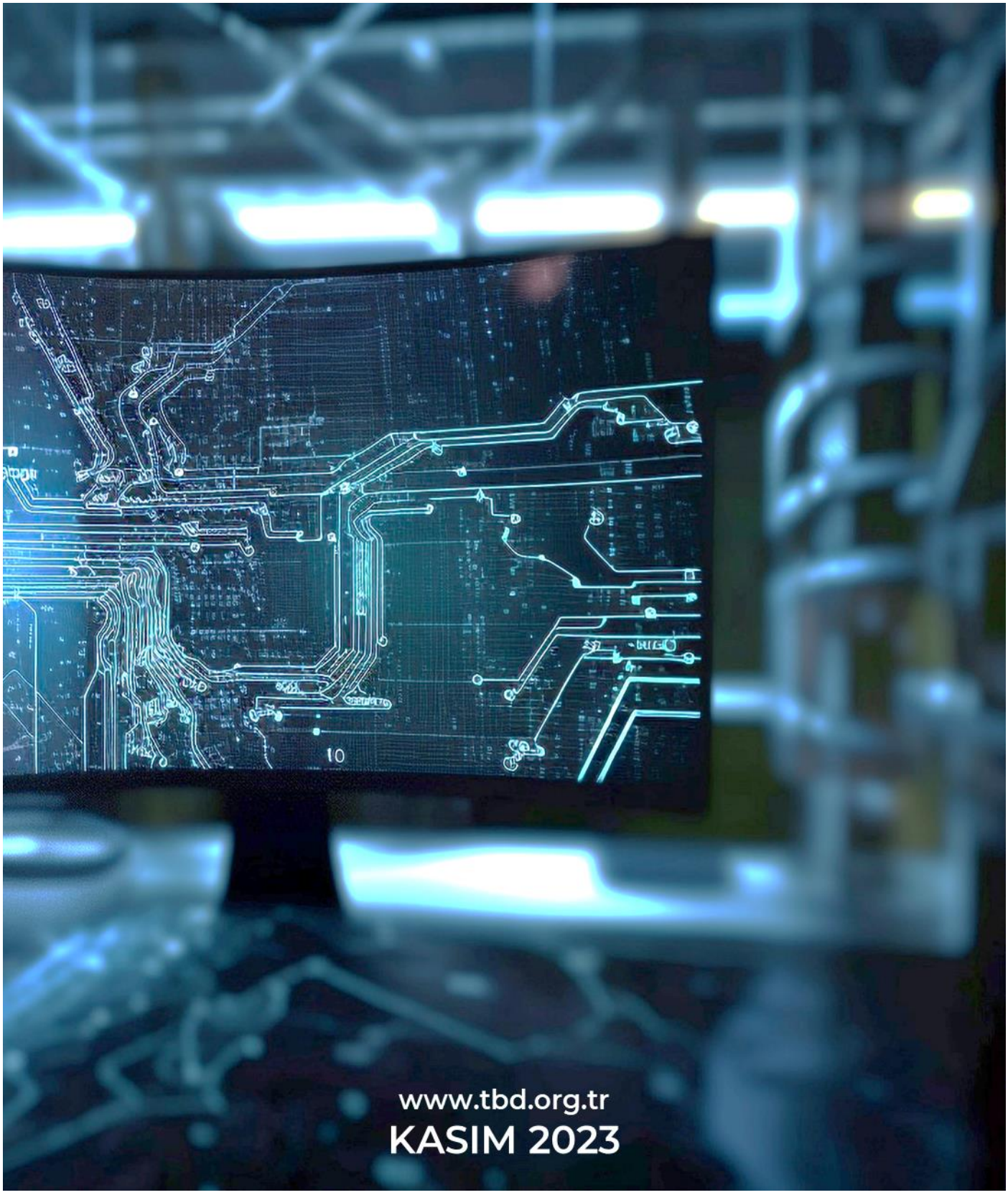
ACİL DURUMLARDA BİLGİ YÖNETİMİ

ANAYURT GÜVENLİĞİNDE BİLGİ YÖNETİMİ VE ACİL DURUMLAR ÖZELİNDE DEĞERLENDİRME



ACİL DURUMLARDA BİLGİ YÖNETİMİ

ANAYURT GÜVENLİĞİ BİLEŞENLERİNE İLİŞKİN BİLGİNİN TÜRLERİ, YÖNETİMİ VE ACİL DURUMLAR ÖZELİNDE DEĞERLENDİRME[1]

ÇALIŞMA GRUBU RAPORU[2] 1. SÜRÜM (Ekim 2023)

Çalışma Grubu Başkanı: Özden ÖZBEN
Çalışma Grubu Üyeleri: Ali SEYHAN
Bülent BORAN
Emre TAŞGIN
Ersin Tufan YALVAÇ
Mete ÇAĞAN

İçindekiler **Sayfa**

[1] Raporun teorik yaklaşımı Özden ÖZBEN'in 2023 tarihli "Anayurt Güvenliğinin Sert Bileşeni Olarak Sınır Güvenliği ve Entegre Sınır Yönetimi" adlı doktora tezinden türetilmiş, diğer alan uzmanlarının katkıları ile sektörlere yönelik unsurlar geliştirilmiş ve çalıştay ile nihai hale getirilmiştir.

[2] Raporun tamamı, TBD tarafından oluşturulmuş olan çalışma grubunun ya da çalıştay üyelerinin kişisel değerlendirmeleri ve bilgilendirme çabaları sayesinde geliştirilmiştir. Raporun içerisindeki herhangi bir kısım, cümle, değinme, değerlendirme, bilgilendirme vb., çalışma grubu başkanının, çalışma grubu üyelerinin ve çalıştay katılımcılarının çalışmış ya da çalışmakta oldukları kurum ya da kuruluşları bağlamamaktadır.

Giriş

Dünyadaki son gelişmeler, tehdit algılarının ve risk unsurlarının çeşitliliğindeki artış, toplumsal ve bireysel kaygılarda durdurulamayan yükseliş, anayurt güvenliğinin ulusal ve uluslararası doğası gibi etmenler, güvenlik kavramının her boyutta ve her kapsamda yeniden ele alınmasını gerektirebilmektedir. Bu yeniden analiz çalışmaları çoğunlukla kurumlarımızın olağan görevleri ve sorumlulukları dâhilinde hali hazırda zaten yapılmaktadır ancak güvenlikleştirerek yapılan analiz çalışmalarına yeni bir bakış getirmek ya da analizlere katkı vermeye çalışmak, kendini sorumlu hisseden her sivil toplum kuruluşunun da görevidir. Bu kapsamda Türkiye Bilişim Derneği'nin konuya ulusal güvenlik temelinde bilgi edinim ve işlem boyutu ile baktığı bu rapor kaleme alınmıştır. Ulusal güvenlik için önemli olduğu değerlendirilen bilgi türleri, bilginin edinim ve işlenmesine yönelik yaklaşımları da içerecek şekilde ele alınmaya çalışılmış, kurumlarımızın bu kapsamdaki çalışmalarına ve yeni nesil projelerine yol gösterebilmek için bir başka bakış açısı geliştirmek hedeflenmiştir.

Amaç

Raporun çıkış hipotezi, ulusal güvenlik için kritik önemde olduğu değerlendirilen bilgi türlerinin çeşitliliğini yorumlama ve kurumlararası birlikte çalışabilme esasları doğrultusunda bu çeşitliliğe daha odaklı yaklaşabilme arayışlarıdır. Doğal olarak kurumlarımız bu kapsamda gereken her türlü önlemi almakta, ilgili ve gerekli projeleri geliştirmekte ve yetkili kurumlar ile etkin iletişim sağlamaktadır. Ancak giriş kısmında vurgulandığı üzere kapsama dair sunulabilecek yeni birşeyler olup olmadığının analizi dahi bu rapor için bir çeşit sonuç niteliğinde olacaktır. Çünkü güvenlik için arayış, tehdit var olduğu sürece devam edecektir, toplumsal olarak buna hazır bulunuşluk durumu ise sürekli ve sürdürülebilir şekilde analizler ile daha güçlenecektir. Rapor kapsamında ulusal güvenlik için bilginin önemi, niteliği, çeşitleri hakkında bilgi verilerek, bilgi edinim ve işleme temelinde ve deneme niteliğinde bir grup proje önerisi de yapılacaktır. (*Bu bağlamda kavramlar ve proje önerileri, düzenlenecek olan çalıştayda da geniş kapsamlı olarak ele alınacak ve raporun nihai hali verilecektir.*)

Kavramlar ve Tanımlar

Ulusal güvenliğe ve ulusal güvenliğin her bir bileşenine yönelik değerlendirmeler yapılırken, muhtelif unsurları muhtelif gerekçeler ile derinlemesine analiz edebilmek mümkün olabilmektedir. Ancak geniş boyutlu ve her birinin birbirleri ile etkileşiminin analizleri çoğu zaman yapılmamakta ya da çoklu bir değerlendirme yerine yine tek bir unsura bir diğerinin etkisi oranında analizler yapılmaktadır. Anayurt güvenliğinin her bir bileşeni farklı ağırlıklarda etkileyicilere sahiptir ve anayurt güvenliği genel başlığı altında bunların bir bütün halinde işlenmesi ve değerlendirilmesi ile önlem alma ya da müdahale çabaları değer kazanır. Örneğin, ekonomi güvenliğine yönelik analizler sanayi güvenliğine, ticaret güvenliğine ve enerji güvenliğine de değinebilmektedir.

Ancak örneğin ekonomi güvenliğinin etkileyicileri arasında en az bunlar kadar kritik gıda güvenliği, tarım güvenliği, sosyal güvenlik, kritik altyapı güvenliği, yeraltı ve üstü kaynakları güvenliği vb. unsurlar da yer almaktadır. Bu bileşenlerin, bütüncül bir bakış altında birbirleri ile bilgi temelinde olası etkileşimlerinin yeniden tanımlanmasının, yeni nesil güvenlik analizlerine temel oluşturabileceği değerlendirilmektedir. İlgili tüm paydaşlar tarafından bilgi çeşitliliğinin tüm olası alternatiflerinin farkında olunduğunda ve bu bilgilerin kurumlararası operasyonlara dâhil edilebilmesi için yeni nesil bütünsel projeler geliştirilmesi halinde, tehdidin ve riskin karmaşıklaşan doğasına karşı daha proaktif ulusal bir duruşun sergilenebileceği yorumlanmaktadır. Özetle çok boyutlu ve çok bileşenli (bütüncül) bir bakış açısı kazanabilmek, anayurt güvenliğinin etkili ve ilgili her bir alt bilgi unsurunun da hesaba katılması sayesinde nispeten daha geniş ölçekli, daha yoğun ve etkin tedbirlerin alınmasını sağlayabilecektir.

Bu bakış, ilgili olduğu değerlendiirlebilecek her kurum için gerekli görülmeyebilir ya da zaten bu kapsamda her türlü önlemin alındığı ve gerekli olabilecek altyapının tesis edildiği değerlendirilebilir. Rapor eğer bu yorumun üretilebilmesine dahi katkı sağlayabilecek ve "bu kapsamda kurumumun hazır ve yetkin olduğunu düşünüyorum" sonucunu üretecek ise aslında zaten görevini de yerine getirmiş olacaktır. Güvenlik ilişkili bilgi edinim ve işlem temelinde kurumsal proaktiviteye katkı sağlamak için organizasyonel farkındalığın sağlanabilmesi de bu kapsamda yeterince önemli bir sonuçtur.

Anayurt Güvenliği çok temel bir tanımlamayla: "Varlığını, güvenliğini, yapısını, sağlığını, huzurunu, kaynaklarını, kültürel ve sosyal yapısını vb. herhangi bir yöntem ile olumsuz etkileyebilecek tehdit ve tehlikelere karşı anayurdun (devletin tüm birimlerinin, vatanın, ulusun, her kurumun ve bireyin) kendini koruma ve olası hasarları minimize etme çabasıdır".[3] Bir başka ifade ile "Anayurt Güvenliği" kavramı, ortaya çıkma ihtimali taşıyan her tür tehlikelere ve tehditlere karşı anayurdun dirençli kılınması ve güvenli kalmasının sağlanması için dâhili (ulusal) ya da harici (uluslararası) eksenlerde gösterilen tüm çabalar olarak özetlenebilir.

Risk, tehdit ya da tehlike kavramları genellikle birbiri yerine kullanılabilmektedir ancak doküman içerisinde, aşağıdaki tanımlamalara dayanarak kullanılmıştır:

Tehlike, ilgili kapsamda değerlendirme yapılan unsura herhangi bir şekilde zarar verme potansiyeli taşıyan, risk oluşturabilecek ya da tehdide dönüşebilecek bir durumu ifade eder. Tehlike, henüz risk taşımamaktadır ya da tehdit içermemektedir ancak tehlikeyi içeren durum ile etkileşim içerisinde olmak risk ve tehdit oluşturabilmektedir. Bu bağlamda tehlike, etkileşim içerisinde olunmadığında risk üretmeyen ya da tehdit oluşturmayan ancak bu potansiyelleri taşıyan durum olarak özetlenebilir.

Tehdit ve risk birbirine yakın görünse de farklı anlamlara sahiptir. Temelde her iki kavram da tehlike ile tetiklenir. Temel farklılık, tehdidin somut verilere, riskin ise senaryo veya soyut kurgulamalara dayanmasıdır.[4] Tehdit, tehlikenin somutlaşmış ve hissedilen bir sonucudur. Bir durumun ya da nesnenin tehdit içerdiği yorumlanıyorsa, o durum ya da nesne hakkında tahmin edilebilir seviyede bilgi ve hazırlık vardır denilebilir.[5] Tehdit tanımı yapılırken, özellikle dışarıda yer alan tehlikelerin içerdiği potansiyel etki ve sonuçların bilinmesi, öngörülmesi ve yönetilmesi için içeride hazır bulunulması durumu önem taşır.[6] Kapsam dâhilinde insan ya da devlet için değerli olan varlıklar hakkında korku ve endişe oluşturma çabası tehdidin özelliklerindendir ve uygulamaya geçmekten daha güçlü bir doğası vardır.[7] Tehdit, bir devletin ulusal menfaatlerinin, yurt içi veya dışından bir grubun ya da

[3] Özden Özben, "Anayurt Güvenliğinin Bir Sert Bileşeni Olarak Sınır Güvenliği ve Entegre Sınır Yönetimi", M5 Ulusal Güvenlik, Savunma ve Strateji Dergisi, s 20, Sayı 340 Kasım 2019.
[4] M. Salih Elmas, "Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik", USAK Yayınları, Ankara, 2013, s 74.
[5] Elmas, Age, s 74.
[6] Elmas, Age, s 75.
[7] Ahmet Küçükşahin, "Güvenlik Bağlamında Risk ve Tehdit Kavramları Arasındaki Farklar Nelerdir ve Nasıl Belirlenmelidir?", s 18, Erişim tarihi 17 Kasım 2022: https://gsd.msu.edu.tr/Content/sayilar/dokuman/GSD_4/GSD_4_Art_1_122006.pdf

devletin ya da devletler grubunun niyet, faaliyet ve girişimlerinin doğrudan hedefi olması durumudur.[8]

Bilinmeyen sulardaki olası tehlikeleri tanımlayan Latince "Risco" terimi farklı disiplinlerde farklı tanımlara sahip olabilmektedir ancak sosyal bilimlerde tehlike içeren bir durumun ya da olayın kesin olmayan alternatif, istenmeyen ve negatif sonuçları olarak özetlenebilir.[9] Bu tanımda kritik vurgu, değer yüklenen unsurların gerçekleştirilen eylemler sonucu negatif etkilenme olasılığı üzerine yapılmıştır. İnsanın potansiyeli ve bu potansiyelin gerçekleştirilmesi ile ilgili bir kavram olarak yorumlanan riskin varlığından, meydana gelmese dahi sanki olmuş gibi kararlar alınmaya başlandığında bahsedilecektir.[10] Risk açısından düşünüldüğünde bugünü, geleceğin taşıdığı potansiyel üzerinden değerlendirmek gerekir.[11] Risk, henüz gerçekleşmeden önce nasıl bir politika izlenerek önlenmesi gerektiğinin belirlenmeye çalışıldığı bir senaryodur.[12] Belirli bir zaman aralığında belirli bir hedefe ulaşamama ve dolayısıyla zarara uğrama olasılığı olarak tanımlanan riskin en belirgin özellikleri; 'tam ve net olarak bilinememesi, zamanla değişkenlik göstermesi, olumsuz sonuçlar doğurma olasılığına sahip olması ve yönetilebilir olması' seklinde sıralanabilmektedir.[13] Ancak nelerin nasıl olabileceğine yönelik geliştirilen senaryolar, bu senaryoların sınıflandırılması, ağırlıklandırılması ve her birine yönelik tedbir ve eylem adımları risk yönetimini oluşturur. Risk senaryolarının niteliği ve dolayısıyla bu senaryolara dayalı olarak alınan tedbirlerin başarıya ulaşımı, olası senaryoları ve çözümleri geliştiren uzmanın tecrübelerine oldukça bağlıdır[14].

