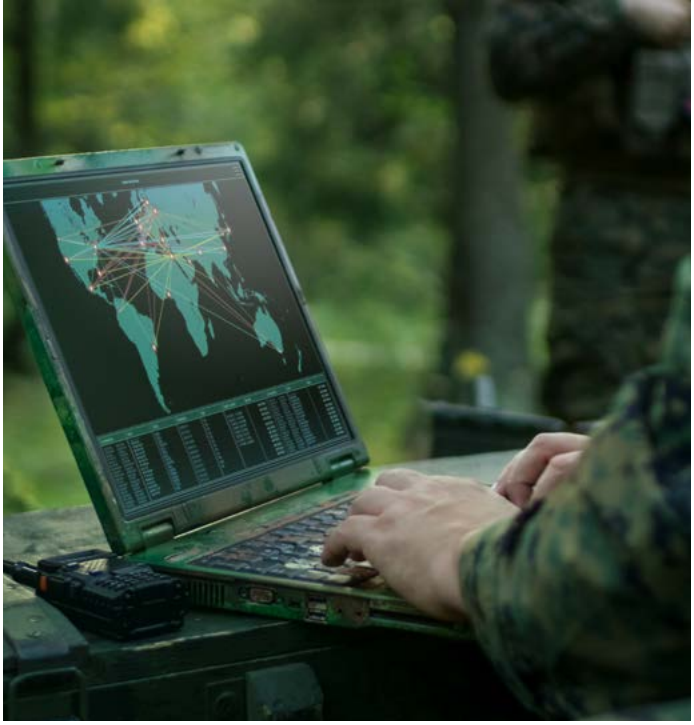
thinktech
STM Teknolojik Düşünce Merkezi



Askeri Operasyonlarda Partnerlerin Veri Paylaşımı

Tarih boyunca askeri operasyonlar genellikle kara, deniz ve hava kuvvetlerinin bilgi ve kaynak paylaşımları ve koordineli çalışmalarıyla yürütülmüştür. Ancak günümüzün gerçeği bu olmayabilir. Özellikle uluslararası operasyonlar söz konusu olduğunda bu son derece eksik bir senaryo gibi görünüyor. Accenture, Nisan 2018 tarihli bir analizle[1], özellikle uluslararası ortak operasyonlar söz konusu olduğunda veri paylaşımının değişen boyutlarına odaklandı. Accenture Kıdemli İnovasyon Yöneticisi Dr. Valtteri Vuorisalo ve Accenture Müdürü Yacine Zaitri'nin kaleme aldıkları bu analizden değerlendirmeler şöyle:

Veri paylaşımı askeri operasyonların destekçisi değil, geleceği konumundadır. Özellikle çok uluslu operasyonları gerçekleştirmenin ve yürütmenin olmazsa olmaz parçasıdır. Ancak harekâtlara hız ve çeviklik katacak verinin paylaşımı kadar nasıl korunduğu da önemli bir unsur olarak karşımıza çıkmaktadır.

Benzer fikir ve ortak çıkarlara sahip devletler müşterek bir hedefe ulaşmak için birlikte çalışmak durumundalar. Yeni dünya düzeninde bu tür operasyonlar çok daha sıklıkla yaşanıyor. Ancak çok uluslu operasyonlara geçiş düşünüldüğü kadar kolay bir hadise değil.

Tek bir ülkenin farklı birimleri arasında bile oldukça zorlayıcı bir unsur olan veri paylaşımı, çok uluslu operasyonların karmaşıklığı söz konusu olduğunda bilgi yönetimi ve paylaşımı alanlarında çok daha karışık bir hal alıyor; farklı diller, farklı coğrafi bölgeler/mimari sistemler, farklı veri standartları, farklı güvenlik sınıflandırmaları gibi zorlayıcı birçok unsur ortaya çıkıyor. Ayrıca merkezi bilgi yönetiminin merkezi neresi olacak, statik mi dinamik mi yürüyecek?

Dikey Paylaşımdan Yatay Paylaşıma Geçiş

Bugünün askeri veri paylaşımı ast-üst boyutunda aktarılıyor; yani hiyerarşik, dikey. Veri ile kastedilen; çok geniş kapsamlı bir bilgi parçacığı, bir kuvvet birliği hakkındaki konum bilgisi olabileceği gibi bir platforma dair tasarım şeması da olabilir. Yani verinin içeriği ve ilgilendirdiği birimler birbirinden çok farklı alanları işaret edebilir.

Ordu unsurları arasında dikeyde veri paylaşımı hâlâ bir ihtiyaç. Bununla birlikte ortak tatbikatlar, ortak askeri operasyonlar gibi devletlerin birlikte organize ettikleri faaliyetlerde ise yeni bir ihtiyaç olarak yatay veri paylaşımın da önemi hayli artmış durumda. Zira çok uluslu operasyonlarda veri,

1 https://www.accenture.com/t20180423T074249Z__w__/us-en/_acnmedia/PDF-76/Accenture-multi-level-security-vuorisalo.pdf

farklı devletlerin, partnerlerin askeri güçleri arasında, yani yatay şekilde paylaşılmak durumunda. Küresel bir yönetim danışmanlığı ve teknoloji şirketi olan Accenture, birkaç yıl önce ABD ve müttefikleri için birden fazla kaynaktan gelen veriyi toplayan bir istihbarat ve izleme sistemi geliştirdi. JCDX (Joint Cross Domain Exchange -Ortak Alanda Çapraz Sorgulama) isimli bu sistem kapsamlı bir yaklaşım mantığı üzerine kurulmuş, farklı kaynaklarla uyumlu, kapsamlı ve hemen hemen gerçek zamanlı bilgiyi müttefikler tarafından paylaşılır kılıyordu.

