimiz için, aktörün bu bilgileri nasıl ve hangi yöntemle çektiğini, nereden paylaştığını görüyoruz. İletişimin önünde ISS olduğunu belirtmiş. Bu arada, bu veri sıkıntısını doğruladık, sonra da duruma müdahale edilmesi için bildirmiştik.

Ancak, bazı veri sıkıntıları gerçek olmayabiliyor, sahte oluyor. Sahte veri sızıntıları haberleri görüyoruz. Bilinen bir tehdit aktörü TikTok veri tabanını sızdırdığını iddia etmişti. Ancak, belli bir süre sonra bunun verisinin gerçek olmadığı ortaya çıktı, paylaştığı verilerin başka bir veri sızıntısına ait olduğunu belirledik.

Bunun dışında, dark web üzerinde DDOS aktivitelerini görüyoruz. Burada biz Rus kaynaklı DDOS gruplarını inceledik. Örneğin bu grupların Alman İstihbarat Servisine ait bir web sitesini kullanılamaz hale getirdiğini görüyoruz, servis dışı bıraktığını görüyoruz. Bunun dışında, sağ taraftaki net grubunun düzenlediği Amerikan Hava Yollarına yönelik saldırısını görüyoruz, daha doğrusu saldırı duyurusunu görüyoruz.

Bu DDOS aktivitelerini yapan gruplar arasından bir grup seçip inceledik. Bu grup NATO ülkelerini oldukça tehdit etmekte ve aktif olarak saldırılar düzenlemekte. Bu grubun altında aslında başka DDOS grupları bulunuyor; Rayt, Zarya, Kajuk, Jeki, Rajiva, Renua gibi. Bunun dışında, Sparta gibi gruplar da eklendi bunun altına. Legia grubu bir emir veriyor ve bu emir gruplar arasında paylaşılıyor. Örneğin Jeki Polonya'ya saldırırken, Zarya Almanya'ya saldırabiliyor gibi.

Bu DDOS aktivitelerine örnek olarak bir içeriği göstereyim. Bu DDOS grubu genellikle Rusya dış politikasına yönelik faaliyetler göstermekte. Litvanya, Rusya'nın bir bölgesi olan Kaliningrad'a tren geçişini durdurduktan sonra bu DDOS grubunun Litvanya'nın altyapılarına DDOS saldırıları düzenlediğini görüyoruz. Bu sektörler arasında lojistik sektörleri, ISP'ler, havaalanları, enerji şirketleri gibi şeyler bulunmakta.

Fidye aktivitelerine baktığımızda, karşılaştığımız en aktif grup Floty şu anda. Bu grubun kendine ait ... bulunmakta. Hatta ilk ürünü birkaç ay önce ödemişlerdi. Bunun dışında, bu grup kendine ... 1000 dolar ücret ödüyordu. Şu an bu devam ediyor mu bilmiyorum.

Bu grubun işleyiş faaliyetleri şöyle: Türkiye'ye yönelik bir saldırı düzenlemişler. ... Proje Hizmetleri şirketine. Bu şirketin bu saldırıyı durdurabilmek için yapabileceği üç seçenek var. Sürelerini uzatabilirler. Bu aktörler fidyeyi bulaştırdıktan sonra bir sayaç çalışmaya başlıyor. Bu sayaç tamamlandığında bütün veriler herkese açık olarak paylaşılıyor. Bu süreyi 24 saat uzatmak için 10 bin dolar, bütün verileri satın alıp paylaşılmasını engellemek için 335 bin dolar vermeniz gerekiyor. Grubun yaptıkları işleri sol tarafta görebiliyorsunuz. Büyük bir grup.

Fidye grupları sadece siber anlamda tehdit oluşturmuyorlar, bunun dışında işler de yapıyorlar. Mesela, Mobil ... adlı grubun yaptığı duyuruyu görüyoruz. Bu grup katiller kiralayarak, fidye bulaştırdıkları şirketleri tehdit etmeye başlıyorlar, kendilerine gerekli fidyeyi ödemeyen kişileri öldürecekleri gibi uyarılarda bulunmuşlardı. Daha sonra pek bir şey çıkmadı sanıyorum.

