KİTAP ÖZETİ

The Coupling of Safety and Security

Exploring Interrelations in Theory and Practice

Editörler: Corinne Bieder & Kenneth Pettersen Gould

SpringerBriefs in Safety Management | 2020 | 11 Bölüm

ENAC, Université de Toulouse | University of Stavanger | https://doi.org/10.1007/978-3-030-47229-0

Dr. Öğr. Üyesi Ebru BAĞÇI

Kitabın Genel Çerçevesi ve Yapısı

Neden Bu Kitap Yazıldı?

- Emniyet (safety) ve güvenlik (security) yönetimi giderek kesişiyor
- 9/11 sonrası güvenlik, endüstriyel yönetimin merkezine girdi
- İki alan farklı kurumsal geçmişe sahip: farklı eğitim, teknoloji, düzenleme
- Yöneticiler iki ayrı yapı mı yoksa birleşik yönetim mi sorusunu cevaplamak zorunda
- Araştırma literatüründe büyük boşluk: pratikte nasıl birlikte yönetiliyorlar?
- Küreselleşme ve dijitalleşme her iki alanı da daha sistematik risklere bağlıyor

Kitabın 3 Ekseni

- KAVRaMSAL EKSEN: Tanımlar, benzerlikler, farklılıklar — Bölüm 1, 2, 5
- TEKNİK & METODOLOJİK: Mühendislik araçları, oyun teorisi, tasarım — Bölüm 3, 4, 6
- YÖNETİM & PRATİK: Operasyonel gerilimler, kültür, işyeri — Bölüm 7, 8, 9, 10
- Son bölüm (11): Sentez — araştırma ve yönetim zorlukları
- 11 yazar, farklı disiplinler: mühendislik, sosyoloji, organizasyon, havacılık, güvenlik bilimi

Temel Gerilim

- Emniyet: açıklık, paylaşım, şeffaflık
- Güvenlik: gizlilik, kısıtlı bilgi, güvensizlik
- İkisi aynı anda nasıl yönetilir?
- Ortak: kayıp önleme, risk yönetimi
- Ayrışan: kötü niyetin varlığı, belirsizliğin doğası, mesleki bilgi tabanı

Emniyet (Safety) = kasıtsız tehlikeler | Güvenlik (Security) = kasıtlı/kötü niyetli tehditler | Risk = ikisini kapsayan üst çerçeve

BÖLÜM 1

Emniyet ve Güvenlik: Bir Araya Getirmenin Zorlukları

Kenneth Pettersen Gould & Corinne Bieder | Stavanger & Toulouse | BÖLÜM 1/2

Tarihsel Gelişim

- Emniyet: 1970'lerden itibaren endüstriyel güvenliğin temeli. Enerji, kimya, ulaşım sektöründe köklü kurumsal yapı.
- Güvenlik (Security): Soğuk Savaş döneminde devlet güvenliği = askeri boyut. Sivil sektörde ikincil öneme sahipti.
- Kırılma noktası: 11 Eylül 2001. TSA kuruldu, EASA güvenlik yetkisi aldı. Güvenlik artık sivil havacılığın merkezine girdi.
- Bugün: Her iki alan da 'sistematik risk' kavramıyla buluşuyor. Küresel olaylar yerel savunmasızlıkları etkiliyor.
- Kritik altyapılar (enerji, havacılık, nükleer) hem en yüksek emniyet hem de en yüksek güvenlik gereksinimlerine sahip.

3 Yaklaşım Ekseni ve Yönetimsel Soru

- 1. KAVRAMSAL: Tanımlar, benzerlikler, farklılıklar (Blokland & Reniers; Jore)
- 2. TEKNİK/METODOLOJIK: Mühendislik araçları, yöntem entegrasyonu (Leveson; Wipf; Bongiovanni)
- 3. YÖNETİM/PRATİK: Örgütsel kültür, operasyonel zorluklar (Brooks&Coole; La Porte; Schulman; Boustras)
- Kritik soru: İki ayrı birim mi yoksa birleşik yönetim mi? Organizasyonlar tereddüt içinde.
- Araştırma açığı: Veri paylaşımı — güvenlik araştırmaları gizliliği zorunlu kılarken emniyet araştırmaları maksimum açıklığı hedefler.