Neyin risk ya da tehdit olduğu, bu analizi yapanın yetenekleri tarafından saptanır. Yönetebilme gücü varsa risk, müdahale gerektirdiği yorumlandığında tehdit sınıfında algılanacaktır. Risk yönetilemediğinde tehdit durumuna geçecektir.[15] Asimetrik tehdit ise, hazırlıksız bir anda ortaya çıkardığı ani durum sebebi ile ekonomik, sosyal, siyasal yapılara

[8] Nihat Akçay, "21. Yüzyılda Türkiye'nin Tehdit Algılamaları ve Güvenlik Açılımları", Doktora Tezi, Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, 2008, Bursa, s 17.
[9] Elmas, Age, s 76.
[10] Elmas, Age, s 77.
[11] Rasmussen, M. V., "The Risk Society at War", Cambridge University Press 2006, Cambridge, s 3.
[12] Rasmussen, Age, s 4.
[13] Ahmet Küçükşahin, İskender Cahit Şafak, Çağdaş Dedeoğlu, "Güvenlik Bağlamında Risk ve Risk Yönetimi", Güvenlik Stratejileri Dergisi, Yıl: 2009 Cilt: 5 Sayı: 10, s 12.
[14] Özden Özben, "Ensuring Turkey's Border Security and Defense Industry: Current Evaluations", PERCEPTIONS: Journal of International Affairs, 26 (2), s 277-298, 2022.
[15] Küçükşahin, Age, s 19.

zarar veren tehdit algılamasıdır.[16] Her ne kadar uluslararası ilişkiler temelinde asimetrik tehdit ulusların ve devletlerin bu kapsamda birbirine zarar verme durumu gibi tarif edilse de örneğin doğa ve insan arasındaki etkileşim de zaman zaman karşılıklı olarak asimetrik nitelik taşıyabilir ve bu bağlamda anayurt güvenliği ekseninde ele alınabilir.

Ulusal Güvenlik İçin Bilgi

Çok kısa olarak "Anayurt Güvenliği", değerlerine zarar verebilecek unsurlara karşı dirençli olmak ve bu direnci korumak olarak tekrar özetleyebiliriz. Bu tanım biraz daha açıldığında şu detaya ulaşılabilir: Anayurdun, devletin, sistemin, halkların, ırkın, dilin, inancın, törenin, toprağın, gıdanın, ekonominin, demografinin, kültürün, duruşun, kalışın, bakışın vb., varlığını, yapısını, huzurunu, kaynaklarını, sağlığını, içeriğini, direncini, özünü, şeklini, niceliğini, niteliğini vb., değiştirebilecek, bozabilecek, olumsuz etkileyebilecek, zayıflatacak, sarsacak, tedirgin edecek vb., her tür risk, tehdit ve tehlike türü için devletin, toplumun, bireylerin, varlıkların birbirlerini ve kendilerini koruma, muhtemel negatif sonuçlara karşı dirençli olabilme ve bu sonuçları yönetebilme açısından dirençli, hafifletebilme açısından dirayetli kalabilme çabasıdır. Fark edilebileceği üzere bu detaylı tanımda, rapor kapsamında kaldığı değerlendirilen birçok bilgi unsuru bulunur:

- Ulusal değerlere yönelik bilginin çeşitliliği,
- Bu değerlere ve korunması gereken özelliklerine yönelik bilgi çeşitliliği,
- Tehlikeye, tehdide, riske ilişkin bilginin çeşitliliği,
- Korumaya, korunmaya, azaltmaya, önlemeye, yönetebilmeye yönelik yetkinliklerin bilgi çeşitliliği
- Dirayetli kalabilme, dirençli olabilme ve sürdürülebilir güvenlik sağlama gibi kavramlar açısından bilgi çeşitliliği ve
- Güvenliğin artık daha da karmaşıklaşan doğası gereği güvenliği ulusal boyutta bütüncül yorumlama ve yönetmeye yönelik bilginin çeşitliliği.

[16] Ahmet Küçükşahin, Tamer Akkan, "Değişen Güvenlik Algılamaları Işığında Tehdit ve Asimetrik Tehdit", s 50, Erişim tarihi 17 Kasım 2022: https://dergipark.org.tr/tr/download/article-file/84559

Dolayısıyla bu bilgi çeşitliliğinin her bir kombinasyonu (raporun önerdiği yeni nesil güvenlik analizleri bakışı gereği) farklı niteliklerde hazır bulunuş ve çözüm alternatiflerini de içerebilecektir. Bu genel bakış, raporun ana yaklaşımını da şekillendirmektedir.

Anayurt Güvenliği Bileşenleri[17]

Dirençli ve dirayetli olabilmek ve kalabilmek, devletin, toplumun, bireylerin ve varlıkların, riskin, tehdidin ve tehlikenin her türüne karşı hazır bulunabilme ve en uygun zamanda tek bir bütün gibi etkin ve verimli davranabilme aklının ulusal boyutta icra edilebildiği bir yapıyı ifade etmeye çalışır. Aşağıda anayurt güvenliği kavramı bileşenlerine ayrılmış ve bu bileşenlerin içerikleri verilmiştir.[18] Tehdidin ve gösterilecek tepkinin türüne dayanarak iki farklı kapsamda bileşenlerine ayırma yapılabilir:

- Sert Bileşenler ve
- Yumuşak Bileşenler.

Anayurt güvenliğinin çerçevesinin tanımlanması adına kategorize edildiği çalışmalar da bulunmaktadır. Yılmaz, tanımı yaparken tüm toplumun etkinliği olduğu, çok yönlü koordinasyon gerektirdiği, proaktif ve reaktif olduğu, bilimsel temele dayandığı, yeni bir organizasyon ifade ettiği, yaşam kalitesini güvence ettiği, insan kökenli olana ek olarak doğal kaynaklı olanı da dikkate aldığı ve ülke sınırları içerisinde yürütüldüğünü vurgular.[19] Aşağıda verilen kategorizasyonda her bir bileşen için bu yorumlama ayrı ayrı ele alınabilecek ve gerektiğinde birbirinden ayrıştırılabilecektir. Örneğin sınır güvenliğinde proaktivite, sadece ülke sınırları içerisinde yürütülebilecek bir aktivite niteliğinde olamayabilecektir. Ya da siyasi ve politik güvenliğin uluslararası politikanın dinamiğinden de etkilenebilmesi söz konusudur. Bu bakış altında güvenliğin çerçevesinin, aşağıdaki maddelerin her biri için ayrı ayrı tanımlanabileceği değerlendirilmektedir.

[17] Özden ÖZBEN, "Anayurt Güvenliğinin Sert Bileşeni Olarak Sınır Güvenliği ve Entegre Sınır Yönetimi" Doktora Tezi, Polis Akademisi, Mayıs 2023, Ankara.
[18] Özben, Perception, s 279.
[19] Sefer Yılmaz, "Defining Homeland Security And Its Underlying Concepts", Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi, Cilt 22, Sayı 1, 2013, s 89.

Anayurt Güvenliği Sert Bileşenleri

Tehdidin, doğrudan devlete, vatana, ulusa, ayrıca fiziksel, sosyal, kültürel vb. varlıklara ve değerlere ani bir şekilde zarar verme ihtimali taşıması ya da gösterilecek tepkinin veya alınacak tedbirin doğrudan sert kuvvet kullanımı gerektirmesi durumudur.[20] Örneğin:

a. Askeri Güvenlik,

Tehdidin tamamen askeri nitelikte olduğu, verilecek tepkinin tamamen askeri özellikler taşıması durumudur. Birbirlerinin askeri kabiliyetlerinin karşılıklı olarak algılanması durumuna ve hali hazırda sahip olunan askeri yeteneklerin seviyesine dayanan iki aşamalı güvenlikleştirme unsuru olarak yorumlanabilecek bir tehdit seviyesi içerir.[21] Devletlerin askeri güçlerini geliştirmeleri ve olası tehditlere karşı öncelikle kendi yeteneklerine güvenmeleri gerektiği düşüncesi[22], askeri güvenlik tanımının güvenlikleştirme ve tedbir odaklı temel yaklaşımıdır.

Bu kapsamda alınacak tedbir doğal olarak askeri niteliktedir, askeri tehdit sahibi olan güçlere karşı kendisini savunma eylemidir ve silahlı kuvvetler tarafından yürütülür.[23] Terörizmin muhtelif türlerine karşı gerekli tedbirlerin alınması ve uygulanması da çoğunlukla askeri güvenlik başlığı altında ele alınır.

b. Siyasi ve Politik Güvenlik,

Bir ülkedeki mevcut siyasal düzenin, iktidarın, siyasi işleyişin, ulusal politika geliştirme ve uygulama yeteneklerinin güvenliği anlamında ele alınmaktadır. BM Sözleşmesi Madde 2(4), devletlerin toprak bütünlüğüne ek olarak siyasi bağımsızlığına karşı da tehdit ya da kuvvet kullanımından kaçınılması vurgusunu yapar. Siyasi güvenlik tüm vatandaşların ve siyasi partilerin güvenliğini de içerir ancak sadece tek zümrenin güvenliği anlamında değildir.[24]

Sosyal, politik, demografik, etnik yapıların ve modellerin dış etkilere ve manipülasyonlara karşı daha dirençli olabilmesinin sağlanabilmesi için alınabilecek önlemler,

[20] Özben, Perception, s 280.
[21] Barry Buzan, "Askeri Güvenliğin Değişen Gündemi", *Uluslararası İlişkiler Dergisi*, Cilt 5, Sayı 18 (Yaz 2008), s 109.
[22] Selin Erkul, "Askeri Güvenlik Çalışmalarına Dönüş: Önleyici Savaş", Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi Y.2018, C.23, S.2, s 646.
[23] Ebru Yavuz Yayla, "Basın Özgürlüğü ve Milli Güvenlik Kapsamında Sınırları", Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Nisan 2019, s 70.
[24] Yavuz Yayla, Age s 75.

yürütülebilecek faaliyetler, hazırlıklar ve etkileşimleri içerir. Öte yandan devletlerin uluslararası arenada kendilerini ifade edebilmeleri ve uluslararası hukuk kapsamında haklarının korunabilmesi için önlemler alabiliyor olması, farklı niteliklerde ortaya çıkma ihtimali olsa dahi, bu kapsamda bir güvenlik bileşeni olarak ele alınabilecektir.

c. Sınır Güvenliği (Yeşil Vatan, Mavi Vatan, Gök Vatan, Siber Vatan),

Belirlenmiş tüm sınırlar için sınır güvenliğinin sağlanabilmesi adına askeri, fiziksel, kurumsal, yapısal vb. modellerin geliştirilmesi, uygulanması, önleyici, koruyucu, azaltıcı tedbirlerin alınması bu kapsamdadır. Rapor kapsamında ilgili bölümlerde detaylı olarak ele alınmıştır.

d. Kritik Altyapı Güvenliği,

Eksikliği ya da zarar görmesi durumunda devletin, toplumun, ulusal sistemin işleyişinin negatif olarak etkilenmesine yol açabilecek her türlü altyapının güvenliğinin sağlanması bu kapsamda ele alınabilecektir. Kritik bir altyapı, ulusun ekonomik refahı, fiziksel ve ruhsal sağlığı, güvenliği vb. veya bunların herhangi bir kombinasyonu için çok önemli olan sistem ve varlıkları içerir.[25] Çoğunlukla devlet kaynakları ile tesis edilmişlerdir. Enerji hatları, bilgi ve iletişim sistemleri, su şebekeleri, ulaştırma hatları ve sistemleri, endüstriyel tesisler, kurumsal yönetim sistemleri vb. bu içerikte ele alınabilmektedir.

Rapor kapsamında örneğin finansal sistem ekonomi güvenliği ile, enerji tedarik ve üretim yetkinlikleri enerji güvenliği ile, tarımsal üretim ve arz altyapısı, gıda, su ve tarım güvenliği ile, ulaştırma sistemlerinin güvenliği ise ulaştırma güvenliği ile bağdaştırılarak ve ayrı ayrı değinilmesi gerektiği yaklaşımı altında ele alınmıştır.

e. Afet Yönetimi,

Sel, yangın, deprem gibi doğal sebepler ile tetiklenen tehditlerin, devletin işleyişine, toplumun düzenine ve sağlığına zarar verebilecek nitelikte ve yerel birimlerin yeteneklerinin ötesindeki bir seviyede ortaya çıkma olasılığı bu kapsamdadır. Bazı durumlarda afetlerin ani ve şiddetli etkileri olabilmektedir, kitlesel yıkıcılık özelliği taşıyabilme potansiyeline dayanarak silahlı kuvvetlerin desteğine de ihtiyaç duyulabilmektedir. Bu sebeple sert bileşenlerin içerisinde kaldığı yorumlanmaktadır.

[25] Cristina Alcaraz, Sherali Zeadally, "Critical Infrastructure Protection: Requirements and Challenges for the 21st Century", International Journal of Critical Infrastructure Protection, Volume 8, January 2015, Elsevier, s 53.