Bunun dışında, dark web'te illegal marketleri sıklıkla görüyoruz. Geçtiğimiz günlerde burada Türkiye'ye ait bir savunma sanayi şirketine ait verileri tespit etmiştik, bunu USOM'a bildirerek önlem almasını sağladık.

Bunun dışında, dark web üzerinde kredi kartı satışları sitelerini görüyoruz. Bu satış platformunda kullanıcılara ait yaklaşık 7 bin tane kredi kartı satışı olduğunu tespit ettik. Bazı kişilerin adı açık olarak belirtiliyor, kredi kartı bilgileri olan kişilerin. Bu kişilerden biriyle anlaşabiliyorlar, bu kişinin olduğunu gördüm. Yaklaşık 28 bin adet topal öğrencisi ve 781 yorumu olduğunu buldum. Ayrıca bu kişinin Twitter hesabını da tespit etmişler. Bu bilgileri tabii ki blurlamak zorunda kaldım.

Sunumum bu kadardı. Dinlediğiniz için teşekkür ederim. (Alkışlar)

OTURUM BAŞKANI- Teşekkür ediyoruz arkadaşlarımıza.

Sayın katılımcılar; oturumumuzun sonuna geldik. Ben plaketleri verdikten sonra, hem kapanış konuşmasını yapmak, hem de varsa soruları almak üzere sözü Şeref hocama bırakacağım. Her şey için hem katılımcılara, hem sizlere, hem emeği geçen herkese teşekkür ediyorum. Oturumumuzu burada kapatıyorum ve panelistlerimize teşekkür belgelerini takdim etmek istiyorum. (Alkışlar)

KAPANIŞ VE DEĞERLENDİRMELER

Prof. Dr. ŞEREF SAĞIROĞLU- Değerli katılımcılar; çalıştayımızda ilk saatten beri siber vatan konusunu farklı yönlerden ele aldık. Endüstriyel açıdan ele aldık, üniversiteler açısından ele aldık, kurum-kuruluşlarımız açısından ele aldık; en son gençlerimizi de dinledik, dark web açısından ele aldık. Bunun elektronik ortamlarda tutulan kayıtlar açısından önemine değindik. Pek çok açısı var. En önemlisi, ontolojik bakış açısını ele aldık. Bunların değerlendirilmesi gerekiyor. Belki sizlerin burada önerileri varsa onları da almak isteriz.

Ben ilk sözü Barış Albayımıza vermek istiyorum, bu alana katkısı yüksek.

Buyurun Albayım, siber vatanla ilgili görüşlerinizi alalım, ondan sonra diğer katılımcılara da söz vereceğim.

Buyurun lütfen.

Alb. BARIŞ ...- Çok teşekkür ederim.

Birçoğunuz belki biliyordur, ama bir karikatürle başlamak isterim. Bir tane fil ve yedi tane görme özürlü kişi, siyah gözlükleriyle, ellerinde bastonlarıyla beraber o fili bir tarafından tutmaya çalışıyorlar ve anlayabildikleri kadarıyla dokundukları şeyin ne olduğuna ilişkin kendi kafalarında bir obje oluşturmaya çalışıyorlar. Bu tür yeni oluşan kavramlarda bu tür davranışları görebiliyoruz. Bunlar sağlıklı ve olağan şeylerdir.

Biz de siber vatanı tanımlarken, endüstrinin kendine ait bir tanımı olabiliyor, akademinin kendine ait bir tanımı olabiliyor, kamunun kendine ait bir tanımı olabiliyor, özel sektörün kendine ait bir tanımı olabiliyor; herkesin siber vatanla ilgili bir görüşü, bir fikri olabiliyor. Bu gayet normal, gayet sağlıklı. Önünde sonunda bunlar bir noktada buluşacaklardır, yani birleşeceklerdir. Benim de kendime göre bir siber vatan tanımım var.