Bölüm 1, kitabın giriş bölümü olarak kavramsal haritayı çizer ve sonraki 10 bölümü koordine eden çerçeveyi sunar.

Kavramsal Ayrımlar ve Sosyal Beklentiler

Emniyet ≠ Güvenlik: İki Temel Tanımlama Aksı

Kasıtlılık Ekseni

Emniyet: Kasıtsız/kazara riskler (süreç arızaları, insan hatası, doğal tehlikeler)
Güvenlik: Kasıtlı/kötü niyetli tehditler (sabotaj, terör, siber saldırı)

Sistem-Çevre Ekseni

Emniyet: Sistemin çevreyi etkilememesi (kimyasal kaçak, kaza)
Güvenlik: Çevrenin sistemi etkilememesi (dışarıdan saldırı)
Ek boyut: Sistemin kendisini zarardan koruması (iç sabotaj)

Gri Alan: Kasıtlılık Her Şeyi Açıklamıyor

İş güvenliği ihlalleri

Emniyet ekipmanını kasıtlı takmayan işçi → emniyet mi, güvenlik mi? Kasıtlılık var ama kötü niyet yok.

Germanwings 9525 (2015)

Yardımcı pilot kapıyı kilitledi ve uçağı dağa sürdü. Emniyet prosedürü (kilitleme) güvenlik tehdidi yarattı.

Dijitalleşme ve siber

OT sistemlerdeki güvenlik açığı hem emniyet hem güvenlik riski. İki alan birbirini besliyor ve zayıflatabiliyor.

"Gri alan daha önce bir kaza ile suç eylemi arasındaki farkı belirlemeye indirgenebilirdi; artık bu tanım yetersiz." — Pettersen Gould & Bieder

BÖLÜM 2 — Risk, Emniyet ve Güvenlik: Kavramsal Temel [1/2]

Peter J. Blokland & Genserik L. Reniers | TU Delft & KU Leuven

ISO 31000 Temeli: Risk = "Hedefler üzerindeki belirsizliğin etkisi" → Bu tanımdan hareketle emniyet ve güvenlik yeniden tanımlanabilir

RİSK

Tanım:

Hedefler üzerindeki belirsizliğin etkisi (ISO 31000). Gelecekteki belirsiz durumla ilgilidir.

Detay:

Pozitif (+kazanç) ve negatif (-kayıp) etkileri kapsar. Safety-II anlayışıyla: sadece başarısızlığı değil mükemmel performansı da kapsar.

EMNİYET (Safety)

Tanım:

Hedefler üzerindeki negatif etkilerin olasılığının DÜŞÜK olduğu durum/koşullar bütünü.

Detay:

Kasıtsız riskler bağlamında kullanılır. Güvenliği de (en geniş anlamıyla) kapsar — güvenlik emniyetin alt kümesidir.

GÜVENLİK (Security)

Tanım:

Hedefler üzerindeki KASITLI negatif etkilerin olasılığının düşük olduğu durum/koşullar bütünü.

Detay:

Farklı hedeflere sahip en az iki tarafın varlığını gerektirir. Çatışan hedefler güvenlik sorununu doğurur.

Ortak başlangıç noktası: "Hedefler" kavramı. Hedeflerin net tanımlanması, risk/emniyet/güvenlik yönetiminin temelidir.

Emniyet ile Güvenliği Birbirinden Ayıran 3 Boyut [2/2]

Blokland & Reniers

1

ETKİ BOYUTU (Effect)

Emniyet olayları kasıtsızdır; güvenlik olayları kasıtlıdır.

- Teröristler hedeflerinin amaçlarına kasıtlı zarar verir → güvenlik tehdidi
- Kasıtsız etkilerin tekrarlılığı istatistiksel analizi mümkün kılar → emniyet

2

HEDEFLER BOYUTU (Objectives)

Güvenlik en az iki taraf, çatışan hedefler gerektirir.

- Emniyet: birden fazla tarafın ortak hedefi (kimse kazalanmak istemez)
- Güvenlik: tarafların hedefleri çakışır. Biri diğerinin hedefine kasıtlı zarar verir.

3

BELİRSİZLİK BOYUTU (Uncertainty)

Emniyet istatistiksel veriyle, güvenlik dinamik belirsizlikle baş eder.