Afetlerin temel özellikleri doğal olmaları, can ve mal kaybına sebep olmaları, kuraklık, çölleşme gibi zamana yayılı çevre felaketleri dışında (bu unsurlar çevre güvenliğinin alt maddeleri olarak ele alınmıştır) bir anda hızlıca oluşmaları ve engelleyebilme olasılığının bulunmamasıdır.[26]

İnsanların yaşadıkları ortamda ortaya çıkma olasılığı bulunan doğal tehdit ve tehlikelerin farkında olmaları, sebeplerine ek olarak korunma, önleme ve azaltma yöntemleri geliştirme çabaları Afet Yönetimi olarak adlandırılabilir.[27]

f. Göç Yönetimi,

Devletin sınırları içerisine yabancıların girişinin ve sınırlar içerisinde yabancıların bulunması durumlarının karşılıklı güvenliği sağlayarak yürütülmesi olarak özetlenebilir.[28] Göç önleme, izleme, önleyici tedbirlerin alınması ve uygulanması gibi süreçleri yönetmek için devletin ilgili birimleri ulusal bir bütünlük içerisinde görev yapar. Ekonomik ve siyasi gerekçeler ile oluşabilen göç hareketleri, ülkeler arasındaki tarihsel ve kültürel bağlantılarla da ilgilidir ve kapsama özel politika ve yasal düzenlemeler ile yönetilmelidir.[29]

Anayurt Güvenliği Yumuşak Bileşenleri[30]

Birleşmiş Milletler Kalkınma Programı insani güvenliği, açlık, hastalık, baskı gibi tehditlere karşı insanların günlük hayatlarında güvenliklerinin sağlanması ve korunması olarak ifade eder.[31] Yumuşak bileşenlerin ayrıştırılması anayurt güvenliği bağlamında yapılmaya çalışıldığından temeline insani güvenlik kavramını almamıştır, ayrıştırma insani güvenlik kavramına yönelik tanımlamalar doğrultusunda yapılmamıştır. Literatürde ekonomi, çevre, sosyal güvenlik gibi başlıkların daha az önemsendiği, savaşlar ve silahlanma gibi açık ve sert tehditler ile kıyaslandığında kapalı ve yumuşak tehditler içerdiğine yönelik değinmeler

[26] Ramazan Sever (Ed), "Afetler ve Afet Yönetimi", PEGEM Akademi, 2019, Ankara, s 5.
[27] Tevfik Erkal, Mehmet Değerliyurt, "Türkiye'de Afet Yönetimi". Doğu Coğrafya Dergisi, 14 (22), 2011, s 151.
[28] Perruchoud, Redpath, J., (Ed), Age, s 36.
[29] Sühal Şemşit, "Avrupa Birliği Politikaları Bağlamında Uluslararası Göç Olgusu ve Türleri: Kavramsal Bakış", Manisa Celal Bayar Üniversitesi İ.İ.B.F., Yönetim Ve Ekonomi , 2018, Cilt: 25 Sayı: 1, s 276.
[30] Özden ÖZBEN, Doktora Tezi, Mayıs 2023, Ankara.
[31] Yahya Alameşe, "COVID-19 Salgını ve İnsani Güvenlik", İstanbul Kent Üniversitesi İnsan ve Toplum Bilimleri Dergisi, Cilt: 2 Sayı: 1 Yıl: 2021, s 34.

bulunmaktadır.[32] Buzan ve Wæver, 1989 sonrasında Avrupa güvenlik söylemine çevre, göçmenler, etnik çatışma, örgütlü suçlar ve terörizm gibi konuların dâhil olduğunu ifade etmektedir.[33] Efe ise, AB'nin güvenlik çıkarlarının çoğunlukla enerji, ulaşım ve sınır yönetimini kapsamakta olduğunu ifade eder.[34]

Tehdidin, fiziksel, sosyal, kültürel vb. varlıklara ve değerlere zaman içerisinde nispeten yavaş biçimde zarar verme ihtimali taşıması ya da gösterilecek tepkinin veya alınacak tedbirin öncelikli olarak sert kuvvet kullanımı gerektirmemesi durumu, bileşenlerin yumuşak olarak sınıflandırmalarının temelini oluşturmaktadır.[35] Bu kapsamda bir başka çalışma, ulusal güvenliğin askeri olmayan unsurlarını şu şekilde önermiştir: Politik güvenlik, ekonomi güvenliği, enerji ve doğal kaynaklar güvenliği, anayurt güvenliği, siber güvenlik, insan güvenliği ve çevre güvenliği.[36]

Bileşenlerin "yumuşak" olarak sınıflandırılmış olması, bu başlıklarda bireysel, kurumsal ve ulusal eyleme geçme reflekslerinin yumuşak güç kullanımını gerektirmesi anlamına gelmemektedir. Bu refleksler ve çözüm girişimleri doğal olarak her tür güç kullanımını içerebilecektir ancak burada fark, sert güç kullanımının öncelikli olarak tercih edilmediği durumlar olarak ifade edilmektedir. Yumuşak ve sert bileşen ayrımları esasen refleksin, tepkinin, çözüm girişiminin türünden ve yapısından ziyade neyin korunduğundan hareketle yapılmıştır. Örneğin bir nükleer enerji tesisine düzenlenebilecek siber saldırı için tepkisel çabalar siber güvenlik, enerji temin ve arz kapsamında enerji güvenliği, nükleer felaket ihtimali değerlendirilecek ise çevre ve sağlık güvenliği, enerji kıtlığının yaratabileceği ekonomi güvenliği ve sosyal güvenlik, hatta sanayi güvenliğine kadar uzanan bir çerçevede ortaya çıkabilecektir.

Bu örneğe dayanarak doğrudan bir yumuşak "Nükleer Güvenlik" unsuru eklenmemiştir. Öte yandan nükleer tesisler kritik altyapılardır. Kritik altyapılara karşı ortaya çıkabilecek tehditler için gösterilecek tepkinin sert nitelikte olma ihtimali daha yüksek olabilecektir. Bu

[32] Şafak Kaypak, "Güvenlikte Yeni Bir Boyut: Çevresel Güvenlik", Ekonomik ve Sosyal Araştırmalar Dergisi, Cilt:8, Yıl:8, Özel Sayı, 8:1-22, s 18.
[33] Sinem Akgül Açıkmeşe, "Kopenhag Okulu ve Realist Güvenlik Çalışmalarında Aktör, Tehdit ve Politika: Avrupa Güvenliği Üzerine Bir Değerlendirme", Doktora Tezi, Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Avrupa Birliği ve Uluslararası Ekonomik İlişkiler Anabilim Dalı, 2008, Ankara, s 257.
[34] Haydar Efe, "Avrupa Birliği'nin Ortak Dış ve Güvenlik Politikası Yaratma Çabaları ve Türkiye'ye Etkileri", Doktora Tezi, İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü, Avrupa Topluluğu Anabilim Dalı, 2005, İstanbul, s 270.
[35] Özben, Perception, s 280.
[36] Kim R. Holmes, "What Is National Security", Heritage Foundation, 2015 Index Of U.S. Military Strength, s 19.

örneğe dayanarak nükleer enerji tesislerine karşı olası tehditler, sert bileşenlerin içerisinde "Kritik Altyapı Güvenliği" kısmında da ele alınabilecektir. Bu örnekten görüleceği üzere riskin ne bağlamda ele alındığına, tehdidin ve tehlikenin nerede ne türde ortaya çıkabileceğine bağlı olarak ilgili planlamalar yapılmalı, çok boyutlu ve çok bileşenli analizler yapılarak bütüncül yönetim geliştirilmelidir.

a. Siber Güvenlik,

Geleneksel tanımına göre siber güvenlik, bilgisayar donanımları, cihazları ve ağları ile birlikte önem arz eden verilerin yetkisiz kişiler tarafından erişiminin kısıtlanmasına veya suç odaklı olarak kullanılmasının önlenmesine yönelik koruma faaliyetleridir.[37] Uluslararası Telekomünikasyon Birliği ise siber güvenliği, tüm aktörlerin siber uzayda varlıklarını sürdürebilmek amacıyla kullandıkları tüm uygulamalar, politikalar ve teknolojilerin olarak tanımlar, özetle tüm paydaşların siber uzaydaki risk ve tehditlere karşı korunmasıdır.[38] Bir başka tanım, siber uzayı/ortamı tesis eden tüm bilişim ve iletişim sistemlerinin korunması, bilginin gizlilik, bütünlük ve erişilebilirliğinin eksiksiz sağlanması olarak yapılır.[39] Siber uzay/ortam, insan, altyapı, bilgi ve mantıksal kurgu olarak dört unsur içeren sayısal bir sistemdir, ayrıca tüm bilgi işleme, saklama, iletişim sistemleri ve uygulamalarını da kapsar.[40]

Anayurt güvenliğinin bir bileşeni olarak siber güvenlik, günümüz teknolojik gelişmeleri doğrultusunda anayurdun herhangi bir unsurunu tehlikeye atacak ya da risk oluşturabilecek her türlü sayısal tehdide karşı koruyucu ve kurtarıcı her tür önlemin alınması olarak genişletilebilir. Siber uzayda ortaya çıkabilecek saldırılar, gıda, su, tarım, enerji, ulaştırma, sağlık, ekonomi, sağlık, çevre gibi birçok başlıkta ciddi nitelikte sorun yaratma potansiyeline sahiptir. Bu sebeple ve bu kapsamda ele alınması gerektiği değerlendirilmekte ve yumuşak bileşenlerin içerisine dâhil edilmektedir. Siber güvenlik, her ne kadar verilecek tepkinin olası yapısı sebebi ile yumuşak bileşenler içerisinde tutulsa da, saldırı unsuru olarak kullanıldığında ani ve ciddi zarar verme riski içerir. Aslında bu kapsamda, siber ortamın da sınırlarının bulunması gereğine yönelik bir değerlendirme yapıldığında, siber savunma ya da saldırı güçleri de tıpkı askeri bir

[37] Şahin Kara, "Siber Güvenlik Analizi İçin Yeni Bir Siber Saldırı Simülatörü Geliştirilmesi", Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Doktora Tezi, Ağustos 2022, s 17.
[38] Soner Çelik, "Küreselleşme Sürecinde Değişen Güvenlik Algısı: Siber Güvenlik Örneği", Süleyman Demirel Üniversitesi, Sosyal Bilimler Enstitüsü, Doktora Tezi, Isparta, 2021, s 43.
[39] "Siber Güvenliğe İlişkin Temel Bilgiler", Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT) Bilgi Teknolojileri ve İletişim Kurumu, Telekomünikasyon İletişim Başkanlığı, Temmuz 2014, s 5, Erişim tarihi 4 Ocak 2013:
https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf
[40] Çelik, Age s 37.

güç unsuru gibi ele alınabilecektir. Bu kapsamda yapılacak analizlerin, siber güvenliği sert bileşenler içerisine çekmesi beklenebilir.

b. Gıda, Su ve Tarım Güvenliği,

Sınırların fiziksel anlamda korunması sahip olunan toprağın, denizin, havanın, bilginin uç noktalarına varana kadar muhafaza edilmesi şeklinde yorumlansa da, toprağın niteliğinin, verimliliğinin, işlenebilirliğinin, bütünlüğünün korunması, suyun kullanılabilirliğinin, erişilebilirliğinin, aktarılabilirliğinin korunması, gıdanın üretilebilirliğinin, iletilebilirliğinin, erişilebilirliğinin sağlanması bu kapsamda ele alınabilecektir (gıda güvenliğinin dört bileşeni bulunur: bulunabilirlik, erişilebilirlik, güvenilirlik ve istikrarlılık [41]). Hatta kapsam daha geniş tutulduğunda toprağın kalitesinin yükseltilmesi, dayanıklılığının artırılması, suyun temizliğinin garanti edilmesi ve tüketilen gıdanın toplumsal sağlığa etkilerinin pozitif seviyede tutulması çabaları da bu kapsama girebilecektir (gıda güvenliği, tüketilmesi durumunda insan sağlığına zarar verebilecek tehlikelere yönelik olarak tanımlanabilmektedir [42]).

Bu çerçevede düşünmeye başladığımızda, fark edilebileceği üzere bileşenlerin etkileşimi alanına doğru çekiliriz. Artık gıda ve tarım güvenliğinin sağlık güvenliği ile birlikte ya da su güvenliğinin kritik altyapı güvenliği ile bir arada ele alınması gereksinimleri ortaya çıkacaktır.

c. Ekonomi Güvenliği,

Bu kapsamda üç farklı düzeyde güvenlik tartışmaları yapılmaktadır: sınır ötesi ekonomik ilişkilerde güvenlik, ulusal rekabet gücü ve ekonomik refaha yönelik güvenlik ve yaşama dair olanaklara dayalı bireysel ekonomi güvenliği.[43] Anayurt güvenliği bağlamında ekonomi güvenliğine yönelik analizlerin, aslında her üç bileşeni de içerdiği ya da içermesi gerektiği değerlendirilmektedir. Ekonomik yapının uluslararası arenada rekabet edebilir bir seviyede olması ve bu rekabetin geniş ölçekli ticaret yapılabilecek bir yetenekte kullanılması, ulusal ve dolayısıyla bireysel ekonomik koşulların daha nitelikli bir seviyede olabileceğine işaret eder. Ya da örneğin ulusal ve bireysel ekonomik koşulların seviyesindeki yükseklik, sanayi ve teknoloji alanlarında gelişme göstermeye meyilli bir altyapı sahipliğini ve dolayısıyla

[41] İclal Akın, "Su, Toprak ve İklim Değişikliğinin Güvenli Gıdanın Sürdürülebilirliği Üzerine Etkileri ve Bazı Tespitler", Rahva Teknik ve Sosyal Araştırmalar Dergisi, Cilt: 1, Sayı:1, 2021, s 14.
[42] Gökçe Koç, Ayşe Uzmay, "Gıda Güvencesi ve Gıda Güvenliği, Kavramsal Çerçeve, Gelişmeler ve Türkiye", Tarım Ekonomisi Dergisi 2015; 21(1), s 41.
[43] Halil İbrahim Aydın, Muhammet Cemal Şahinoğlu, Ahmet Ateş, "Ekonomi Güvenliği Üzerine Ekonomi-Politik Bir Çözümleme", Maliye ve Finans Yazıları - 2022 - (117), s 202.

uluslararası alanda kabul gören bir mal ve hizmet sunum yeteneğini de beraberinde getirebilecektir.

Ülke ekonomisinin ulusal çıkarlara dayalı bir modelde yürütülebilmesi için, yüksek teknoloji üretimine yönelik ve istikrarlı bir endüstriyel yapı sahipliği kritik önemdedir.[44] Bu kapsamda anayurt güvenliği bağlamında yukarıda tanımlanan her üç unsurun da niteliğinin yüksek seviyede tutulmasının önemli olduğu vurgulanabilir.

Bir başka tanıma göre ekonomi güvenliği, iktisadi yapının istikrarlılığıdır, anlık şoklara dayanıklılıktır ve dalgalanmalara karşı esnekliktir.[45] Anlık şoklar, COVID-19 gibi küresel salgınlar ya da küresel / yerel ekonomik krizler gibi durumların yaratabileceği geniş ölçekli ve etkisi yüksek sorunlar olarak yorumlanabilir.

d. Enerji ve Doğal Kaynaklar Güvenliği,

Enerji güvenliği, refahın korunabilmesi ve sürdürülebilmesi adına enerjinin yeterli miktarda ve makul bir bedel ile sağlanması olarak özetlenebilir, dört unsuru vardır: Varlık, erişilebilirlik, ekonomiklik ve sürdürülebilirlik.[46]

Ek olarak enerji üretimi için kritik olup olmadığına bakılmaksızın mevcut doğal kaynakların korunması, yeni doğal kaynakların oluşturulması, var olanların verimliliklerinin arttırılması konuları da bu kapsamda ele alınabilecektir.

e. Sağlık Güvenliği,

Temelde insanların sağlıklarının korunması ve hayatlarını sağlıklı olarak sürdürebilmelerinin sağlanabilmesi adına temel sağlık hizmetlerine ve tedavi olanaklarına sahip olmaları anlamındadır.[47] Bu kapsamda birey ve toplum sağlığı açısından tehdit oluşturabilecek her türlü salgın, hastalık, bakteri, biyolojik manipülasyona karşı tedbir alma, ilaç ve kimyasal madde yönetimi, ayrıca sağlık sisteminin bir bütün olarak sürdürülebilmesinin sağlanması da bu tanıma dâhil edilebilir.