Siber vatana geçmeden evvel öncelikle vatan kavramını ortaya koymamız gerekiyor ki, onun önüne daha sonra siberi ekleyebilelim.

Biz vatan kavramını hep anavatanımız üzerinden tanımlamışız. En doğuda Iğdır, en batıda Gökçeada, en kuzeyde Sinop, en güneyde Hatay olan ve dolayısıyla üzerindeki dağlarıyla, tepeleriyle, gölleriyle, ırmaklarıyla bizim olan, toprağının altındaki mineralleriyle bizim olan ve üzerinde hükmetti-

ğimiz, üzerinde birtakım kanunlar koyduğumuz, üzerinde egemenlik haklarımızı ilan ettiğimiz bir coğrafyayı tanımlarız ve onun üzerine her koyduğumuz bayrağın olduğu yere de vatanın bir parçası deriz ve onu korumak için de elimizden geleni yaparız. İşte bunun için Türk Silahlı Kuvvetleri, İçişleri Bakanlığı, çeşitli kamu kurumları elinden geleni yaparlar. Bunu aynı zamanda biz denize de taşıyoruz. Karanın uzantısı olan karasuları da aynı konsept içinde değerlendirilir diyoruz, oraya giren çıkan tüm gemiler bize haber vermek zorundadır diyoruz, oraya birtakım kurallar koyuyoruz; onun altındaki balık bizimdir diyoruz, oraya girecek gemilere gümrükle ilgili, sağlıkla ilgili birtakım kurallar koyabiliyoruz. Onu da uzatıyoruz, diyoruz ki münhasır ekonomik bölge, altından çıkan gaz benim diyoruz, altındaki doğal kaynaklar benim diyoruz. Tabii, uçakların icat edilmesiyle beraber havayı da biz bunun içine aldık ve dedik ki bilmem kaç irtifaa kadar burası benimdir, içeriye giren tüm uçaklar bana haber vermek zorundadır. Bunun gibi birtakım hükümleri bu vatan kavramı içerisine oturtuyoruz.

Vatan kavramı kendi içerisinde bir iyelik içeriyor, bir sahiplik içeriyor, bir hükmetme içeriyor, egemenlik haklarını onun üzerine tanımlamayı içeriyor.

Şimdi yavaş yavaş artık siberi de biz coğrafya olarak tanımlıyoruz. Diyoruz ki, siberin üzerinde de bir sürü varlık var. Bu siber coğrafya üzerindeki varlıklara yönelik de bir vatan kavramı tanımlama noktasına geldik.

Dolayısıyla, siber coğrafya ne, onu da tanımlamamız gerekiyor.

Biz siber coğrafyayı üç katmanla tanımlıyoruz. Fiziksel katmanda, hepinizin çok iyi anlayabildiği, elimizle dokunabildiğimiz somut varlıklar var. Bilgisayarlar, sunucular, cep telefonları, nesnelerin interneti, aklınıza gelebilecek ne kadar dokunabildiğimiz cihaz varsa, bunlara biz siber vatanın veya siber coğrafyanın fiziksel katmandaki varlıkları diyoruz. Bunun üzerinde bir de dijital katman var. Burası da soyut katman. Ağlar, kullanıcı adları gibi varlıklar. Hiç kimsenin alıp cebine koyamadığı, ama varlığından hiçbir şekilde de şüphe duymadığımız varlıklar oluyor bunlar da. En üst katmanda da algı katmanı var. 2016, 2018 ve 2020'deki Amerika Birleşik Devletleri'ndeki seçimlerde algı katmanındaki siber varlıklara karşı bir saldırı yapıldığına ilişkin birtakım istihbarat raporlarını hepimiz okuduk. O da muhakememiz içerisindeki siber varlıkları içeriyor; düşünce yöntemlerimiz, düşünce kaslarımızın siber coğrafyada olan yansımaları. Kısaca, biz bu siber coğrafyayı fiziksel, dijital ve algı katmanında tanımlayabiliyoruz.