- Emniyet: aynı tip olaylar tekrarlanır → tarihsel veri birikir → istatistiksel modeller çalışır
- Güvenlik: saldırganlar tespit edilince taktiklerini değiştirir → tarihsel veri çabuk eskir

Sonuç: Emniyet ile güvenlik arasındaki temel fark kasıtsız/kasıtlı değil, "kötü niyet" ve "çatışan hedefler" varlığıdır.

BÖLÜM 3 — Emniyet ve Güvenlik Aynı Madalyonun İki Yüzüdür [1/2]

Nancy Leveson | MIT Aeronautics and Astronautics

Leveson'un Bütünleşik Tanımı

- EMNİYET: Kazalardan (kayıplardan) özgürlük
- KAZA/OLAY: Paydaşların tanımladığı istenmeyen veya planlanmamış, kayıpla sonuçlanan herhangi bir olay
- Bu tanımda kasıtsız/kasıtlı ayrımı YOK → güvenlik de bu tanımın içinde
- TEHLİKE (Hazard) = GÜVENLİK AÇIĞI (Vulnerability): Her ikisi de sistem durumu; sistem tasarımcılarının elimine etmesi gereken
- Tasarım hatalarının sisteme yerleşmeden önce tespit edilemeyeceğini kabul eder
- Karmaşık sistemlerde nedensellik = zincirleme başarısızlıkların ötesinde → sistem teorisi

STAMP Modeli ve Paradigma Değişimi

- Geleneksel model: Domino/İsviçre peyniri → kaza = başarısızlıklar zinciri
- STAMP: Emniyet ve güvenlik = dinamik kontrol problemi
- Hedef: tüm sistem davranışı üzerinde kısıtlamalar uygulamak
- STPA (Sistem Teorisine Dayalı Süreç Analizi): Güvenlik senaryolarını emniyet analizine yalnızca birkaç ek adımla ekler
- CAST: Gerçekleşmiş kazaların/saldırıların nedensel analizi — hem kasıtsız hem kasıtlı için kullanılabilir
- Yüzlerce karşılaştırmalı çalışmada STAMP tabanlı yaklaşım geleneksel yöntemleri her seferinde geçti

"Güvenilirlik analizi emniyet için yeterli değil; sistem tasarım hatalarını yakalaması için sistem teorisi gerekli." — Leveson, MIT Press 2012

STPA(Sistem-Teorik Süreç Analizi - System-Theoretic Process Analysis) Uygulaması: Uçak Fren Sistemi Örneği [2/2]

Nancy Leveson — MIT

STPA Adımları: (1) Sistem tehlikelerini tanımla → (2) Güvensiz kontrol eylemlerini belirle → (3) Nedensel senaryolar oluştur → (4) Emniyet + GÜVENLİK kısıtlamaları tasarla

Örnek: Uçak Tekerlek Freni — Tehlike H-4.1: İniş sırasında yetersiz yavaşlama

Emniyet Senaryosu (Kazara)

- BSCU (Braking and Steering Control Unit-Fren ve Dümenleme Kontrol Ünitesi) sistemi tekerleklerin durduğunu yanlış algılıyor (sıfır hız)
- Islak pistten dolayı tekerlekler kayıyor → hız sensörü gecikmeli sinyal gönderiyor
- Ağırlık sensörü arızası → sistem hâlâ havada zannediyor
- Otobrake devreye girmiyor → H-4.1 gerçekleşiyor

GÜVENLİK Senaryosu (Kasıtlı)

- Saldırgan hız sensörü çıkışını manipüle ediyor → sisteme sahte 'sıfır hız' sinyali gönderiyor (spoofing)
- Saldırgan fren komutunu engelliyor (DoS saldırısı) → komut iletilemiyor
- Saldırgan sistemin alternate mod geçişini tetikliyor → BSCU devre dışı kalıyor
- Sonuç: aynı tehlike (H-4.1) farklı yoldan gerçekleşiyor — kontrol mekanizması özdeş

Sonuç: İki senaryo için savunma mekanizması birleşiyor — mekanik hız sınırlayıcı (interlock) veya analog RPM (Revolutions per minute) göstergesi her ikisini de önler.