[44] Aydın, Şahinoğlu, Ateş, Age s 209.
[45] Aydın, Şahinoğlu, Ateş, Age s 207.
[46] Mitat Çelikpala, "Enerji Güvenliği: NATO'nun Yeni Tehdit Algısı" Uluslararası İlişkiler, Kış 2014, Vol. 10, No. 40, Özel Sayı: NATO'nun Dönüşümü ve 21. Yüzyılda Güvenlik), Uluslararası İlişkiler Konseyi İktisadi İşletmesi, s 85.
[47] Alameşe, Age s 38.

f. Çevre Güvenliği,

Çevre Güvenliği, çevre temeline dayalı tehditlerden korunmayı ve bu çerçevede olası negatif etkileri indirgemeyi içeren bir kavramdır, ayrıca çevreye verilebilecek zararlar da bu kapsamdadır.[48] Güvenlik stratejilerinin şekillenişinde doğa, en iyi ihtimalle, çevresel sorunlar bağlamında gündemin alt sıralarında yer alırken geleneksel strateji anlayışında yeni bir güvenlik kaygısı olarak etiketlenmektedir.[49] Çevreye verilebilecek her tür zarar (çevrenin güvenliği), doğrudan ya da dolaylı olarak sağlık ve ekonomi güvenlikleri için de etkileyici durumdadır, bu açıdan bakıldığında çevreye verilen zarar ile çevre temeline dayalı tehditlerin birbirini doğurduğu söylenebilir.

Sanayi güvenliği ile çevre güvenliği arasında da bir çeşit paradoks bulunur. Sanayileşmenin yarattığı çevresel negatif etkiler ile çevre güvenliğinin sağlanabilmesi adına endüstriyel anlamda atılması gereken önleyici adımlar birbirini kısıtlar niteliktedir. Çevre güvenliğine yönelik geniş kapsamlı bir tanımın "sürdürülebilir kalkınma" ile çatışabileceği değerlendirilmektedir.[50]

Çevre güvenliğinin üç ana unsuru vardır: tüm canlıların varlığına ve hayatlarına etki edebilecek çevresel krizler, çevre ilişkili problemlerin yaratabileceği ekonomik ve siyasi sorunlar ve çevresel kaynaklara yönelik hak iddialarının yaratabileceği çatışma ihtimali.[51]

g. Sanayi Güvenliği,

Endüstriyel yetkinliklerin ve üretim kabiliyetlerinin bağımsız bir niteliğe ulaştırılması, ayrıca endüstriyel verilerin üretilmesi, değerlendirilmesi, korunması, geliştirilmesi gibi kavramların bu başlık altında değerlendirilebileceği yorumlanmaktadır. Endüstriyel yetkinliklerin artırılabilmesi ve bu doğrultuda sürdürülebilir kalkınma sağlanabilmesi çabalarının dışında özellikle savunma sanayii gibi özel alanlarda araştırma – geliştirme, teknoloji yönetimi, tasarım, üretim, bakım, işletme gibi süreçlerin ve işlevlerin eksiksiz işlemesinin sağlanması da bu kapsam altında tutulabilecektir. 3 Temmuz 2004 tarihli, 5. Tertip, 43. Cilt ve 25511 sayılı resmi gazetede yayınlanmış olan 5202 numaralı Savunma Sanayii

[48] Şeyma Şiraz, Elif Sarız, "AB Sürecinde Türkiye ve Çevre Güvenliği", Gaziantep Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi, 13. Uluslararası Kamu Yönetimi Sempozyumu, 2019, s 1307.
[49] Çağdaş Dedeoğlu, "Güvenliğin Doğası ve Doğanın Güvenliği Üzerine Bazı Notlar", Tolga Sakman, (Ed), "Devlet Doğasının Değişimi: Güvenliğin Sınırları", TASAM Yayınları, Uluslararası İlişkiler Serisi, Nisan 2017, İstanbul, s 534.
[50] Damla Kocatepe, "Güvenlik Çalışmalarında Çevre Güvenliği Sorunsalı", Kafkas Üniversitesi İktisadi ve İdari Bilimler Fakültesi, KAÜİİBFD, Cilt, 9, Sayı 17, s 344, 2018.
[51] Kaypak, Age s 14.

Güvenliği Kanunu, savunma sanayiinde araştırma, geliştirme, imalat ve montaj yapan kurum ve şahıslara ait bilgi, belge, proje, malzeme ve hizmetlerin güvenliğinin sağlanması ve korunması olarak kapsamı içermektedir.

h. Ticaret Güvenliği,

Güvenli bir toplum yaratabilme kaygısı ile açık bir ticari iletişim evreni tesis edebilme çabası birbiri için tehdit içerebilecek unsurlar olarak ele alınabilecektir. Küreselleşmenin karşılaşılabilecek ticari etkileri, yerelde ve uluslararasında pozitif ya da negatif yapılarda olabilecektir. Hatta örneğin bazı durumlarda negatif etkisinin pozitif etkiye göre daha fazla korunmasını gerekebilecek durumlar da ortaya çıkabilecektir (örneğin yüksek maliyetine karşın yerli ürünlerin tercih edilmesi gibi). Özetle ticaret güvenliğinin kendi içinde kendine has ve değerlendirmeye esas unsurları bulunabilecektir. Bu sebeple ve ticaret güvenliğinin çoklu etkileyicilik ya da etkilenme potansiyeline dayanarak anayurt güvenliğinin hassas bir yumuşak bileşeni olarak (sosyal, kültürel, ekonomik, çevre vb.) ele alınabileceği / alınması gerektiği yorumlanmaktadır.

Ticaret için hammaddeye duyulan ihtiyacın yanı sıra pazar arayışları da kritik önemdedir ancak süreç boyunca güvenlik önemli bir sorun potansiyeli taşıyabilir. Bu kapsamda ticari güvenlik, (bireysel ve kurumsal olarak ulusal ve uluslararası ölçekte) yatırımların siyasi güvenceye sahip olması, güvenli mal ve finansal hareketlerin sağlanması[52] ve ticaretin sürdürülebilir olduğuna / olacağına yönelik güven duygusunun tesis edilmesidir.

i. İletişim Güvenliği,

Toplumsal / bireysel iletişim / etkileşim güvenliği, muhtelif platformlar aracılığı ile iletişime, etkileşime, bilgilenmeye ve bilgilendirmeye yönelik altyapıların sağlanması ve korunmasıdır. Geniş çerçeveli bir tanım, her tür yazılı, sözlü, görsel iletişimin muhtelif kaynaklar aracılığı ile yapılabilmesine yönelik güvenliğin sağlanması kavramını içerebilir. Ancak iletişim ve etkileşimde esneklik, illegal girişimler için farklı düzlemlerde bir ilgi alanı doğurabileceğinden, genel güvenlik kaygıları açısından bu dengenin korunması önem arz edecektir. Bu bakış açısı altında ve diğer bileşenler ile etkileşiminin analiz potansiyeli taşıdığından hareket ile bir yumuşak güvenlik bileşeni olarak tespit edilmiştir.

[52] Fikret Birdişli, "Neoliberalizmin Ulusal Güvenlik Siyasalları Üzerine Etkileri ve Türkiye'nin Güvenlik Siyasası Üzerine Bir inceleme", Stratejik Araştırmalar Dergisi, TASAM, Sayı 13, 2009, s 48.

j. Ulaşım Güvenliği,

Ulaşım güvenliğinin trafik kazaları ve terör sebepli olarak iki alt maddede işlenmiş olmasına rağmen[53] aşağıdaki kapsamlarda da ele alınabileceği değerlendirilmektedir: Devletin vatandaşlarına ya da ziyaretçilerine serbest ve sorunsuz ulaşımı sağlaması ve sınırları içerisinde her alana giriş ve çıkış hakkını sunabilmesi. Ek olarak ulusal ve uluslararası ulaşım / ulaştırma kapsamında gerekli ulusal / uluslararası koordinasyonun sağlanması ve yolcu can ve sağlık güvenliğinin tesis edilmiş olması. Bu doğrultuda ulaşım ve ulaştırma altyapılarının nitelikli bir şekilde tesis edilmesi, etkin ve verimli ulaşım araçlarına sahip olunması. Bu kapsam, yolların, araçların, köprülerin, havaalanlarının, limanların, demiryollarının vb. sürekli işler durumda tutulması ve illegal amaçlı kullanımlar için sürekli ve düzenli kontrol sağlanması başlıklarını da içerebilecektir. Ancak kontrol ve izlemenin ulaşım ve ulaştırma akışının sekteye uğratmaması da sağlanabilmelidir.

k. Eğitim Güvenliği,

Devletin her vatandaşının eğitim haklarının korunması, eğitim olanaklarına sahip olması ve eğitim için gereken koşulların sağlanmasıdır. Ayrıca eğitim sisteminin işleyişine ve geliştirilmesine yönelik olası teknik ve sosyal engellerin tespiti, bu olası engellerin uygun yöntemler ile aşılması, eğitim için gerekli insan, altyapı, sistem gibi ihtiyaçların giderilmesi, eğitim yöntemlerinin geliştirilmesi, korunması ve millileştirilmesi de bu kapsama girecektir. Buradaki temel yaklaşım, vatandaşın sorunsuz ve güvenli bir şekilde eğitim alabilmesinin sağlanması, eğitiminin sürdürülebilmesi konusunda gereken tedbirlerin alınabilmesi ve karşılaşılabilecek önleyicilerin giderilmesidir. Eğitim güvenliğinin sağlanmasının, analizi yapanın yaklaşımına göre, diğer tüm bileşenler ile etkileşimde olabileceği yorumlanmaktadır.

l. Sosyal ve Kültürel Güvenlik

Bu kapsamda güvenliğin sağlanması, küreselleşmenin negatif etkilerine ya da örneğin kamu diplomasisi faaliyetlerine karşı halkın dil, inanç, ırk, örf, töre, ahlak gibi ulusal ve etnik niteliklerinin, ayrıca sosyal ve kültürel değerlerinin ve varlıklarının korunabilmesi için yürütülecek faaliyetler ve tedbirler olarak özetlenebilecektir.

Kültürel güvenliğe yönelik tehditlere bir örnek olarak göçmen hareketleri gösterilebilir. Değişik kültürlerden göçmen alan ülkelerde göçmen karşıtlığı, ulusal kültürel yapıya tehdit

[53] İrem Ayhan Selçuk, "Ulaşım Güvenliğini Sağlamada Bir Araç Olarak Planlama", İdealkent, Sayı 23, Cilt 9, (2018), s 136.

potansiyeli ile gelişmektedir.[54] Farklı tehdit kaynaklarının kültürel güvenlik ile bağlamlarının analiz edilmesinin, kültürel güvenliğe yönelik kavramsal karmaşayı kısmen giderebileceği değerlendirilmektedir.[55] Bu bakış açısı altında sosyal ve kültürel güvenlik, yumuşak bileşenler içerisinde tutulmuştur.

Yukarıdaki maddelerden görüleceği üzere bazı bileşenler tek boyutlu değil, çok boyutlu bir şekilde ortaya çıkabilmektedir. Örneğin bir nükleer felaket kısmen enerji güvenliğinin, altyapı güvenliğinin, belki çoğunlukla çevre ve sağlık güvenliğinin etkileyicisidir. Okuyucu, çalışmalarının amacına göre nükleer felaketin bir afet olduğunu veya etkilediği asli unsurun sağlık güvenliği olduğunu da yorumlayabilecektir. Bileşenlerine ayırma yaklaşımının bu sebeple kritik önemde olduğu değerlendirilmekte ve rapor kapsamında analizler bu doğrultuda yapılmaktadır. Analizinin yapılmasına ihtiyaç duyulan konu enerji güvenliği ise bu kapsamda tüm etkileyiciler kapsama alınabilmeli, çevre güvenliği kapsamında yorumlama yapılacaksa kapsam bu çerçevede tutulmalı, sağlık güvenliği temele alınacaksa merkezde sağlık güvenliği tutularak diğer etkileyiciler denkleme katılabilmelidir.

Bileşenler bazı durumlarda sadece bir bileşeni değil, çoklu bileşenleri etkileme ya da kendisine diğer bileşenler içerisinde tanım bulabilme olasılığına sahip olabilmektedir. Bu sebeple bileşenlerin kesişim alanlarının ve oluşturduğu kümelerin bütüncül olarak ele alınması gerektiği değerlendirilmektedir. Bir örnek kesişim kümelenme yapısı Şekil 1'de verilmektedir. Bu gösterimde herhangi iki yumuşak bileşen arasında bir kesişim alanı bulunmuyor olması, bileşenlerin birbiri ile etkileşiminin olmadığı kabulünden ziyade, araştırmacı için ihmal edilebilir ya da kapsam haricinde olduğu şeklinde yorumlanmalıdır. Örneğin şekilde sağlık güvenliği ile sanayi güvenliğinin etkileşim alanı gösterilmemiştir ancak küresel bir salgın yaşanması durumunun sanayi ve üretim güvenliğine etkileri analiz edilecek olduğunda bu alan daha baskın bir şekilde gösterilebilecektir. Özetle neyin çalışıldığına bağlı olarak bu etkileşim haritası yeniden yapılandırılabilir.

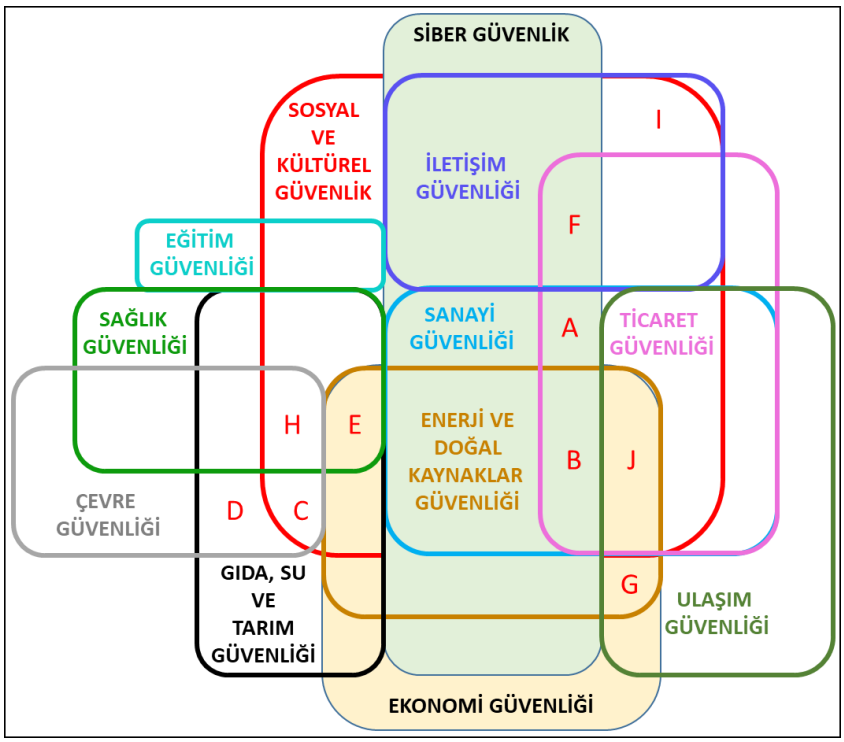
Temeline siber güvenliği ve ekonomi güvenliğini alan bu yaklaşım dışında araştırmacı, örneğin sosyal ve kültürel güvenliği ve belki eğitim güvenliğini tabana yerleştirip, diğer bileşenlerin bu kapsamda kesişim alanlarını ortaya çıkarmaya da çalışabilecektir. Böyle bir

[54] Şükriye Gökçe Gezer, "Kültürel Güvenlik", Güvenlik Yazıları Serisi, No.50, Kasım 2019, s 2. Erişim tarihi 6 Ocak 2023:
https://trguvenlikportali.com/wp-content/uploads/2019/12/KulturelGuvenlik_SGGezer_v.1.pdf
[55] Gezer, Age s 4.

durumda etkileşim ve kesişim alanları başka bir analiz ortamı ve daha farklı yorumlama ekseni sunabilecektir. Şekil 1.2'deki etkileşim haritasında A alanı, ticaret ve sanayi güvenliğinin siber güvenlik ile etkileşimini gösterirken, B alanı ayrıca ekonomi güvenliğini de denkleme almaktadır. G alanı, enerji ve ulaşım güvenliğinin ekonomi güvenliği açısından tanımına yönelik iken J alanı bu analizlere ticaret güvenliğini de eklemektedir. I, iletişim güvenliğinin sosyal ve kültürel değerlere karşı olumsuz etkilerini araştırmayı hedefleyen bir araştırmacının odağı olabilirken F alanındaki bir araştırmacı, iletişim ve ticaret güvenliğini sosyal ve kültürel güvenlik ile bağdaştırmaya çalışıyor olabilir.

