Gündem Haber Giriş: 12 Mart 2021 Cuma 10:40 | Son Güncelleme: 12 Mart 2021 Cuma 10:50 | Kaynak: TRT Haber

Yerli ve milli projeler casusluğa karşı nasıl korunuyor?

Son Haberler Tümü

19:08 Giresun'da kuaför ile yolcu taşımacılığında HES zorunluluğu

19:09 'Mebus ve Şair: Mehmet Akif Ersoy' sergisi Milli Şair'in yaşamına ışık tutacak

19:10 Yunanistan'da cruise gemisinde yangın

18:54 Bolu'daki tarihi Kiliseli Tüccar Han hizmete girmeyi bekliyor

18:36 ABD'de can kaybı 530 bin 833'e yükseldi

Sertaç Aksan

Ülkemizin yerli ve milli savunma sanayiinde ortaya koyduğu ürünler ve sahadaki sonuçları tüm dünyanın dikkatini çekiyor. Peki bu sistemler proje aşamasında ya da sonrasında nasıl korunuyor? Uzmanına sorduk...

Karada, denizde, havada … Kimi zaman bir piyadenin omzunda, kimi zaman bir pilotun kaskında, kimi zaman bir bahriyelinin kullandığı radarda… Yerli ve milli savunma sanayiindeatılan adımların yansımalarını giderek daha fazla yerde görmeye başlıyoruz.

Üzerine titrediğimiz yerli ve milli savunma sanayii ürünlerimiz ve sistemlerimiz için en çok merak edilenlerin başında ‘casusluk ya da kopyalanma olaylarına karşı nasıl korunuyor?’ sorusugeliyor… Sadece bu da değil, örneğin Türkiye’nin başka ülkeye sattığı bir platformun akıbeti, teknoloji transferinin sınırları ya da karşı tarafın eline geçen bir S/İHA’dan hangi bilgilerin alınabileceği gibi konular sıkça soruluyor…

Deniz Harp Enstitüsü Öğretim Görevlisi Ayhan Sunar’a hem bu soruları yönelttik, hem de bualanda gelecek döneme dair beklentilerini sorduk.

[Deniz Harp Enstitüsü Öğretim Görevlisi Ayhan Sunar]

Bu işin temelinde ‘insan’ var

Sunar, diğer unsurlara değinmeden önce en başta ‘insan’ faktörünün üzerinde durulmasıgerektiği görüşünde…

Firmaların, para/güç/iktidar bağımlılığı gibi bireysel zafiyetlere karşı uyanık olması ve hatalarıntespiti halinde müsamaha göstermemesi gerektiğine işaret eden Sunar’a göre varlığını sadece ticari menfaatleri ile sınırlı görmeyen bir bakış açısı çok önemli.

İstihbarat ve istihbarata karşı koyma noktasında bilgisi ve vizyonu olan firmalara ihtiyaç olduğunu söyleyen Ayhan Sunar, “Vatanına ve değerlerine bağlı ahlaklı çalışanların bilgili ancak zafiyeti olan çalışanlardan yukarıda tutulması gerekiyor. En bilgili ve tecrübelisi de olsa,doğru davranmayan çalışana tolerans göstermeyecek bir bakış açısı gerekli” diyor.

[Casusluk olaylarının temelinde çoğunlukla 'insan' unsuru yer alıyor.]

Siber dünya ve sosyal alana dikkat

Ayhan Sunar’a insan dışındaki unsurların neler olduğunu soruyoruz… “Siber dünya ve sosyal alan” diyen Sunar, siber dünyanın getirdiği risklere dair bilgi seviyesinin toplum genelinde artması ve yaygınlaşması gerektiğini vurguluyor.

Sosyal alan olarak betimlendiği kısmı biraz daha açan Sunar, bu alanda çalışan kişilerin sadecemesai saatleri içinde değil, mesai saatleri dışında da karşı istihbaratın tehdidi altında olduğunu anlattı. Sunar’a göre sosyal alanda farkındalığımızın yüksek olması, risk olacak işaretleri algılayabilmemiz lazım.

Sanayi güvenliği nasıl sağlanıyor?

Savunma sanayii özelinde ele alındığında Türk firmalar için MSY-317-2(C) Savunma SanayiiGüvenliği Yönergesi’nin ‘zorunlu ve temel rehber’ olduğu bilgisini paylaşan Sunar, “Burada temel olarak kişisel ve fiziki alt yapıya yönelik düzenlemeler belirlenmiş durumda. Ayrıca yazışmalar, belgelerin saklanma usulleri, korumalı/kontrollü sızdırmaz alan özellikleri, siber güvenliğe yönelik temel tedbirler de söz konusu düzenlemelere dahil” dedi.

[Kimi zaman düşen S/İHA'lardaki kritik bilgiler düşman unsurların eline geçmeden silinebiliyor.]

Düşen bir S/İHA'nın tüm bilgileri karşı tarafa geçer mi?

Son dönemlerde özellikle sosyal medyada S/İHA konusunda oldukça farklı yaklaşımlar okumakmümkün… Farklı coğrafyalarda kimi zaman teknik sebeplerle kimi zaman vurularak düşen S/İHA'ların bilgilerinin düşman unsurların eline geçtiği inancı bu paylaşımlardan biri.
Gerçekten de durum böyle mi?

"Tersine mühendislik mümkün olabilir ancak her sistem ve durumda farklılık gösterebilir. Uzun bir süreçtir genellikle... Ayrıca düşman toprağında düşen; büyük hasar görmemiş sistemlerin bileşenleri ve tasarım/üretim teknolojilerinin incelenmesiyle de kabiliyetleri hakkında genel fikiredinilebilir. Ancak bu donanımla sınırlıdır.