BÖLÜM 4 — Havacılıkta Emniyet Güvenliğe Karşı [1/2]

Heinz Wipf | Airnav Consulting Zurich | HEMS operasyonları üzerine ampirik vaka çalışması

Bağlam: HEMS (Helikopter Acil Tıp) operasyonları → Alçak görüşlülük + engel dolu ortam + tek navigasyon kaynağı olarak GNSS. Doğal parazit = emniyet riski; kasıtlı sinyal müdahalesi = güvenlik tehdidi.

ICAO Tanımları ve SE Perspektifi

- GÜVENLİK (ICAO): 'Sivil havacılığı yasadışı müdahale eylemlerine karşı koruma'
- EMNİYET (ICAO): 'Havacılık faaliyetleriyle ilgili risklerin kabul edilebilir düzeye indirildiği ve kontrol altında tutulduğu durum'
- Geleneksel ayrım: Güvenlik = kolluk kuvvetleri + havalimanları; Emniyet = operatörler + ekipman + prosedürler
- SE (Sistem Mühendisliği) bakışı: Tehlikeler (hazards) emniyetle, güvenlik açıkları (vulnerabilities) güvenlikle ilişkilendirilir
- RF kanal örneği: Doğal sinyal gürültüsü → emniyet; kasıtlı parazit (jamming/meaconing/spoofing) → güvenlik
- Temel soru: İki alan ayrı yönetilmeli mi yoksa birleşik çerçeve mümkün mü?

Üç Saldırı Türü ve Özellikleri

- JAMMING (Engelleme): Güçlü RF sinyali ile alıcıyı engelleme. Maliyet ~1.000€. Tespit edilmesi KOLAY. Düşük teknik bilgi.
- MEACONING(Tekrarlı sinyal gönderimi): Sinyali gecikmeli yeniden yayma → sahte konum. Maliyet ~10.000€. Tespit RİSKİ DÜŞÜK. Orta teknik bilgi.
- SPOOFING(Kimlik sahtekarlığı): Sahte GNSS sinyali enjeksiyonu → navigasyon tamamen kontrol altına alınabilir. Maliyet ~100.000€. Tespit riski düşük. Yüksek teknik bilgi.
- Sinyal-parazit oranı (SNR): İki alan için kritik ortak metrik
- Uçuş fazı riski: İniş ve kalkış → YÜKSEK; En route → DÜŞÜK (yükseklik artar, mesafe uzar, sinyal gücü azalır)

Ampirik veri: Skyguide/İsviçre helikopter uçuşlarında RF parazit izleme kaydedildi — GNSS kalite bozulması sürekli tespit ediliyor.

Oyun Teorisi ile Emniyet-Güvenlik Bütünleşik Modeli [2/2]

Heinz Wipf

Oyun Teorisi Sınıflandırması: Oyuncu Sayısı ile Emniyet-Güvenlik Ayrımı

Oyuncu Sayısı	Alan	Oyun Türü	Yaklaşım	Örnek
0 (makine-makine)	Emniyet	Stratejik değil	Deterministik matematik	Otomasyon, kontrol sistemleri
1 (doğaya karşı)	Emniyet	Tek oyunculu	Optimizasyon / karar teorisi	Sosyo-teknik sistemler
2 (çatışma)	GÜVENLİK	Stratejik / rekabetçi	Oyun teorisi	Saldırı-savunma, GNSS müdahale
≥3 (koalisyon)	Emniyet + Güvenlik	İşbirliği oyunu	Koalisyon teorisi	Havacılık ekosistemi

Nash Dengesi ve Altyapıya Saldırı Paradoksu

Paradoks

Neden radyo altyapısına saldırı bu kadar nadir? GNSS sinyalleri herkese açık; saldırganlar bu altyapıyı kendi operasyonları için kullanıyor. Nash dengesi: saldırmak saldırgana da zarar verir → caydırıcı etki.

Bütünleşik Sonuç

Emniyet ve güvenlik, aynı üst kümenin oyuncu sayısıyla ayrışan alt kümeleridir. Oyun teorisi bütünleşik bir çerçeve sunar: 0-1 oyuncu = emniyet alanı; 2+ oyuncu = güvenlik alanına giriş.