İşte bu global siber coğrafya içerisinde -biraz önce Mustafa'nın yaptığı

tanımla biraz örtüşüyoruz burada; ağzına sağlık- bizim üzerinde hak ilan ettiğimiz, bizim üzerinde egemenlik haklarımızı ilan ettiğimiz ve bizim hükmetmek üzere seçtiğimiz coğrafyaya, fiziksel, dijital ve algı katmanları beraber siber vatan diyoruz.

Burada coğrafyasızlık çok önemli bir şey. Çünkü fiziksel katmandakiler bizim alışık olduğumuz coğrafi tanımların içerisine sığıyor. Burada diyoruz, enlem boylam olarak burada. Ama dijital katman ve algı katmanına geçtikten sonra artık orada bir enlem boylam yok. Orası coğrafyasız bir alan. Dolayısıyla, alışık olduğumuz kaslarımızla buna yönelik birtakım kurallar koymak pek mümkün olmuyor, birazcık değiştirmemiz gerekiyor oradaki yaklaşımımızı. Ki şu an zaten dünyadaki uluslararası hukukun siber alana yansıtılmasına yönelik çabalar ve tereddütler zaten burada kilitleniyor. Burası da gelişecektir önümüzdeki dönemde diye değerlendiriyoruz.

İşte bu bağlamda siber vatanı üç katmanda da görüp, coğrafyasız olduğunu çok iyi bir şekilde anlamamız, idrak etmemiz gerekiyor. Bu örneği her yerde vermeye çalışıyorum. Türkiye Cumhuriyeti vatandaşlarına ait kredi kartı bilgileri veya birtakım bilgiler bir bulut hizmet sağlayıcısı tarafından Amsterdam'da, Kuzey Amerika'da veya Güney Amerika'da olabilir. Ama fiziksel olarak başka bir coğrafyada olması, oraya yapılan saldırının bizimle alakasız olduğu anlamına gelmemektedir. Oraya yapılan saldırının, bizim dijital katmanımızdaki siber vatanımıza yapılan bir saldırı olmasından mütevellit, siber vatana karşı yapılmış bir saldırı olarak değerlendirilmesi gerektiğini düşünüyoruz. Dolayısıyla, siber vatanımıza karşı yapılan saldırılara karşı bizim de cevap verme hakkımızı her zaman elimizde bulundurduğumuzu herkese söyleyebiliyoruz.

Bu bakış açısıyla siber vatanı tanımlamamız ve önümüzdeki dönemde bu bakış açısıyla mevzuatımızı, bu bakış açısıyla kurumlarımızı, bu bakış açısıyla personel kaynağımızı geliştirmeye yönelik kapasite geliştirme faaliyetlerimizi oturtmamız çok daha faydalı olacaktır.

Çok geç oldu, sizi de evlerinizden alıkoymayayım, bu kadar kısa bir şeyle tamamlamış olayım. (Alkışlar)

Prof. Dr. ŞEREF SAĞIROĞLU- Teşekkür ederiz.

Evet, bunun dışında, ben katkı vermek istiyorum diyen kimse var mı?

Buyurun Hüseyin hocam.

Dr. HÜSEYİN BAYAZIT- Albayım, siber vatana ilişkin söylediklerinize çok doğru, tüm o katmanlar iç içe geçiyor. Fakat biraz önce konuşan genç ar-

kadaşımızın yaptığı tanımda önemli bir nokta var. Siber vatana ilişkin bir tanım yaptı genç arkadaşımız ve tanımın içerisinde de çok önemli bir şey söyledi. Amaç, hedef. Tanımımız benzeşiyor ve örtüşüyor. Ortak akıl, ortak duygu, bu çok çok önemli. Şunu anlatmaya çalışıyorum: Ontolojik bakış. Muharebe sahası ontolojik bakıyor. Çok önemli bu tanımlar. Fakat bu tanımın içerisinde çok önemli bir nokta var; amaç hedefi de getiriyor. Şunu söylemek istiyorum: Burada tanımın boyutlarını verip, amaç ve hedeflerini ve egemenlik haklarımız vesaireyi koyup ve bunun üzerine de daha sonra müfredatı koyarız. Tabii, bunun yanına vizyon ve misyonu da koyabiliriz. Ondan sonra da optimizasyon süreciyle ilgili kurumsal yapı vesairesi geliyor.