Kritik yazılımlar normal şartlar altında sistemler tarafından düşme anında sıfırlanmakta yani düşman eline geçmemektedir. İstihbarat örgütlerinin bir sistem hakkında bilgi edinmek için sistemi ele geçirmekten ziyade, söz konusu hedef ülke içinde barış zamanı faaliyetleriyle bilgiyitransfer etme gayreti içinde olduklarını unutmamalıyız.

Düşen veya ele geçirilen sistemler buzdağının aşikar olan görünen yüzüdür. Örneğin bir ithalatlistesinin, malzeme listesinin barış zamanı hedef ülkede ele geçirilmesi hem çok daha kolay, hem de düşen bir sistem hakkında elde edeceğinizden daha fazla bilgiyi içerebilir."

[Türkiye son yıllarda savunma sanayii ihracatını artırdı. Ukrayna'ya satılan Bayraktar TB-2'ler de bu kalemlerden biri.]

İhracat ve ortak üretim gibi durumlarda süreç nasıl işliyor?

Deniz Harp Enstitüsü Öğretim Görevlisi Ayhan Sunar'a başka ülkelere satılan savunma sanayiiürünlerini ve ortak üretim yapılan kimi projeleri de soruyoruz…

"İhracat ile az, ortak üretimle bir miktar teknolojiyi, bilgiyi dost ülke ile paylaşmış hale gelirsiniz" diyor Sunar… Sonrasında ise ihracat ürünlerinin iki versiyonu olduğunu paylaşıyor…Bunlardan ilki üretici ülkenin kendinize özel versiyonu, diğeri ise kritik kabiliyetleri içermeyen ihracat "export" versiyonu…

Sürecin yazılım boyutunda ise kritik noktanın 'yazılım kaynak kodunun transferi' olduğunun altını çizen Ayhan Sunar, şunları söyledi:

"Satılan bir ürünle kaynak kod transfer edilmez. Genellikle, kaynak kod transferi satış olarak değil, teknoloji transferi olarak adlandırılır. Dolayısıyla satılan bir ürünle teknoloji transfer edilmiş olmaz. İhracat gerekli ve önemlidir. Pek çok düzenleme ile bir tarafta teknoloji korunabilir, diğer tarafta ülkemiz için önemli bir ekonomik girdi sağlanabilir. Bu ürünlerimizin ihracatları da izne tabidir. Kullanıcısı devletler arası olarak taahhüt edilmiş şekilde, devletimizinizin verdiği ülkelere ihracat yapılabilir."

Kurumlar arası bilgi transferi nasıl yapılıyor?

Ülkemizin savunma sanayii alanında hem kamu kurumlarının hem de kamu-özel teşebbüs birlikteliğinin çok önemli olduğunu biliyoruz. Herhangi bir projede silah sistemleri farklı birkurumda, elektronik altyapı farklı bir kurumda, yazılım başka bir kurumda yapılabiliyor…

Peki çok farklı kurumların çalıştığı bir projenin güvenliği nasıl sağlanıyor? Ayhan Sunar bu soruya yanıt verirken öncelikle 'kriptoloji' hususuna dikkat çekiyor ve ülkemizde kriptolojininamiral gemisinin TÜBİTAK olduğuna işaret ediyor.

Kimi farklı firmaların da kriptoloji alanında değer kattıklarını anımsatan Sunar, "Bilgiler korunaklı iletişim hatlarımızdan iletiliyor. Çok kritik bilgiler ise eski ve güvenli usulle; elden kripto kuryeleriyle teslim edilebiliyor. Kriptolojide risk gelişen kuantum teknolojileri ile ilgili. Kuantum teknolojileri, mevcut konvansiyonel kriptojolinin sonunu hazırladı ancak buna karşı daalınan önlemler ve geliştirilen yeni kripto sistemleri var. Ülkemiz kriptoloji alanında TÜBİTAK ve ASELSAN'ın, akademinin ve bu alanda faaliyet gösteren diğer bazı firmalarımızın gayretleriyle iyi bir noktada. Zafiyetler genellikle sistemlerin teknolojisinden değil, sistemleri işletenler yani insan faktörü üzerinden çıkıyor. Bu tüm dünyada böyle" görüşünü paylaşıyor.

[Kimi yerli/milli savunma sanayii projelerinde farklı kurumlar birlikte çalışıyor.]

İzinsiz erişim halinde kendini silecek

Burada temel bir noktayı daha merak ediyoruz ve Türkiye'ye yönelik casusluk faaliyetlerindeson yıllarda savunma sanayiinin öne çıkması konusunu hatırlatıyoruz…

Ayhan Sunar'a göre ekonomik istihbarat, askeri istihbarat gibi ulusal gücün çok önemli bileşeni... Bu alanda bazı düzenlemelerin gözden geçirilebileceğine değinen Sunar, şunlarısöyledi:

"İstihbarata karşı koymak, savunma teknolojilerinde öncelikle iyi bir tasarımla başlar. Donanımveya yazılım, sistemlerin kopyalanmaya veya izinsiz erişime izin vermeyecek şekilde tasarlanması ve geliştirilmesi gereklidir. Bir yazılım sıfırlama 'zeroize' teknikleriyle izinsiz erişim halinde kendini silebilir, bir donanım içine gerektiğinde kendini imha edebilecek imha mekanizmaları konulabilir.

Herhangi bir teknoloji elimize geçtiğinde, ilk sormamız gereken soru bunun güvenlik boyutu olmalıdır. Güvenliği kontrol altına alınmamış teknolojilere çok hızlı sahip olmamalıyız çünkü teknoloji bazen istihbaratın zayıflatılması maksadıyla bazı ülkeler tarafından servis edilebilir."

Etiketler: ASELSAN | Savunma Sanayii | SİHA | Tübitak | Yerli ve Milli Teknolojiler