"Emniyet ve güvenlik, oyuncu sayısıyla belirlenen aynı temelin farklı tezahürleridir." — Wipf, 2020

BÖLÜM 5 — Güvenlik ve Emniyet Kültürü: İkili mi Yoksa Farklı Fenomenler mi?

Sissel H. Jore | University of Stavanger | In Amenas saldırısı vaka analizi

In Amenas Vakası (Ocak 2013)

- Cezayir çölündeki doğal gaz tesisi, ~800 çalışan
- 32 ağır silahlı terörist baskın düzenledi
- 4 gün süren rehine krizi: 40 kişi hayatını kaybetti (5'i Statoil çalışanı, 10 ulusiyetten)
- Soruşturma raporu: Statoil güvenlik risk yönetim sistemine sahipti FAKAT kültür yetersizdi
- Öneri: Emniyet kültüründen ayrı, bağımsız bir güvenlik kültürü oluşturulmalı
- Sonuç: Norveçli petrol şirketlerinin %50'si 2015'te 'güvenlik kültürü' kavramını benimsemiş durumda
- Problem: Kavramın operasyonelleştirilmesi belirsiz, uygulamalar tutarsız

Gerring Kavramsal Yeterlilik (7 Kriter)

- Tanışıklık: Emniyet kültüründen türetilmiş, sezgisel ✓
- Rezonans: Güvenlik tehditleri için anlamlı ✓
- Parsimonluk: Sınırlı, belirsiz göstergeler ✗
- Koherans: Emniyet kültüründen ayrışma zor ✗
- Farklılaştırma: Belirsiz sınırlar ✗
- Derinlik: Az sayıda paylaşılan özellik ✗
- Teorik fayda: Potansiyel var, geliştirilmeli ≈
- Alan faydası: Norveç petrolünde kullanılıyor ✓

Temel Gerilimler

- Emniyet kültürü: açıklık, şeffaflık, adil kültür
- Güvenlik kültürü: gizlilik, sınırlı bilgi paylaşımı
- Adil kültür güvenlikte işe yarar mı? (Saldırgan kötü niyetlidir)
- Zayıf sinyalleri tespit etmek: rakip stratejik gizler → öğrenme zorlaşır
- Her çalışanın güvenliğe adanması: meslektaşlara güvensizlik → emniyet kültürüyle çelişkili
- SONUÇ: Teoride ayrı; pratikte bütünsel yaklaşım gerekli
- Güvenlik kültürü = güvenliği bireysel sorumluluk haline getiriyor

"Güvenlik kültürü kavramı emniyet kültürü kadar tartışmalıdır; ancak dijitalleşen dünyada farkındalık ve dayanıklılık için vazgeçilmezdir." — Jore

Kullanıcı Emniyet ve Güvenlik Deneyimi: Havalimanlarında Tasarım İnovasyonu

I. Bongiovanni

Havalimanında 3 Yaklaşım: Yasal → Yönetsel → Tasarım Odaklı

	Yasal Yaklaşım	Yönetsel Yaklaşım	Tasarım Yaklaşımı ★
Odak	Yasa	Kaynaklar/Hedefler	KULLANICILAR
Misyon	Sıfır olay	Etkin risk azaltma	Kullanıcıyı memnun et
İnovasyon Kaynağı	Mevzuat değişiklikleri	Regülasyon + bütçe	Kullanıcı ihtiyaçları
Temel Soru	Standartları karşıladık mı?	Mevzuata uygun ve verimli miyiz?	Emniyet-güvenliği unutulmaz deneyim yaptık mı?
Ayrım/Bütünleşme	Ayrı rejimler	Koşula bağlı	Birleşik deneyim

Kullanıcı Persona Haritaları ve Yolculuk Analizi

Alfred (64) — Risk Kaçınıcı Gezgin

Yılda bir kez kızını ziyaret eder. Güvenlik kontrolünü 'büyüleyici' buluyor, personelle sohbet ediyor. Bürokratik süreçleri güvenlik amacıyla tolere eder. Tasarım hedefi: bilgilendirici, merak uyandıran deneyim.

Wendy (41) — Hızlı İş Gezgini

Haftada 2 uçuş, zaman çok kıymetli. Güvenlik kontrolünü 'sinir bozucu' buluyor. Son dönemde saldırı olmadığı için gereksiz görüyor. Tasarım hedefi: SecScreenApp — bekleme süresi, duty-free teklif, anlık geri bildirim.