Bir başka örnek olarak E, ekonomi güvenliği temelinde gıda ve su güvenliğinin sağlık güvenliğine etkisini ve bunun sosyokültürel değerler ile bağlantısını betimlerken, H alanı bu kapsama çevre güvenliğini almakta ancak ekonomi güvenliğini çıkarmaktadır. Benzer şekilde D gıda ve su güvenliği ile çevre güvenliğini bağdaştırır. C ise gıda, su ve sağlık güvenliklerini sosyal ve kültürel güvenlik bağlamında analiz etme potansiyelini sunar. Bu örneklerden görülebileceği üzere analizin odağına ve yöntemine göre alternatifler çoğaltılabilmektedir. Bu kesişim kümelerinin araştırmacı açısından farklı temellere oturtulması yaklaşımı ise bambaşka kapsamlar sunabilecektir. Bu potansiyele dayanarak bileşenlere ayırma yaklaşımı detaylandırılmış ve görselleştirilerek örnekler verilmiştir.

Şekil 1: Bir Örnek Olarak Siber Güvenlik ve Ekonomi Güvenliği Temeline Dayanan Anayurt Güvenliği Yumuşak Bileşenler Etkileşim Haritası



Kaynak: Özden ÖZBEN, "Anayurt Güvenliğinin Sert Bileşeni Olarak Sınır Güvenliği ve Entegre Sınır Yönetimi" Doktora Tezi, Polis Akademisi, Mayıs 2023, Ankara.

Yukarıdaki yorumlamalar anayurt güvenliğinin sert ve yumuşak bileşenlerinin birbirleri içindeki etkileşimlerine yönelik örnekleri vermeye çalışmış olsa da, tehdit türleri, risk analizi çalışmaları veya araştırma alanları, doğal olarak yumuşak ve sert bileşenlerin birbirleri arasındaki etkileşimi de ele almayı hedefleyebilecektir. *Bu rapora esas teşkil eden anayurt güvenliği için bilgi yönetimi kavramı, belirtildiği üzere sadece tek bir disiplin içerisinde bilginin edinimi ya da işlemi olmaktan ziyade, çoklu sektörel ya da disipliner bilginin, kurumlararası birlikte çalışabilirlik esasları doğrultusunda edinimi, paylaşımı ve işlemi anlamında ele alınmaktadır.*

Daha önce değinildiği üzere sert bileşenler için alınacak tedbirlerin doğrudan sert kuvvet kullanımı gerektirmesine rağmen, yumuşak bileşenlere aynı doğrultuda refleks geliştirme yöntemi tercih edilmeyebilir. Yumuşak bileşenlerden herhangi birinde ortaya çıkabilecek tehditler için de sert güç önlemleri doğal olarak alınabilecektir. Ancak rapor, bu bağlamda operasyonel müdahale ya da eylem planlarını tasarlamayı hedeflemediğinden, hangi

durumlarda nasıl bir tepkinin gösterileceği yapılan analizlere konu olmamıştır. Fakat ardıl çalışmalar için motivasyon unsuru olduğu yorumlanmaktadır.

Anayurt güvenliğinin bileşenlerinin her birine gösterilecek tepkilerin türlerinin de tarif edilmesi ya da tanımlanması gerektiği düşünülebilir. Örneğin ilk anda siber güvenlik kapsamında olduğu değerlendirilen bir tehdit için, yaratabileceği etkilere bakarak daha saldırgan tedbirlerin de alınması konusu gündeme gelebilecektir. Böyle bir durumun sert güç kapsamında mı ele alınması gerektiği tartışmaya açıktır. Bir başka örnek, kritik altyapılara karşı ortaya çıkabilecek bir tehdidin hangi durumlarda sert güç ile karşılanması gerektiğine yönelik karar alma mekanizmasıdır. Bu gibi karar alma ilişkili olası alternatiflere doğru yanıtlar verebilme çabasına dayanarak tanımlamalar yapılmıştır.

"Anayurt Güvenliğine Karşı Tehdit" kavramının esnek yapısına rağmen rapor kapsamında "Anayurt güvenliği bileşenlerinden herhangi birini veya bir grubunu herhangi bir seviyede olumsuz etkileme olasılığına sahip mevcut ve olası riskler bütünü" olarak ele alınmıştır ve değerlendirmeler bu tanım ekseninde yapılmıştır. Anayurda karşı ortaya çıkabilecek tehdit, risk ve tehlikenin boyutu, seviyesi ve düzlemi de, sınıflandırmaların yapılabileceği bir başka alan olabilecektir. Devlet merkezli bakış ile güvenliğin tüm olasılıkları üzerindeki yorumlamalar, çoğunlukla sınır güvenliği temeline dayandırılarak yapılmaktadır. Kocabaş, tehditlerin sınır içi güvenliğe yönelik olarak maddi ve manevi nitelikler de taşıyabileceğini yorumlar.[56] Ancak yukarıda bahsedildiği üzere sınır güvenliği, anayurt güvenliğinin bir alt unsurudur.

Tehdidin hangi boyutta, seviyede veya düzlemde olduğu (fiziksel, sosyal/kültürel, ekonomik vb.), hangi boyutta/düzlemde ne seviyede önlem alınması ve tepki gösterilmesi gerektiğinin temel yaklaşımlarını da çizecektir. Akçay, tehditleri hayati (varlığa, milli egemenliğe ve toprak bütünlüğüne yönelik) ve milli (iç istikrarı bozabilecek politik, ekonomik, doğal karışıklıklar) olarak sınıflandırmıştır. İki tür tehdidin daha varlığından bahseder: temel (bölgesel istikrarsızlık, demokratik olumsuzluk, mafyalaşma, suç oranı artışı vb.) ve ikincil (uzun vadede temel ya da milli tehdit olabilecek durumlar).[57] Ayrıca Akçay, iç (kökü iç ya da dış olabilen bütünlüğe ve milli refaha tehlike yaratan, ekonomik, sosyolojik vb.) ve dış (bir ülke

[56] Kocabaş, Age,, s 5.
[57] Nihat Akçay, "21. Yüzyılda Türkiye'nin Tehdit Algılamaları ve Güvenlik Açılımları", Doktora Tezi, Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Bursa 2008.

ya da terör örgütü kaynaklı) tehditlerin varlığını yorumlar. Ayrıca asimetrik tehdit tanımını da şu şekilde verir: "Hazır bulunamama sebebi ile etkisinin yüksek olabileceği, siyasi, sosyal ve ekonomik yapılarda istikrarsızlık sağlama potansiyeline sahip, düşük seviyede kuvvet ve teknoloji kullanarak etkin olmayı amaçlayan tehditlerdir".[58]

Tehdit, birbirinden farklı tehdit türlerinin birleşimi gibi de yorumlanabilmektedir.[59] Karabulut çalışmasında tehdidi devlet, toplum ya da bireyin varlığına ve değerlerini olumsuz etkileme ihtimali olan olgular olarak tanımlar ve üç farklı yapıda olduğunu belirtir: elde olanın kaybedilme riski, elde olmayana sahip olamama riski, aktörden bağımsız olan ve küresel nitelikli riskler. Karabulut ayrıca tehdidin, bu farklı biçimlerinin bir bileşkesi olarak tanımlanabileceğini de vurgular. Karabulut'a göre tehdidin türünden bağımsız olarak aktör, üç farklı halkada bir güvenlik sistemi tesis eder: içten gelebilecek tehlikeler için en iç halka, sınır komşularını içeren yakın çevre güvenlik halkası ve küresel tehdit halkası olarak en dış halka.

Kritik altyapı güvenliğine yönelik bir örnek şu kapsamda verilebilecektir: Kritik altyapı güvenliğinin enerji güvenliği temelinde sağlanmasında bir grup zorluk bulunur. Enerji dağıtım sistemlerinin ulusal ve uluslararası enerji ağlarına bağlı olması ve bilgi iletişim sistemlerinin de benzer şekilde uluslararası sisteme entegre olması sebebiyle muhtemel bir siber saldırı, fiziksel saldırı boyutunda etki oluşturabilecektir.[60] Ek olarak enerji temininde, arzında, dağıtımında yaşanabilecek sorunlar, sosyal ve ekonomik sonuçlar da doğurabilecektir ve analizlere konu olacak şekilde her biri değerlendirmelere konu olabildiğinde, analizler daha bütüncül yapılabilecektir. Yani kritik altyapıların sadece fiziksel olarak değil, güncel siber saldırı örneklerine dayanarak siber boyutta / düzlemde de korunması gerekliliği açıktır. Özetle tehdidin bileşeni, türü, derinliği, düzeyi (seviyesi), boyutu, düzlemi, etki alanı birden çok bileşende ortaya çıkabileceğinden bir bütün olarak ele alınmalıdır, sadece fiziksel korumanın yeterli olabileceği yanılgısına düşülmemelidir.[61]

Örneğin sadece enerji, sadece ekonomi, ya da sadece gıda ve tarım güvenliği temelinde bilgi yönetimi üzerinde analizler yapılacak olduğunda doğrudan ya da dolaylı diğer

[58] Akçay, Age,, s 17.
[59] Bilal Karabulut, "Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek", Doktora Tezi, Gazi Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Ankara, 2009. s 141.
[60] National Research Council, Committee on Science and Technology for Countering Terrorism, 2002. "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism". Washington, DC: The National Academies, Press. s 313. Erişim tarihi 19 Ekim 2022: https://doi.org/10.17226/10415
[61] Özben, Perception, s 282.

etkileyicilerin de denkleme katılabilme şansı olacaktır. Böylece tek boyutlu ve tek bileşenli analizler yerine çok bileşenli ve çok boyutlu (bütüncül, entegre) analizlerin yapılması mümkün olabilecektir.[62] Bu yaklaşım, entegre terimi kapsamında daha geniş ve etkin bir çerçevede güvenlik analizi yapabilmeyi sağlayabilecektir. Ayrıca, güvenlik yönetiminin neden ve nasıl entegre olması gerektiği, entegrasyon unsurlarının neleri ne amaçla içermesi gerektiği gibi sorulara daha net yanıtlar alınabilecek, daha az kaynak kullanımı ile daha etkin sonuçlar üretilebilecektir.

Bilgi işlem yönetimi perspektifinden bakıldığında, (ilgili bileşenlerin tümü için) anayurt güvenliğine yönelik bilgi yönetimini zorlaştıran 5 unsur bulunur:[63]

- Anayurt güvenliğinin esnek ve değişken tanımı,
- Çok sayıda karar verici ve kurumsal karmaşıklık,
- Çok sayıda ve belirsiz tehdit unsurları,
- Bilgi işlem projelerin verimlilik analizlerinin yapılmasındaki güçlük ve
- Kurumların farklı durumlar için farklı eylem planlarına sahip olmaları.

Ancak bu unsurların her biri, politika geliştirme açısından bakıldığında sadece bilişsel açıdan değil, yönetsel, kurumsal, sosyal vb. açılardan da önem taşımaktadır. Anayurt güvenliği tanımları, sorumlu kurumların ilgi alanlarına göre farklı önem ağırlıklarına sahip olabilecektir. Daha önce değinildiği üzere anayurt güvenliğinin bir bütün olarak ele alınması gerekliliği, çok sayıda ve çok boyutlu tehdit bileşenlerine çok sayıda kurum ve yetki ile yaklaşmanın yaratabileceği (olası) kaotik duruma dayanır.

Böyle bir bakış açısı ile genişletilebilecek projelerin olası ek faydaları ise aşağıdaki gibi ifade edilmeye çalışılmıştır:

- Gereksinimler doğrultusunda ortak bilgi paylaşım platformunun oluşturulması.
- Ortak bilgi işlem ve analiz platformu sayesinde önleyici ve engelleyici tedbirlerin etkin ve anında alınabilmesinin sağlanması,
- Risk değerlendirme yapılabilmesi, bu amaç doğrultusunda faydalanıcı kurumların etkin katılımının ve kullanımının sağlanması.

[62] Özben, M5, Age, s 20.
[63] John G. Voeller, "The Wiley Handbook of Science and Technology for Homeland Security", John Wiley & Sons, Inc., Hoboken, New Jersey, USA, 2010, s 3.

- Kurumların etkin katılımlarının kolaylaştırılabilmesi, dolayısı ile bu bütüncül yaklaşım ile, entegre güvenlik yönetimi konseptinde sürekli gelişim sağlanması
- Tehdit oluşumu öncesi, öncül tedbirlerin alınabilmesi için gerekli bilgi ve karar destek altyapısının tesisi
- Kurumsal gereksinimlerin ve olası müdahale planlarının gelişen şartlar doğrultusunda dinamik olarak değiştirilebilmesi için, sürekli gelişen ve kolay yönetilebilir bir sistem halinde olması.
- Olası ulusal ve uluslararası veri sistemleri ile (paylaşılabilir veriler kapsamında) entegre edilebilir bir sistem oluşturulması, dolayısıyla güvenlik yönetimine yönelik ulusal ve uluslararası bilgilerin değerlendirilebileceği ve ilgili kurumların da gerektiğinde kullanımına sunulabilecek ortak veri toplama ve analiz sisteminin oluşturulması.
- Ulusal ya da uluslararası gelişmelere bağlı dinamik gelişim yeteneğine sahip böyle bir sistem ile dâhili kurumların bilgi altyapılarının etkilenmediği ancak karşılıklı gerekli bilgilerin ulusal/uluslararası güvenlik doğrultusunda kullanılabildiği ulusal bir veri yönetim sisteminin kurulması.
- Kurumlar arası bilgi edinim ve yönetim sisteminde etkin örnek bir uygulama geliştirilmesi.
- Konu özelinde kurumsal eğitim ihtiyaçlarının da karşılanabileceği merkezi bir güvenlik bilgi yönetimi altyapısının oluşturulması.
- İzlenebilirlik ve etkinlik analizleri sayesinde, uluslararası platformda değerlendirilebilecek söylemlerin oluşturulmasında kritik bir altyapı edinimi.

Son olarak ve tekraren: ulusal güvenliğin bilgi unsuruna yönelik olarak kurumlar arası birlikte çalışabilirliğin tesis edilmesi, teknik, kurumsal, sosyal ve kültürel hazır bulunurluk, teknolojik pozisyon ve endüstriyel yetkinlikler gibi ilgili tüm kavramlar birlikte ele alındığında ve tehdit, tehlike, risk bilgileri her boyutta/düzlemde analiz edilerek önlemler alınabildiğinde artık tam anlamı ile bütünsel güvenlik bilgisi yönetiminden bahsedilebilecektir.