Prof. Dr. ŞEREF SAĞIROĞLU- Teşekkür ederiz.

Evet, başka söz almak isteyen var mı?

Buyurun.

SALONDAN- Hocam, öncelikle çok teşekkür ederim. Bu çalıştay sayesinde kafamızdaki bazı kavramlar yerli yerine oturdu, savunma açısından baktık. Sadece kayıtlara geçsin diye bir şey söylemek istiyorum.

Siber vatanı tanımladık. İşin içerisine savunmayla beraber bir de uluslararası ilişkilerin siber boyutu giriyor. Bu siber ortamdaki krizler devletlerarası krizlere dönüşecek. Dolayısıyla, uluslararası arenada bu siber krizleri çözebilecek bir siber diplomasinin de artık ülkemizde oturması gerekiyor. İleriki çalışmalarda bunu da gündemimize alırsak iyi olur. Ülkemiz açısından bir siber diplomasi çalışması da olmazsa olmaz gibi duruyor.

Prof. Dr. ŞEREF SAĞIROĞLU- Teşekkürler.

Gençlerimizden söz almak isteyen var mı?

Siber vatan, siber savunma deyince belki daha çok askeri terimlerle tanımlandı; ama siber vatan, sivillerin de, vatandaşların da korunduğu ortamlar veya onların da o ortama katkı vermesi gereken ortamlar. Çünkü sizin siber topraklarınız veya dijital verileriniz dünyanın neresinde varsa, tanıma göre, korumak zorundasınız. Dolayısıyla, dünyanın her yeri sizin sınırınız, her yeri o kısıt içerisinde korumak durumundasınız. Nerede vatandaşlarınız, nerede dijital varlıklarınız varsa, onları korumak zorundasınız.

Tabii ki çok haklısınız, dünyanın her yeri toprağınız haline geliyor. O zaman, uluslararası diplomasiyi de geliştirmek gerekiyor. Bu terim ve terminolojilerin içini onun için doğru doldurmamız gerekiyor; doğru anlamak ve doğru doldurmak gerekiyor. Bugüne kadar düşündüğümüz siber güvenlik

bakış açısını artık değiştirmemiz gerekiyor. Bugünkü toplantının, bu çalıştayın sonuç çıktısı belki bu. Artık yeni bir paradigmayla olaya bakıp, bu değişime-dönüşüme, yeni bakış açısına hepimizin hazır olması gerekiyor. Çünkü bunu kabul ederek başlamamız gerekiyor. Dünya değişiyor, doğru; ama bu değişimde tanımlarımız da değişiyor, bakış açılarımız da değişiyor, savunma stratejilerimiz de değişiyor ve değişmek zorunda. Artık siber ortamda veya dijital ortamlarda biz de bu savunmanın bir parçasıyız. Biz derken, hepimiz. Kurumlar da, vatandaş da, orada verisi olan, bilgisi olan herkes o bütünün bir parçası.

Tanım olarak da baktığımızda, benim en çok sevdiğim tanım ontolojik bakış açısı. Sabah çok güzel ifade etti Hüseyin hocam, o tanımın üzerine daha çok odaklanmamız gerekiyor. Çünkü bu...

Dr. HÜSEYİN BAYAZIT- Hocam, sizin o makaleniz, o çok çok önemli, o 24 sayfalık makaleniz.