"Sonsuz hüsran yaratıcıları" (eternal killjoys) olmaktan çıkıp, kullanıcıya değer yaratan emniyet-güvenlik deneyimi tasarlamak mümkündür.

BÖLÜM 7 — Emniyet ve Güvenliğin Diverjansı [1/2]

David J. Brooks & Michael Coole | Edith Cowan University, Avustralya | Bilgi kategorisi analizi

Emniyet (OHS Occupational Health and Safety İş sağlığı ve güvenliği.) Bilgi Yapısı

- SIA Modeli: Konsültasyon, bilgi toplama, problem anlama, çözüm geliştirme, uygulama, izleme, değerlendirme
- INSHPO çerçevesi (6 kategori): Tehlike ve riskler; Kontrol önlemleri; İSG yönetimi; Rol ve fonksiyon; Teknik/davranışsal disiplin; Yönetim bilimi
- Risk kaynağı: TEHLIKE (hazard) → kazasal, sağlık etkileri, çevre
- Kontrol yaklaşımı: İnsan odaklı prosedürler; uyum ve hata yönetimi
- Yasal zorunluluk: OHS mevzuatı ile nitelikli uzman çalıştırma zorunlu
- Uluslararası standart: ISO 31000 risk yönetimi — emniyet alanı benimsemiş
- Gelişim: Akademik akreditasyon süreci yol alıyor; büyük ölçüde kurulmuş meslek

Güvenlik (Kurumsal) Bilgi Yapısı

- ASIS International (2009): 18 bilgi kategorisi — Fiziksel güvenlik, personel güvenliği, bilgi güvenliği, araştırma, risk yönetimi…
- Brooks modeli (13 kategori): Çekirdek: risk yönetimi, iş sürekliliği, fiziksel güvenlik, teknoloji, personel, endüstriyel
- Risk kaynağı: TEHDİT (threat) → kötü niyet, suç önleme, terörle mücadele
- Kontrol yaklaşımı: Fiziksel sertleştirme, caydırıcılık, geciktirme; teknoloji odaklı
- Yasal boşluk: Güvenlik uzmanı istihdamı için genel yasal zorunluluk YOK (polis lisansı hariç)
- Gelişim: Bilgi tabanı parçalı, akademik akreditasyon sınırlı; meslek statüsü tartışmalı
- Multidimensional: Ulusal güvenliktençen toplumsal güvenliğe uzanan geniş spectrum

Araştırma sorusu: "Emniyet ve güvenlik bilim dallarının bilgi kategorileri mesleki ayrışma gösteriyor mu?" Cevap: EVET, soyut düzey dışında.

Emniyet & Güvenlik Bilgi Kategorileri Karşılaştırması [2/2]

Bilgi Boyutu	EMNİYET (OHS)	GÜVENLİK (Kurumsal)	Durum
Risk Kaynağı	Tehlike (hazard) — kazasal	Tehdit (threat) — kötü niyet	⚡ Ayrışma
Temel Teoriler	Kaza modelleri, iş sağlığı teorileri, insan faktörü	Suç teorileri, CPTED, caydırıcılık, istihbarat	⚡ Ayrışma
Risk Kontrolü	İnsan odaklı, prosedürel uyum, hata yönetimi	Fiziksel sertleştirme, tespit-geciktirme-müdahale	⚡ Ayrışma
Mevzuat	OHS yasaları — uzman çalıştırma zorunlu	Genel zorunluluk yok; sektöre özgü düzenlemeler	⚡ Ayrışma
Risk Yönetimi	ISO 31000 — kapsamlı, standartlaşmış	ISO 31000 — kullanılıyor ama farklı bağlam	≈ Ortak Zemin
Mesleki Gelişim	Büyük ölçüde kurulmuş; akademik akreditasyon var	Gelişmekte; parçalı bilgi tabanı	⚡ Ayrışma
Güvenlik Fonksiyonu	INSHPO: emniyet uzmanının güvenlik işlevi var (hayat güvenliği)	Güvenlik emniyet uzmanlığını kapsamaz	Tek yönlü örtüşme

Sonuç: "İki mesleği tek pratikte birleştirmek, her ikisinin sınırlarını ve anlayışını seyreltir." Ancak hayat güvenliği (life safety) ortak alandır.