Sektörel Örnek Yaklaşımlar ile Anayurt Güvenliğinde Bilgi Yönetimi

Güvenlik Açısından Kesintisiz İletişimin Önemi

Haberleşme altyapısı, güvenliği tehdit eden her türlü durumda ülkenin en kritik hayat damarlarından biridir. Güvenliğin sağlanabilmesi adına gerekli koordinasyonun sağlanması, operasyon ve destek birimlerinin yönlendirilmesi, halkın bilgilendirilmesi ve hiyerarşik süreçlerin eksiksiz işleyebilmesi için kesintisiz bir iletişim altyapısı hayati öneme sahiptir. Örneğin, ilk yardım ve arama - kurtarma operasyonlarında, terör saldırıları veya halk ayaklanmalarında, kritik altyapı zafiyetlerinde vb. güvenliğin sağlanması ve yürütülmesi, ayrıca bu bağlamda kurumlararası ve kamusal bilgilendirme için haberleşme altyapısının kesintisiz olması gereklidir.

Konuyu bilgi edinim ve işlem açısından değerlendirdiğimizde örneğin deprem haritaları, analiz raporları ve tarihçesi, sel ve heyelan gibi tehditlerin yoğun olduğu bölgeler, çatışma veya terör saldırılarının tarihsel, coğrafi ve siyasi unsurları gibi tüm bilgiler ilgili tüm kurumlarımız tarafından hali hazırda edinilmekte, izlenmekte ve işlenmektedir. Bu kapsamda, belirsiz ancak gerçekleşme ihtimali olduğunu öngörebildiğimiz olası tüm güvenlik bileşenleri için hazır bulunabilmek ya da operasyonel sürdürülebilirlik için kesintisiz iletişim mutlak bir gerekliliktir.

Devlet unsurları, taktik, operasyonel ve stratejik yönetim planları ile güvenlik ilişkili temel hizmetleri yürütür. Doğal afetler, terör saldırıları, pandemiler ve bunun gibi olağanüstü durumlar, devletin temel fonksiyonlarının olağan işleyişini ciddi şekilde etkileyebilir. Güvenlik ilişkili konularda iletişim altyapısı kesintiye uğradığında, operasyonel süreçler, kurtarma ve risk azaltma faaliyetleri, kriz yönetimi ve halkın bilgilendirilmesi gibi önemli işlevler ciddi şekilde tehlikeye girebilir. Bu temel gerekçe, son dönemlerde yürütülen ulusal güvenliğie yönelik yerli ve milli bir iletişim sisteminin geliştirilmesi çabalarının da temelini oluşturmuştur.

Aşağıdaki örnek temel hizmetlerin, önlemlerin ve güvenlik tedbirlerinin tümünün ortak noktası (hangi güvenlik unsuruna ilişkin olduğundan bağımsız olarak), kesintisiz bir iletişime ihtiyaç duymalarıdır: İzleme, yönetme, devlet fonksiyonlarının devamlılığı, kurtarma ve yardım sağlama, kamusal bilgilendirme, kurumlararası etkileşim, uluslararası etkileşim vb.

Kurumların güvenlik yönetimi stratejilerinin ve planlarının önemli bir parçası olarak iletişim altyapısının korunması ve kullanılabilirliği kritik önemdedir. Bu strateji ve planlar, haberleşme ağlarının dayanıklılığını artırmayı, yedekleme ve çeşitlendirme senaryolarını içermelidir. Ayrıca güvenlik odaklı faaliyetlerde iletişimin nasıl yönetileceğini, kimlerin öncelikli erişim sağlayacağını ve kamuoyunun nasıl bilgilendirileceğini de içermelidir. İletişim altyapısının korunması, yedeklenmesi, iletişim önceliklerinin ve hiyerarşilerinin önceden belirli olması, güvenlik konulu iletişim modellerinin ve iletişim stratejilerinin senaryo tabanlı tatbikatlar ile doğrulanmasının bu bağlamda yürütülebilecek önemli çalışmalar olduğu değerlendirilmektedir. Kurumlarımız mutlaka bu kapsamlarda gereken faaliyet ve hazır bulunuşlarını yönetmektedirler ancak bu raporda hangi kurumun nasıl bir faaliyet yaptığı ya da yapmakta olduğunu analiz etmek yerine, Türkiye bilişim sektörünün bakış açısı verilmeye çalışılmaktadır. Süreçleri ve kurumsal yetkinlikleri tekraren ele almanın güvenlik bakışına, yaklaşımlarına ve kültürüne katkı sağlayacağı yorumlanmaktadır.

Güvenlik temeline dayalı iletişimin sürdürülebilmesi için yönetsel ve teknik önlemlerin alınması, yedek sistemlerin ve hızlı onarım stratejilerinin (her coğrafi bölge ihtiyaçları ve her kurum ihtiyaçları doğrultusunda) planlanmış olması önemlidir.

İletişim önceliklerinin belirlenmesi ve kritik iletişim hatlarının tanımlanması, bir güvenlik tehdidi ortaya çıktığında hangi adımların atılması gerektiği konusunda da önemli bir rehber niteliğinde olacaktır. Hangi iletişim türlerinin ve gruplarının öncelikli olduğunun belirlenmesinin ve güvenlik ilişkili olası tüm tehdit türleri için senaryolara dayalı olarak bu önceliklerin gözden geçirilmesinin önemli olduğu değerlendirilmektedir. Ek olarak, kamuoyu bilgilendirme yaklaşımları, basın açıklamaları ve güvenlik iletişimi stratejilerinin de önceden belirlenmiş olmasına ek olarak, bu stratejileri uygulamak için hangi durumda hangi altyapı ve teknolojilerin kullanılacağının da alternatif senaryoları ile birlikte planlanmış olmasının, güvenlik yönetimi için temel nitelikte bir gereksinim olduğu yorumlanmaktadır.

Türkiye için ULAK A.Ş. kamu güvenliği kapsamında önemli ürün, çözüm ve teknolojiler üzerine çalışmaktadır. Örnek olarak Kanada, Ulusal Acil Durum İletişim Sistemi (NEBS) adlı bir program yürütmektedir. Bu program, hükümetin, yerel yönetimlerin ve telekomünikasyon operatörlerinin işbirliği içinde iletişim altyapısının devamlılığını sağlamak için yapılması gerekenleri planlamaktadır. Singapur, Acil Durum Yönetim Ajansı (EMA) aracılığıyla kriz durumlarına yanıt vermek için acil durum planlarını ve tatbikatlarını koordine

eder. Tayvan, deprem ve diğer doğal afetlere karşı özel olarak tasarlanmış yeraltı iletişim merkezleri inşa etmiştir. Bu merkezler, haberleşme altyapısını koruma ve kurtarma ekiplerine iletişim sağlama konusunda kritik bir rol oynamaktadır. Avustralya'da, acil durum hizmetleri tarafından kullanılan özel bir haberleşme ağı olan Emergency Alert System (EAS), halka anında uyarılar ve bilgilendirme mesajları göndermek için kullanılmaktadır.

İletişim altyapısının kesintisiz çalışması, güvenlik yönetimi planlarının ayrılmaz bir parçası olduğu değerlendirilmektedir. Haberleşme ağlarının dayanıklılığını artırmak ve alternatif yollar sunmak da bu kapsamdadır. Güvenlik yönetimi planları ayrıca iletişimin hiyerarşisini de içerebilmelidir.

Bir ülkenin haberleşme altyapısının güvenlik ilişkili olağanüstü durumlara hazırlıklı olması, ulusal güvenlik, ekonomik istikrar ve toplumsal huzur açısından kritik bir öneme sahiptir. Bu nedenle, kapsama yönelik ihtiyaçlar daha geniş bir perspektifte ele alınabilmeli ve alternatif çözümler için sektör beklenti ve yetenekleri sürekli olarak gözden geçirilmelidir. Kamu otoriteleri bu konuda rehberlik etmeli ve ilgili tüm paydaşların alınacak tedbirlerin bir parçası olması sağlanmalıdır.

İletişim bağlamında yedek altyapının etkili olabilmesi için doğru ekipmanların seçilmesi ve düzenli bakımının yapılması gereklidir. Ayrıca yedek altyapı, ana altyapıdan farklı teknolojileri içerebilir. Bu, farklı senaryolara uyum sağlama ve kesintilere karşı daha dayanıklı bir iletişim ağı oluşturma açısından önemlidir. İhtiyaç halinde operatörlerin, servis sağlayıcıların birbirlerinin şebekelerine bağlanması gerekirse, ihtiyaç duyulabilecek farklı ürünlerin de acil durum stokları içerisinde tutulması önemlidir. Ticari ve teknik tercihlerle her operatör ve kamu kurumu farklı teknolojileri kullanmayı tercih edebilir. Güvenlik tehdit senaryoları için yapılacak planlamalarda ise diğer bir operatör veya kamu kurumunun şebekesine bağlantı gerekirse, kendi ürün stoklarından farklı bir ürün ile ara bağlantı yapmaları gerekebilecektir. Bu senaryolara hem teknik eğitim seviyesinde hem de farklı ürünleri yedek envanterlerinde tutmak şeklinde ön hazırlı olmak, güvenlik açısından ulusal düzeyde mücadelenin önemli bir parçasıdır.

Bunların yanı sıra operatörlerin kendi şebeke yedeklemeleri için farklı teknolojileri de eş zamanlı olarak kullanabilecek şekilde hazırlıklı olması, zaman yönetimi konusunda önemli bir katkı sağlayacaktır. Örneğin karasal transmisyon şebekelerine alternatif olarak uydu

bağlantısı ve mikrodalga linkler veya bunun tam tersi senaryolar ile yeterli kapasitede yedekleme yapılabilecek şebeke alternatifleri kriz anında devreye alınabilecek şekilde planlanabilir. Yedek altyapı için ayrıca güç kesintilerine karşı dayanıklı enerji kaynakları da sağlanabilmelidir. Kullanılacak olan kesintisiz güç kaynakları, jeneratörler ve bunların yakıt stokları ile lojistiği bunun yanında güneş panelleri, rüzgar tribünleri gibi alternatif enerji kaynakları ile yedeklemeler planlanabilir. Farklı enerji kaynaklarının operatörler tarafından kurulması ve işletilmesi konusunda gerekli hukuki ve regülatif düzenlemelere ihtiyaç duyulabilecektir.

Güvenlik tehdidinin türüne göre örneğin iletişim şebekelerine ek olarak enerji şebekelerinin ve/veya üretim tesislerinin de devre dışında kalması ihtimaline karşı, alternatif enerji kaynaklarına ve iletişim için jeneratör yakıtlarına öncelikli ve hızlı erişim sağlanması için gerekli hukuki ve teknik altyapının hazırlanmış olması da bir başka çalışma konusu olabilecektir. Taşınabilir yedek altyapıların alt merkezlerde ve güvenlik tehdidinin türüne göre ilgili yerlerde tutulması da bir başka alternatif çözüm yaklaşımı ve yeni nesil proje önerisi niteliğinde olabilecektir.

Özellikle 6 Şubat 2023 tarihinde yaşadığımız deprem felaketi, kritik altyapılarımızın ne derece önemli olduğunu gözler önüne sermiştir. Örneğin şehirlerde yer alan baz istasyonlarının büyük oranda bina çatılarında yer alması ve depremle beraber altyapının da çökmesi neredeyse tüm sistemi işlevsiz duruma getirme riski ortaya çıkarmıştır. Operatörlerin altyapı kuracakları binaları seçerken sadece imar durumlarını değil, teknik incelemeler ile örneğin doğal afetlere dayanıklılığını da bağımsız kurumlara kontrol ettirmesinin gerekli olacağı yorumlanmaktadır. Operatörler tarafından özellikle üzerinde çok sayıda transmisyon elemanı, mikrodalga link, uydu yer istasyonu vb içeren kule ve ünitelerde güvenlik ve dayanıklılık seviyesi standartları yükseltilmeli, kurumlarımız tarafından yedeklilik planları düzenli aralıklarla alınarak sorgulanmalıdır.

Ekonomi Güvenliği Açısından Örnek Değerlendirme

Ulusal güvenliğin herhangi bir seviyede ya da alanda tehdit edilmesi durumunda ele alınması gereken bir diğer önemli alan, ekonomik anlamda devlete verilebilecek olası doğrudan hasarlar ve bu hasarların yaratabileceği dolaylı etkilerdir. Güvenlik temelinde ekonomik etkilenmenin

büyüklüğünü, hacmini ve etkilerini değerlendirebilmek, olası negatif etkilere karşı hızlı ve etkin çözümler üretebilmek adına aşağıda verilen örneklerdeki gibi bazı verilere / veri türlerine ve daha altında ise bunları işleme, iletme, saklama modellerine ihtiyaç duyulabilecektir:

- Gayri Safi Yurtiçi Hasıla (GSYİH): Bir ülkenin ekonomik büyüklüğünü ve performansını ölçen temel göstergedir. GSYİH verileri, bir krizin ekonomi üzerindeki etkilerini anlamak için izlenir. Kriz döneminde GSYİH düşüşü veya negatif büyüme, ekonomik sıkıntıları gösterebilir.
- İşsizlik Oranları: İşsizlik oranları, iş gücü piyasasının sağlığını gösterir. Kriz dönemlerinde işsizlik oranlarının yükselmesi, ekonomik sorunların bir işareti olabilir.
- Enflasyon Oranları: Enflasyon, genel fiyat düzeylerinin artışını ölçer. Kriz dönemlerinde hiperenflasyon veya deflasyon gibi olağandışı durumlar oluşabilir. Enflasyon oranları ekonomik istikrarın göstergesi olarak izlenir.
- Merkez Bankası Faiz Oranları: Merkez bankası faiz oranları, para politikasının bir yansımasıdır. Kriz dönemlerinde merkez bankaları faiz oranlarını düşürerek ekonomiyi desteklemeye çalışabilir.
- Tüketici Harcamaları ve Perakende Satışlar: Tüketici harcamaları ve perakende satışlar, hane halklarının ekonomiye olan güvenini yansıtır. Kriz dönemlerinde tüketici harcamalarının azalması, ekonomik daralmanın bir göstergesi olabilir.
- Dış Ticaret Verileri: İhracat ve ithalat verileri, dış ticaret dengesini ve ülkenin uluslararası ticaret performansını gösterir. Kriz dönemlerinde dış ticaretteki daralma veya dengesizlikler önemli olabilir.
- Borç ve Kredi Verileri: Hane halklarının ve işletmelerin borç yükü, kriz dönemlerinde finansal zorlukların bir göstergesi olabilir. Kredi verileri, finansal sistemdeki sıkıntıları yansıtabilir.
- Endüstriyel Üretim ve İmalat Verileri: Sanayi üretimi ve imalat verileri, ekonominin üretim sektöründeki durumunu gösterir. Kriz dönemlerinde endüstriyel üretimdeki düşüşler ekonominin kötüye gittiğinin bir işaretidir.
- Yatırım Verileri: Özel sektörün yatırım aktiviteleri, ekonominin gelecekteki büyüme potansiyelini etkiler. Kriz dönemlerinde yatırımların azalması, ekonomik belirsizliği yansıtabilir.

- Bankacılık Sektörü Verileri: Bankaların likidite durumu, kredi verme kapasiteleri ve zarar durumları, kriz dönemlerinde ekonomik sağlık hakkında bilgi verir.