Prof. Dr. ŞEREF SAĞIROĞLU- O bir girişti. O birinci kısım. İkinci kısmı fırsat bulup yazamadım. Meslek Odamızda çok yoğun günlerimiz var, Oda faaliyetlerimiz var, Odamıza yeni bir uluslararası bakış açısı getirmeye çalışıyoruz, yeni projelerimiz var, söz verdiğimiz işler var, bunları yapmak zorundayız. Odamızın faaliyetlerinden birisi de bu; yeni bakış açılarını Odaya kazandırmak. Artık sadece bir konuda SMM'lik değil, yüksek gerilim işletme sorumluluğu gibi, topraklama gibi alanlarda değil, başka alanlarda da sorumluluğumuz var. Bunların en başında da siber güvenliğin geldiğini ifade edeyim. Yani bu sorumluluğumuzu, tabii ki bu halkayı genişleterek, hep beraber yeni hedeflere, yeni felsefelere, yeni bakış açılarına doğru götürmemiz, bu paradigma değişikliğini hayatımıza uygulamamız gerekiyor. Bugünkü çalıştayın sonucunda gördüğümüz durum bu.

Ben, bir defa, kişisel olarak, Çalıştay Başkanı olarak büyük keyif aldım. Çok farklı bakış açılarını tek bir ortamda bir arada gördüm. Sizlerin de keyif aldığınızı düşünüyorum. Bunların kayıtları yayınlanacak, tabii ki kişilerden izin almak kaydıyla; orada sakin kafayla tekrar dinleyip, bunları değerlendirip, sonuç bildirgemizde yayınlayacağız.

Katılan, katkı veren herkese çok teşekkür ediyorum. Bu saate kadar buradaydınız. Başkanımız da bekliyor, sponsorlarımıza da dışarıda bir teşekkür belgesi vereceğiz, Başkanımızla beraber. Son olarak hepinizi buraya davet edeyim, bir kapanış fotoğrafı çektirelim, sonra da dışarıda sponsorlarımıza bir teşekkür edelim.


ato
Ankara
Ticaret Odası
SİBER
VATAN ve SAVUNMA
ULUSAL ÇALIŞTAYI


ato
Ankara
Ticaret Odası

SİBER VATAN ve SAVUNMA ULUSAL ÇALIŞTAYI

Çalıştay Düzenleme Komitesi

Halil İbrahim Yılmaz, ATO Başkan Vekili
Prof. Dr. Şeref Sağıroğlu, EMO Ankara Şubesi YK Başkanı / Çalıştay Başkanı
Cevdet Aslan, EMO Ankara Şubesi Başkan Yardımcısı
Hatice Bilge Alğın, EMO Ankara Şubesi YK Yazmanı / Çalıştay Başkan Yardımcısı
Engin Pekyılmaz, EMO Ankara Şubesi Sayman Üyesi
Ertuğrul Kadir Işık, EMO Ankara Şubesi YK Üyesi
Murat Subaşı, EMO Ankara Şubesi YK Üyesi
Tuncay Lamci, EMO Ankara Şubesi YK Üyesi
Ayhan Şahin, EMO Ankara Şubesi YYK Üyesi
Kenan Erpir, EMO Ankara Şubesi YYK Üyesi
Berkan Ateş, EMO Ankara Şubesi YYK Üyesi
Okan Gümüş, EMO Ankara Şubesi YYK Üyesi
Yeşim Sekizelma, EMO Ankara Şubesi YYK Üyesi

Destekleyenler

ACM Gazi, Bilgi Güvenliği Derneği, CIGRE Türkiye,
EMO-Genç Gazi, Elektrik Tesisat Mühendisleri Derneği,
Gazi AI R&D Center, GaziCyber, IEEE Gazi

ankara.emo.org.tr ankara@emo.org.tr emoankara emoankara emoankara emoankarasubesi emoankarasubesi

31 EKİM 2022 • Pazartesi

09.00 - 17.30

ATO MECLİS SALONU
Söğütözü Mahallesi
2176. Cadde No: 1/1
06530 Çankaya/ANKARA

SİBER VATAN ve SAVUNMA ULUSAL ÇALIŞTAYI

DÜZENLEYİCİLER

ELEKTRİK MÜHENDİSLERİ ODASI • TMMOB • 1954
ANKARA ŞUBESİ

ato Ankara Ticaret Odası

SPONSORLAR

DIWW DRIVE

emc²ekare

Labris NETWORKS

ankara.emo.org.tr ankara@emo.org.tr emoankara emoankara emoankara emoankarasubesi emoankarasubesi