BÖLÜM 8 — Emniyeti Sağlamak... ve Sonra Güvenlik: Sürprizlere Hazırlıklı Olmak [1/2]

Todd R. La Porte | UC Berkeley | Nükleer santral, uçak gemisi, hava trafik kontrol saha araştırmaları

HÜCRE I [Yüksek/Yüksek]

Emniyet VE güvenlik ikisi de yüksek. En nadir kombinasyon.
Örnek: Nükleer uçak gemileri, nükleer reaktörler.
Kritik soru: Kaynaklar bunalıma girince ne olur?

HÜCRE II [Emniyet↑/Güvenlik↓]

Emniyet köklü, güvenlik yetersiz. Artan tehdit ortamında güvenlik kapasitesi artırılmalı. Örnek: NASA, sivil havacılık.
Kritik soru: Emniyet grupları güvenlik işlevi için kaynaklarından taviz verecek mi?

HÜCRE III [Emniyet↓/Güvenlik↑]

Güvenlik köklü, emniyet yetersiz. Örnek: ABD silah laboratuvarları, polis teşkilatları, istihbarat birimleri.
Kritik soru: Güvenlik grupları emniyet yenilikleriyle uyum sağlayabilir mi?

HÜCRE IV [Düşük/Düşük]

İkisi de yetersiz — organizasyon derin çukurda. Hem iç tehlikeler hem dış tehditler artıyor. Örnek: Eski NASA, bazı kamu kurumları.
Kritik soru: Liderler kaynak gereksiniminin boyutunu anlıyor mu?

"Politika talepleri güvenlik veya emniyet kapasitesini bir kez kurulduktan sonra neredeyse hiçbir zaman açıkça azaltmaz." — La Porte

Yol Bağımlılığı, Kademelenen Gerilimler ve Geçiş Protokolleri [2/2]

Todd R. La Porte

4. Durum: Yol Bağımlılığı — "Kim Önce Geldi?"

Organizasyonel yanıtlar, emniyet ve güvenlikten hangisinin önce kurulduğuna göre şekillenir. İlk gelen önceliği belirler; ikincisi ona uyum sağlamak zorunda kalır. Bu 'yol bağımlılığı' gerilimlerin hem biçimini hem yoğunluğunu belirler.

Kademelenen Operasyonel Yanıtlar ve 2 Hipotez

Artan Tehlike Seviyeleri ve Yanıtlar

- Seviye 1: İşyeri emniyeti — iç ve saha taşımacılığı
- Seviye 2: Yerel tehlikeli madde hazırlığı (kimya-radyasyon)
- Seviye 3: İtfaiye kapasitesi
- --- Emniyet'ten Güvenliğe Geçiş ---
- Seviye 4: BT güvenlik duvarları
- Seviye 5: Fiziksel izinsiz giriş önleme
- Seviye 6: Personel güvenlik alanları; 24/7 gözetim
- Seviye 7: Saldırı ekipleri, istihbarat kapasitesi

2 Temel Hipotez

- H1: Operatörler ve 'tehlikeye yakın' yöneticiler, emniyet-güvenlik geçişi için yüksek konsensüslü kurallar geliştirir. Her setin tetikleyicileri diğerini güçlendirmez.
- H2: Geçiş protokolleri (emniyet → güvenlik veya tersi) ağırlıklı olarak 'tehlikeye yakın' çalışma gruplarının ve orta düzey yönetimin yetkisindedir.
- Yönetimsel çıkarım: Kıdemli liderlik yeni beceri zorunluluğunu meşrulaştırmalı, çift kapasiteli ekipler için destek sağlamalı.

"Sürpriz ve hazırlıksızlığı beklemek, ve tehlikeye yakın olanlar için sempati ve anlayışla karşılamak — bu bir liderlik yükümlülüğüdür." — La Porte

BÖLÜM 9 — Emniyet ve Güvenlik: Yönetsel Gerilimler ve Sinerjiler [1/2]

Paul R. Schulman | Mills College & UC Berkeley | HRO araştırma programı

"Emniyet yönetimini iyi yapıyorsak güvenlik de kendiliğinden çözülür." — Büyük bir kamu kurumunun CEO'su. Schulman'ın yanıtı: "Bu, uygun olmayan bir gerçek dışılıktır."