Veri işleme, iletme, saklama modelleri

- Etki Değerlendirmesi: Güncel ve doğru veriler sayesinde hasarın boyutu, üretim kayıplarını, istihdam düşüşünü, madde, hammadde stokları gibi ekonomik değerleri olan kalemlerin takibi yapılır.
- Toparlanma Planlaması: Tehdit sonrası toparlanma sürecinin planlanması hayati önem taşımaktadır. En çok etkilenen ve stratejik öneme sahip konumların üretim kayıplarının istihdam düşüşünün tespiti için veri ve veri analizlerinin yapılması gerekmektedir.
- Kaynak Yönetimi: Ekonomi, Kıt kaynakların alternatif kullanım olanaklarını inceleyen bir bilim dalıdır. (Robbins). Zaten sınırlı olan kaynaklar Kriz dönemlerinde daha ulaşılmaz hale gelmektedir. Mevcut verilerin analizi ile kriz dönemlerinde kaynakların etkin kullanılması, acil yardım yapılması konusunda hızlı karar verme olanağı sağlar.
- Politika ve Strateji Belirleme: Güvenlik tehdidinin savuşturulmasının ardından veriye dayalı yaklaşım etkin sonuçlar elde etmeyi sağlar. Vergi indirimleri, finansal yardımlar sonrasında alt yapı politikalarının belirlenmesinde veri önemli bir araçtır.
- Belirsizlik Azaltımı: Veri sayesinde kriz dönemlerinde tutarlı tahminler yapılarak doğru kararlar alınmasını sağlar.
- İletişim ve Bilgilendirme: Güvenliğin tehdidi, beraberinde doğru olmayan, endişe veren ya da kaos yaratabilen bir çok olayı da tetikler. Bu yüzden doğru iletişim kanalları kullanmak ve bilgilendirmeler yapmak paydaşlar açısından tehdidin boyutu, etkilerini anlamak için gerekli bir araçtır. Ve yine bu durum veri analizlerinin yapılarak doğru stratejilerin belirlenmesi sayesinde gerçekleşir.
- Uzun Vadeli Stratejiler: Yaşanan bir acil durumu sadece anlık olarak değerlendirmemek doğru bir yaklaşım olacaktır. Uzun vadede yaşanabilecek benzer krizlerde stratejilerin oluşturulması yine toplanan, elde edilen veri

sayesinde süreklilik sağlayacaktır. Bu veriler sayesinde benzer krizlerden korunma stratejileri geliştirilebilir.

- Uluslararası işbirliği: Gerekli durumlarda uluslararası yardım ve dayanışma sağlanabilmesi acil durum dönemlerinde sağlanabilecek anlık ve doğru veri ile sağlıklı yürütülebilir. Bu koordinasyon, lojistik ve operasyon konularında hayati önem taşımaktadır.

Yukarıdaki veriler ve veri kullanımı yaklaşımlarının, ekonominin genel sağlığı ve ekonomi güvenliğine tehdit oluşturabilecek etkileri anlamak için önemlidir. Kriz yönetimi ve kriz sonrası toparlanma stratejileri oluştururken bu veriler kullanılarak daha etkili kararlar alınabilecektir.

Ekonomik güvenlik açısından yurt savunması ve verilerin bir kaynaktan yönetilmesi, etkili güvenlik ve kriz yönetimi stratejileri geliştirmek için kritik bir rol oynar. Bu yaklaşım, tedbir alma süreci, müdahale süreci ve tesir azaltma süreci gibi alt başlıklarda da verilerin toplanmasını, paylaşılmasını, analiz edilmesini ve yönetilmesini içerir. Bu sürecin nasıl işleyebileceğine dair temel adımlar aşağıda örneklenmektedir:

- Merkezi Veri Yönetimi Sistemi Oluşturma: Ekonomi güvenliği temelinde bir merkezi veri yönetim sistemi oluşturulmalıdır. Bu sistem, farklı veri türlerinin toplandığı, saklandığı, güncellendiği ve paylaşıldığı bir platform olabilir. Bu platform, bir veri ambarı veya coğrafi bilgi sistemi (CBS) gibi teknolojik altyapılarla desteklenebilir.
- Veri Toplama Protokolleri: Veri toplama protokolleri oluşturulmalıdır. Hangi tür verilerin ne zaman, nasıl ve hangi yöntemlerle toplanacağı belirlenmelidir. Bu protokoller, saha çalışanlarına ve veri toplayıcılarına rehberlik eder.
- Veri Standardizasyonu: Toplanan verilerin standart bir formatta olması önemlidir. Bu, verilerin daha kolay analiz edilmesini, karşılaştırılmasını ve paylaşılmasını sağlar. Coğrafi koordinatlar, birimler, zaman damgaları gibi standartlar belirlenmelidir.
- Gerçek Zamanlı Veri Aktarımı: Verilerin gerçek zamanlı olarak aktarılması önemlidir. Mobil uygulamalar, sensör ağları, uzaktan algılama teknolojileri gibi yöntemlerle veriler hızla toplanıp merkezi sistemde işlenebilir.

- Veri Analizi ve Modelleme: Toplanan veriler, analiz edilerek olası etkilerin önceden tahmin edilmesi, etkilerinin modellenmesi ve risk değerlendirmelerinin yapılması için kullanılabilir. Veri madenciliği, istatistiksel analiz ve yapay zekâ gibi yöntemler bu aşamada kullanılabilir.
- Veri Paylaşımı ve İletişim: Veriler, ilgili paydaşlarla (kamu kurumları, özel sektör, sivil toplum kuruluşları) paylaşılmalıdır. Bu, etkili bir koordinasyon ve işbirliği sağlayarak daha iyi bir güvenlik yönetimi sağlar.
- Karar Destek Sistemleri: Veriler, karar vericilere gerçek zamanlı bilgi sağlamak için kullanılabilir. Karar destek sistemleri, hızlı ve etkili müdahaleleri destekleyebilir.
- Topluluk Katılımı ve Farkındalık: Verilerin toplanması ve paylaşılması sırasında toplulukların ve bireylerin katılımı önemlidir. Halkın güvenlik yönetimine ilişkin farkındalığı artırılmalı ve veri toplama süreçlerine dâhil edilmelidir.
- Veri Güvenliği: Toplanan verilerin güvenliği ve gizliliği sağlanmalıdır. Hassas bilgilerin korunması ve yetkisiz erişimin engellenmesi gereklidir.

Bu yaklaşım, güvenlik yönetiminin daha veri odaklı, hızlı ve etkili bir şekilde yürütülmesine yardımcı olabilir. Teknolojik araçların ve uygun altyapının kullanılması, verilerin yönetimi ve paylaşımının daha kolay hale gelmesine katkı sağlayabilir.

Güvenlik Odaklı Bilgi Yönetiminde Akıllı Karar Destek Sistemleri

Karar destek sistemleri yöneticilere karar vermelerinde yardımcı olmak üzere kurulmuş sistemlerdir[64]. Karar destek sistemlerinde esas olan kararın alınması değil, kararın alınmasına destek olmaktır. Karar destek sistemleri eldeki bilgilerle problemleri analiz edip çözmeye çalışır. Karar destek sistemleri, karar verme süresi boyunca karar vericinin verileri bulup çeşitli çözümleri denemesine imkân sağlar.

Karar destek sistemleri özelikle yarı-yapılanmış (semi-structured) ve yapılanmamış (unstructured) kararların alınmasında yardımcı olurlar. Karar destek sistemleri tüm kademelerdeki yöneticilere karar vermelerinde yardımcı olmalıdır. Karar destek sistemleri

[64] TÜRKİYE BİLİŞİM DERNEĞİ Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu Bilişim Platformu XII KAMUDA KARAR DESTEK SİSTEMLERİNİN KULLANIMI VE BİR MODEL ÖNERİSİ www.tbd.org.tr

karar alma sürecinin tüm evrelerinde destek sağlamalıdır. Karar destek sistemleri çeşitli karar verme süreçlerine destek sağlamalıdır; fakat bunlardan birine bağlı olmamalıdır. Karar destek sistemleri bağımsız kararları desteklediği kadar, birbirine bağlı kararları da desteklemelidir. Karar destek Sistemleri'nin kullanım kolaylığı olmalıdır.

Karar destek sistemlerini kullanan firmalar kullanmayanlara oranla daha avantajlıdır. Bu avantajlar şöyledir[65]: Verimlilik daha yüksektir. verimlilik daha kararlıdır, zaman içinde daha az değişiklik gösterir. Karara ulaşma süresi daha kısadır. Daha fazla alternatif gözönünde bulundurulur. Kararlarını gerekçeli olarak açıklayabilme olanağına sahiptir. Karar alma durumu üç seviyede gerçekleşir[66]:

- Stratejik karar verme seviyesi
- Taktik karar verme seviyeleri
- Operasyonel karar verme seviyeleri

Karar Destek Sistemine İhtiyaç Duyulması kamuda mevcut iş süreçlerinde verilen kararların doğru olmaması halinde karar vericiye doğrudan bir maliyetin yansımaması, yürütülen süreçlerde etkinlik ve verimlilik kavramalarının sistematik bir şekilde takip edilerek kurumsal performansa katkısının ortaya konamaması ve hatta kurumsal performansın objektif değerlere dayalı olarak ölçümlenememesi nedenleri ile kullanıcıların karar destek sistemlerini kullanma ihtiyacı içinde olmadıklarını ifade etmek ve bu ihtiyacın ortaya konabilmesi için sabırlı çalışmalar yapılmasını vurgulamaktadır.

Karar vericilerin karar vermelerine yardımcı olmaya yönelik olan kantitatif yaklaşımlar, karar ortamının matematik-istatistik modelini kurmak ve model üzerinde işlem yapmayı kapsar. Karar sürecine kantitatif analizlerin de katılmasının nedeni, daha iyi-daha etkin karar vermede yardımcı olmasıdır. Karar almaya yardımcı olmak amacıyla kullanılan kantitatif model kurma-uygulama süreci aşağıdaki aşamalarda özetlenebilir:

- Karar probleminin belirlenmesi,
- Problemin formüle edilmesi,
- Model kurma,

[65] http://www.geocities.com/akircali/planlama/planlama.html#21
[66] TÜRKİYE BİLİŞİM DERNEĞİ Kamu Bilgi İşlem Merkezleri Yöneticileri Birliği Kamu Bilişim Platformu XII KAMUDA KARAR DESTEK SİSTEMLERİNİN KULLANIMI VE BİR MODEL ÖNERİSİ www.tbd.org.tr

- Bilgi derleme,
- Modelin çözümü,
- Modelin geçerliliğini araştırma ve duyarlılık analizleri,
- Sonuçların yorumu ve
- Karar verme, uygulama ve kontroldür.

Endüstri, yönetim ya da teknik işlerde insan emeğinin yer almadığı, üretimde yer alan hizmetlerin bir kısmı ya da tamamının makinelere bırakıldığı süreç otomasyon olarak adlandırılmaktadır. İnsan emeğinin yoğun bir şekilde yer aldığı otomasyon sistemleriyse yarı otomasyon olarak bir kavram haline gelmiştir.

Son 25 yıl içerisinde bilgi teknolojilerindeki gelişmelere bakıldığında ilk yıllarda en büyük önemin "veri toplanması" na verildiği söylenebilir. Yıllar boyunca verinin toplanması yönündeki yatırımlar hızla artmış, bu da verinin toplanması ile ilgili teknolojik gelişmeleri daha da hızlandırmıştır. Buna paralel olarak toplanan verilerin saklanması ve güvenliği ile ilgili teknolojik gelişmeler de aynı hızla gerçekleşmiştir. Verilerin, bilgiye dönüşmesi ve ardından yöneticilerin vereceği kararlara temel sağlaması asıl hedef olduğundan, büyük miktarlarda toplanan verilerin arşivlenmesi, sorgulanması ve onlardan rapor üretilmesi gündeme gelmiştir. Günümüzde ise toplanan verilerin bir arada tutulabilmesi, ayrıştırılabilmesi, derlenmesi ve anlamlı bir hale getirilerek raporlanmasının önemi fark edilmiştir.

Yöneticilerin, kurumlarıyla ilgili strateji belirlemeleri, politika üretmeleri ve ihtiyacı olan bilgilere anında erişebilmeleri amacıyla ihtiyaç duydukları akıllı karar destek sistemleri, iş zekâsı (Business Intelligence) kavramı tarif etmiştir. İş zekâsı, veri sürümlü KDS kapsamında yer alan ve kurumda oluşan operasyonel veriyi, amacına uygun ve kullanışlı bilgiye transfer ederek kullanıcılara sunulması işlemini gerçekleştiren bir uygulamadır.

Akıllı karar destek Sistemleri Uygulamaları[67], dijital çekirdekte başlayan akıllı işletmeler, süreç otomasyonu ve inovasyonu teşvik ederek, yeni büyüme alanları açarak ve olağanüstü deneyimler sunarak tüm iş kollarında verileri eyleme dönüştürmeyi sağlayan bir stratejidir.

[67] https://www.vektora.com/Cozum/akilli-isletmeler

Bir karar probleminin matris formu ile belirlenmesi beş farklı karar problemini oluşturur[68]. Ayrım, ortaya çıkması beklenen olaylara göre yapılır ve karar verenin olaylar hakkındaki bilgi derecesini yansıtır. Olaylar ve gerçekleme olasılığı arasındaki ilişkiyi tanımlayan bu ayrım aşağıdaki gibidir:

- Belirlilik hâlinde karar verme,
- Risk hâlinde karar verme,
- Belirsizlik hâlinde karar verme,
- Kısmi bilgi hâlinde karar verme ve
- Rekabet hâlinde karar verme (Oyunlar).

Yirminci Yüzyılın ortalarında görülen en önemli bilimsel gelişmeler içinde üst sırayı doğrusal programlamadaki gelişmeler almıştır. Dünyadaki çoğu şirketlerin bilgisayar kullanımıyla, 1950'lerden itibaren doğrusal programlamanın şirketlerin iş yaşamına etkisi olağan üstü olmuştur.

Günümüzde binlerce değişkenli ve binlerce kısıtlayıcılı problemler, bilgisayar yardımıyla çözülebildiğinden, doğrusal programlamanın uygulama alanı sadece kıt kaynakların dağıtımı ile sınırlı kalmamış, diğer birçok alanda da önemli uygulamalar olmuştur. Bu konuda şu örnek liste verilebilir: Personel programlaması, Beslenme (diyet) problemleri, Üretim planlaması ve envanter kontrolü, Ulaştırma ve lojistik problemleri, Atama problemleri, Tarımsal planlama, Hava kirliliğinin kontrolü, Sermaye bütçeleme problemi, Kısa dönemli finansal planlama, Dinamik yatırım planlaması, Reklam seçimi problemleri, Portföy seçimi problemi ve Karışım problemleridir.

Çoğu operasyonel kararın makinelerle verildiği bu teknoloji tabanlı model, şirketlerin hızlı değişen pazar koşullarına ve müşteri tercihlerine uyum sağlamasına; iş ortaklarıyla birlikte hızlı hareket edebilme kabiliyetiyle geleneksel işletmelere karşı güçlü bir rekabet avantajı kazanmasına olanak sağlar[69]. Akıllı işletmeler, veriyi yapay zeka ile süreçleri otomatize etme, müşterilerini etkileme, çalışanları kuvvetlendirme ve tamamen yeni gelir imkanları elde etme yoluyla, sadece ölçme ve değerlendirmenin ötesinde kullanır.