Bu veri merkezli ve yenilikçi sistem çok seviyeli güvenlikle, yani her bir veri nesnesinin tek tek güvenceye alındığı ve ilgili birimler tarafından güvenli ve sorumlu biçimde paylaşıldığı modelle birleştirilmesi halinde çok daha rafine bir veri koruma ve paylaşım sistemi ortaya çıkabilir.

Çok Düzeyli Güvenliğin Üç Ayağı
Partner ülkelerin operasyonel işbirliği sürecinde inşa etmesi gereken çok düzeyli güvenlik için üç önemli ihtiyaç söz konusudur:

Yataylık İhtiyacı: Verilerin dikeyden yataya doğru yeniden oryantasyonu, askeri hedeflere ulaşmak için kritik öneme sahip. Bu tür bir veri akışı ortak yönetim hızını artıracak, karar verme ve harekât planlama alanlarında çok daha doğru karar verilmesine vesile olacak. Sadece bu türden veri akışları, koalisyonun hızlı ve yüksek kaliteli karar verebilmeleri için gerekli durumsal farkındalık düzeyini oluşturabilir.

Çeviklik İhtiyacı: Terör örgütleri ve paramiliter örgütler, birçok kanal kullanarak, bildiğimiz internetten farklı ve karanlık işlerin döndüğü derin internet ortamı olarak tanımlanan "Dark net"e kadar ulaşıp stratejik öneme sahip bilgileri paylaşabiliyor. Bu tür illegal örgütleri kısıtlayan hukuki bir sınır da yok. Koalisyon ortakları arasındaki anlık ve yatay veri paylaşımı, silahlı kuvvetlerin ortaya çıkan tehditlere ivedilikle cevap verebilmesi ve illegal örgütlere karşı koyabilmesi için tek çıkar yol olarak öne çıkıyor.

Güvenli Yönteme Duyulan İhtiyaç: Silahlı kuvvetler koalisyon ortaklarıyla hem dahili hem de harici birçok veri paylaşmak durumunda. Bu verilerin gerçek zamanlı olarak farklı güvenlik seviyelerinde ve farklı ağ katmanlarında kullanılabilir olması gerekiyor.

Birlikte çalışabilirlik ve operasyonel etkinliği artırmayı amaçlayan NATO'nun Birleşik Kuvvetler Ağ Girişimi (FMN), müttefik kuvvetlerin çok uluslu operasyonlarda birlikte çalışılabilirlik seviyesini artırmayı hedefleyen Birleşik Kuvvetler İnisiyatifi'nin (CFI -The Connected Forces Initiative) bir parçası olarak bu yönde olumlu ilerlemeler sağlıyor[2].

Bugün Atılabilecek Adımlar
Veri odaklı çok seviyeli güvenlik gibi 360 derecelik bir sisteme geçişin tek günde gerçekleşemeyeceği muhakkak. Bu geçiş birkaç yıl alabilir. Bu süreçte, savunma güçlerinin atması gereken ilk dört adım şu şekilde sıralanabilir:

- Mevcut teknolojilerin dikeyden yataya veri transferine geçme evresindeki etkilerini değerlendirmek.
- Öncelikli operasyonel ihtiyaçların bir haritasını çıkarıp bunu ivedilikle ele almak.
- Değişimden kaynaklanacak durumların gerçekçi bir raporunu oluşturmak ve değişimin ölçek ve kapsamını doğru belirlemek.
- Standartlara uymak adına, çok seviyeli güvenlik unsurları etrafında koalisyon ortakları, sanayi, ticari ve akademik sektörlerle aktif bir işbirliği sağlamak.

2 https://www.nato.int/cps/ic/natohq/topics_98527.htm

Şimdi Değilse Ne Zaman?
İçinde bulunduğumuz dijital çağ, savunma güçlerinin veri koruma tarzını ve veri paylaşım yaklaşımını gözden geçirip değiştirmemeleri halinde operasyonel başarısızlıklara da davetiye çıkarıyor. En basit tabirle çok seviyeli bir güvenlik paylaşımı artık askeri güçlerin uygulamaya başlaması gereken kaçınılmaz bir yaklaşım. Bu önemli bir ihtiyaç; bugün zamanın ruhunu yakalamış devletler benzeri veri paylaşımı sistemlerini kamu sektörlerinde kullanmaya çoktan başlamış durumda.

Savunma sanayii söz konusu olduğunda veri odaklı çok seviyeli güvenlik uygulaması bir seçenek değil adeta zorunluluk. Aksi takdirde özellikle çok uluslu operasyonların gereksiz risklere atılacağı muhakkak. 2020'li yıllarda kesintisiz ve çok uluslu veri paylaşımı, silahlı kuvvetler için gündelik bir gerçeklik olacak.