[68] İstanbul Üniversitesi Açık ve Uzaktan Eğiti m Fakültesi Karar alma Teknikleri PROF. DR. ERCAN SARIDOĞAN
[69] https://dergipark.org.tr/en/download/article-file/1115277

Teknoloji, bir araç olarak insan yaşamında önemli bir role sahiptir. Uzun insanlık tarihi sürecinde teknoloji, bir yandan karşılaşılan sorunların üstesinden gelmeyi sağlayan bir araçken, diğer taraftan da iş yapma biçimlerimizi ve genel olarak yaşamımızı kolaylaştıran bir işleve sahip olmaktadır. Belirli bir dinamizm içinde yaşanan teknolojik gelişmeler, bireysel alandan toplumsal alana, mekânsal düzlemden örgütsel düzleme yeni biçimler/boyutlar kazandırmaktadır. İfade edilenler bağlamında teknolojinin etki alanındaki en önemli mekânlardan biri de kentlerdir. Buhar Makinesinden bu yana ortaya çıkan teknolojik gelişmeler, kentlerin yaygınlaşmasında aracı bir rol üstlendiği gibi, kentler de barındırdıkları imkânlarla teknolojilerin gelişimine katkı sağlamaktadır. Bu döngü sürüp gitmektedir.

Farklı alanlarda gerçekleşen bilimsel çalışmaların etkisiyle birçok teknolojik gelişmelerin yaşandığı bilinmektedir. Fakat ortaya çıkan bazı teknolojiler, ihtiyaç duyulan bağlamının dışında, farklı konu ve alanlarda geniş bir etki alanına sahip olmaktadır. Bu anlamda 21. yüzyılda etki alanı açısında en önemli teknoloji internettir. Sahip olduğu nitelikleriyle internet; bireysel, toplumsal, kurumsal, iktisadi, vb. alanlarda birçok meseleyi dönüşüme uğratmaktadır. 1990'lı yıllarda kullanım pratiğinin yaygınlaşmasıyla internet, ilk etapta, iletişim odaklı olarak; birey-birey, birey-örgüt veya örgüt-örgüt arasındaki mekânsal sınırlılıkların aşılmasına katkı sağlamıştır. İkinci etapta internet, daha çok mal ve hizmetlerin sunumunun yapıldığı bir tüketim aracına dönüşmüştür. İnternet, ifade edilen bu işlevlerini artırarak devam ettirmektedir. Diğer taraftan yaşanan gelişmeler internete yeni bir boyut kazandırarak, nesneler ile bireyler/kurumlar arasındaki sınırların aşılmasına katkı sağlamıştır. Farklı nesneler ile internetin birbirine entegre edilmesi, nesnelerin interneti (Internet of Things, IoT) kavramı ile karşılık bulmaktadır. IoT, tanıma/algılama, ağ ve uygulama bileşenlerinden oluşmaktadır. Nesnelerin internetini tamamlayan bir diğer teknoloji ise sensörlerdir. Sensörler, ses, ışık, ağırlık, hareketlilik gibi duyarlılık özelikleriyle farklı nesne ve alanlarda karşılık bulmakta ve büyük verinin ortaya çıkmasında aracı bir konuma sahip olmaktadır. Bu bağlamda nesnelerin interneti ve sensörler, birbirini tamamlayan bir niteliğe sahiptir. 2016 yılı sonu itibariyle dünya genelinde kullanılması beklenen bağlantılı nesne sayısı 6,4 milyar ve her gün bağlantısı sağlanan yeni nesne sayısı ise 5,5 milyon olarak bilinmektedir. Nesnelerin interneti ve sensör teknolojileriyle birlikte; mobil telefonlar, büyük veri, bulut gibi teknolojilerin karşılık bulduğu nesneler ve mekânlar, akıllı (smart) kavramı ile nitelendirilmektedir. İnsanların zihinsel yapısına referansla gündeme getirildiği anlaşılan akıllı kavramının nesnelere ve

mekânlara yansıması, sensör teknolojisinde ortaya çıkan verilerle birlikte gündeme gelmektedir.

Teknolojide ortaya çıkan yeni gelişmelerle birlikte "akıllı (smart)" kavramı, bir ön ek olarak birçok konuda (akıllı mahalle, akıllı sokak, akıllı müze, akıllı park, vb.) karşılık bulmaktadır.

Karar vericiler ister merkezi yönetim olsun ister yerel yönetim olsun her gün yüzlerce karar verme durumu ile karşı karşıya kalmaktadır. Özel şirket sahipleri, STK yöneticileri veya birey ve aile üyeleri aynı durumdadır. Günümüz teknolojilerinde henüz insan beyni gibi bilişim sistemi tarafından tam karar verip uygulama aşamasında olan bir yapı henüz yoktur. Verilen verileri işleyip bir sonuç çıkarmaktadır. Örneğin Finans, Enerji, Eğitim, Eğlence, Ulaşım, Şehir, Sağlık, Kamu, Tarım, İletişim gibi bilişim teknolojileri ile akıllı hale getirilmektedir.

1927 yılında ülkemizde kent nüfusu %24,2 iken 2015 yılında %92,1 olmuştur. 85 milyon olarak dikkate alındığında 78 Milyon Nüfusumuz şehirlerde yaşamaktadır. Bu da sorunların çözümünden merkezi yönetim den yerel yönetimler üzerinde kalmaktadır. Yaklaşık 10 milyon nüfus 75 milyon nüfusun tarımsal ihtiyaçlarını karşılamaktadır.

Göç meselesi yine aynı şekilde ülkemizin bir göç yolu üstünde olması Kuzey kürenin zenginliğinden faydalanmak isteyen güney kürede yaşayan Afrika sahra altında yaşayanlar ve Güney Amerikalılar kuzeye doğru bir göç halindedir. Yerel göçle birlikte uluslararası göç de ayrı ayrı incelenmesi gerekmektedir.

Yine barınma sorunu bu yüzyılda şehirlerin yapılaşmasında imar sorunları ile karşı karşıya kalmamıza neden olmakta. Yapılan imar planları ya fazla kapasite de planlanmakta ya da eksik kapasite planlanmaktadır. Ya da hiç plan yapılmadan gecekondu, teneke ev gibi yapıların daha sonra ıslahı ve alt yapının sonradan yapılması şeklindedir. Dere kenarına ev yapmak, fay hattı üstüne veya yakını konut yapmak, gibi çeşitli sorunların yanında kontrolsüz gelişen şehrin varoşlarında asayiş ve benzeri olayların yaşanmasına olanak sağlamaktadır.

Yine tabii afetler deprem gibi sel baskını yanında biyolojik hastalık sorunları ile ülkemiz her an farklı olaylarla karşı karşıya kalabilmektedir. Dünya nüfusunun %55 kentsel alanlarda yaşaması insan ilişkilerinin daha yakın olmasına neden olmaktadır. Bu ise afet çeşitliğinin artmasına neden olmuştur. Afet kayıplarının kalkınmada üzerine etkisi çok fazladır.

İklim değişikliği ve iklimin yaşantımızdaki etkisi her geçen gün etkisini artırmakta ve iklim ile baş etmek, iklim koşullarına göre yaşamak değil tabiatın ayarları ile oynamamak gerekmektedir. Sera gazları etkisi her geçen gün gökyüzüne salına karbondioksit gazları ile ormanların yok oluşu dünya ikliminde değişikliklere neden olmaktadır. Bugün dört mevsim yaşayan ülkemizde mevsimler yazdan kışa, kıştan da yaza doğru dönmektedir. En güzel mevsimler ilkbahar ve sonbahar yok olmaya başlamıştır. Dünya sıcaklığının +2 derece artması halinde kıyamet senaryolarından bahsedilmesine neden olacaktır. İklim değişikliği tetikleyen konulardan birisi de enerji kullanımıdır. Fosil yakıtların doğaya salınması, Elektrikli otomobil dönüş olsa da şimdilik mesafelerin yeterince çözüme bulunmayışı da karbon salınımında kurtulmanın yolu 2035 ve sonrasında bu teknolojinin gelişmesine bağlıdır. Yine binalarımızı nasıl ısıtıyoruz veya nasıl soğutuyoruz. Fosil yakıtların en kullanışlı yanı taşınabilirlik olmasıdır. Bu ise güneş paneli çiftlikleri, rüzgâr santralleri önündeki en önemli sorunlardır.

Gıda arzı ise her geçen gün gıdaya ulaşmak oldukça maliyetli bir hal almaktadır. İstanbul'un günlük gıda ihtiyacı 76 ilden karşılanmaktadır. Günlük 270 adet Kamyon Tır İstanbul'a sebze ve meyve taşımaktadır. Şehirlerimiz çevresindeki tarım her geçen gün bitmekte ve tarım arazileri imara açılmaktadır.

Artık her türlü karar alıcılarının da Yönetim bilişim sistemleri kullanarak akıllı teknolojileri de entegre ederek Akıllı Karar Destek Sistemlerini üzerinden alınacak verilere göre Acil Durumlarda Bilgi Yönetimi yapısını kurması gerekmektedir. Karar aşamalarında verinin düzenli olarak acık veri kaynaklarından veya girişini sağlayarak büyük veri ve yapay zeka analizi yapılarak kararların alımında yan bir destek olacaktır. Duygusal veya nicelik kaynaklardan ziyaden nitelikli kaynaklardan alınan veri ile destek sağlanmış olacaktır.

Hangi krize hangi politikalar sunulacak, bunların tespiti, uygulaması yanı sıra planla, uygula, kontrol et, önlem al, (PUKÖ döngüsü) ve SWOT analizinin de kullanılması gerekmektedir.

Nüfusun artışının planlanmasının yanında kentlerin yaşam kalitesinin yükseltilmesi, gıda arzının önemi, iklim değişikliği azaltacak önlemler alınması, hava kirliliğinin azaltılması, yerleşim alanlarının seçimi, göç ve göçün nedenleri, anayurt güvenliği bağlamında akıllı karar destek sistemleri ile kontrolü sağlanabilecek ya da izlenebilecek örnek alanlardır.

Yeni Nesil Olası Proje Önerileri ve Sonuç

Kapsam dâhilinde olası çalışma / tartışma başlıkları aşağıdaki maddelerde özetlenmiştir. Bu maddeler, ulusal güvenlik için (sektör bağımsız ve bilginin tek tek katmanlı ve boyutlu olduğu varsayımından ziyade çok katmanlı ve çok boyutlu olarak ele alınması gerektiğine yönelik yaklaşım doğrultusunda) kurumlararası birlikte çalışabilirlik esaslarını da temel alan bir bakış altında, bilginin edinimi, işlemi ve korunumu kapsamında ele alınmış ve listelenmiştir:

- Güvenlikte bilgi ve veri türleri
- Güvenlik yönetiminde bilginin niteliğinin ve niceliğinin korunumu
- Bilginin senaryo temelinde ve türlere dayalı edinim çeşitleri
- Güvenlik ihlali durumlarında bilginin / verinin iletim ve korunum alternatifleri
- Birikimli bilginin (zamana sari toplanan, envanter ve yetkinlik odaklı) güvenlikte yeri
- Yerel ve genel karar alıcılar açısından bilginin dağıtım hiyerarşisi
- Hiyerarşi temelinde bilginin dağılımı ve dağıtımı modelleri (yönetsel ve teknik başlıklarda)
- Bilginin yerelde ve genelde karar destek unsurları tarafından kullanımı
- Yerelde ve genelde kullanılması önerilen karar destek mekanizmaları çeşitleri
- Büyük veri, IoT, Yapay Zekâ vb. teknolojilerin güvenlik yönetimi için anlamı ve gereği
- Bilginin işlenmesi için dağıtık ve merkezi mimari yapılarda gelişim / değişim / inovasyon
- Birbirleri ile etkileşimde olabilen güvenlik bileşenlerinin bulunması durumunda çoklu bilgi / veri etkileşimi ve dolayısıyla karar destek sistemlerini etkileme açısından analiz modeli
- Güvenlik yönetiminde yerel ve genel envanter ve yetkinlik veri tabanı
- Güvenlik yönetiminde gerçek zamanlı yerel ve genel envanter yönetimi
- Yerel ve genel envanter yönetiminde zafiyet ve eksiklik saptama ve proaktif karar alma yöntemleri
- Gerçek zamanlı karar alma ve kaynak aktarma sistemlerinin geliştirilmesi
- Çalışmalarda ulusal veri sözlüğünün ve ulusal coğrafi bilgi sisteminin kullanımı

- Yerel ve genel politikaların geliştirilebilmesi için analiz modellerinin geliştirilmesi
- Önerilenler yerel ve genel politikalar ve bilgi temelinde anlamı ve önemi
- Envanter ve yetenek yedeklilik, çoklu kullanım (insan / araç, vb.) alternatifleri
- Görselleştirme ve senaryolaştırarak müdahale yöntemleri için kavramsal denemeler

Rapor başlığının kapsayabileceği değerlendirilen yeni nesil projelere bir grup örnek aşağıda verilmeye çalışılmıştır. Bu örneklerden bazıları, kurumların hali hazırda yürüttükleri ve işlettikleri projeleri de içeriyor görünebilecektir. Bu durum, raporun yaklaşımı altında olağan olarak kabul edilmektedir çünkü kurumlarımızın kendilerine has ulusal güvenlik odaklı projeleri genellikle kapalıdır, detayları açık değildir. Bu sebeple okuyucunun ya da kurum temsilcilerinin zaten kurumlarımızda var olan yetkinliklere bu raporda yeni bir proje gibi değinilmesini gereksiz bulabileceği yerler olacaktır. Bu gibi yorumlar için, raporun sadece güncel bir sorunu bilişim ve iletişim sektörünün bakışı altında bir deneme olarak ele aldığı tekrar vurgulanmaktadır.

Anayurt güvenliği temelinde yeni nesil bir grup örnek bilgi ve iletişim sektörü olası projeleri aşağıda listelenmiştir:

- Güvenlik temelinde iletişim planlama ve yönetimi,
- Farklı operatörlerin iletişim ağlarının entegrasyonu,
- Ana transmisyon hatlarının ortak kullanım için ve yedeklilik mimarisinde gözden geçirilmesi,
- Mükerrer ağların bir envanterinin çıkarılması,
- Alternatif iletişim rotalarının otomatik tespiti ve ihtiyaç anında otomatik olarak aktive edilmeleri için ulusal bir ağ izleme ve merkezi yönetim sisteminin tesisi,
- Güvenlik tehditleri doğrultusunda merkezi iletişim sistemlerinden ayrılabilecek olası alt bölgelerin, en azından kendi içerisinde işler durumda tutulabilmesinin sağlanabilmesi için yerel alt ağlar iletişim merkezlerinin olası faydalarının tartışmaya açılması
- Güvenlik odaklı iletişim simülasyon sistemlerinin de destek unsuru olarak tesis edilmeleri,

Güvenlik ilişkili konular doğrultusunda kritik kamu kurumlarının tamamı için (veya adına) daha merkezi ve korumacı bir yaklaşımın tesis edilebileceği de yorumlanmaktadır. Öte yandan kurumların bu bağlamda birlikte çalışabilirlik esaslarının yeniden gözden geçirilmesi, eğitim planlamalarına kamusal ortak güvenlik bileşenlerinin dâhil edilmesi, kurumların ayrı ayrı sahip olduklarına ek olarak bütüncül güvenlik risk analizi ve yönetimi yapısının merkezileştirilmesinin de yeni nesil kritik projelerden olacağı değerlendirilmektedir.

Ek 1.

Çalıştay Değerlendirmeleri

Ek 2.

Engellilerin Bilgiye Erişimi ve Olağanüstü Durumlarda Alınabilecek Tedbirler