Yüksek Güvenilirli Organizasyon (HRO) Emniyet Stratejisi

- Temel formül: Düşük girdi varyansı + Düşük süreç varyansı = Düşük çıktı varyansı
- Teknik sağlamlık: Yedekli bileşenler, yedekleme sistemleri, otomatik kapanma protokolleri
- Öncü yönetim: Kötü senaryoya götürebilecek öncül koşulları izle → zayıf sinyal alıcıları
- Lateral iletişim: Departmanlar arası güven; paylaşılan anlam inşası
- "Güvenilirlik Profesyonelleri": Formel rolünün ötesinde sistem odaklı kişiler; her kademede bulunur
- Prosedürlerin "sahiplenilmesi": Operatörler prosedür revizyonuna aktif katılır — komplacenlik önlenir
- Öncül bölge (precursor zone): Tehlikeli koşullara doğru sürüklenmeyi geriye döndürme kapasitesi

HRO'larda Güvenilirlik Profesyonellerinin Özellikleri

- Formel derecelerle değil sistem güvenilirliğini içselleştirmekle tanımlanır
- Formal bilgi + deneyimsel bilgiyi birleştirir
- 'Sistem' görüşleri kendi formel rollerinden büyük
- Kendi birimi içindeki pratik kaymaları (practical drift) tespit eder ve önler
- Hiyerarşide her seviyede bulunur: operatörden CEO'ya
- 'Tehlikeli bölgeye giriyoruz' veya 'bu eylemi yapmaktan rahatsızım' sözleri ciddiye alınır
- 9/11 sonrası hava trafik kontrolörlerinin tüm uçuşları temizlemesi — güvenilirlik profesyoneli davranışı

HRO araştırması kaynakları: nükleer santral, uçak gemisi, hava trafik kontrolü, ABD nükleer silah laboratuvarı — 5 yıl saha çalışması.

Güvenlik Yönetiminin HRO'ya Özgün Zorlukları [2/2]

Paul R. Schulman

Başarısızlık ≠ Güvenlik Açığı

- HRO emniyet: Sistemin olası başarısızlıklarını haritalayarak önler → belirli sınır koşulları var
- Güvenlik: 'Kaç farklı yoldan sistem başarısız olabilir' değil, 'Kaç farklı yoldan saldırıya açık?' sorusu
- Komplex sistem doğru çalışmasından çok daha fazla yolda başarısız olabilir; düşman stratejisi bu açıkları stratejik hedef yapar
- Germanwings örneği: Kokpit kapısını dışarıya kilitleme (güvenlik önlemi) içeriden sabotajı mümkün kıldı — yeni güvenlik açığı yarattı

Tasarım Kaynaklı Güvenlik Açıkları

- İnternet paradoksu: Her yeni bağlantı yeni güvenlik açığı ekliyor — tasarım ile kırılganlık birlikte büyüyor
- İnternet: Hiçbir doğal sistem bu düzeyde güvenlik açığıyla evrimleşemezdi; biz bunu kasıtla tasarladık
- Siber güvenliği tek organizasyon stratejisiyle yönetmek imkânsız; ulusal ölçekte düzenleme gerekiyor
- Sembolik hedef değeri: Terör her yüksek değerli hedefe ihtiyaç duymaz; korku yaratmak için düşük değerli hedef de yeterli

Emniyet-Güvenlik Stratejik Çelişkileri

- HRO emniyet: Önceden analiz + kapsamlı prosedürler → rijidite, hız kaybı. Güvenlik: hızlı adaptasyon gerektiriyor
- HRO emniyet: Lateral iletişim + bilgi paylaşımı. Güvenlik: bilgiyi sınırla; karşı öğrenmeyi engelle
- Emniyet: 'Konfor bölgem dışına çıkıyorum' söylemini güçlendir. Güvenlik: bilgiyi kısıtla, sahte sinyal riski
- Çözüm arayışı: 'Yüksek çözünürlüklü güvenilirlik' — daha geniş zaman ufku, uluslararası öncül takip

"HRO çerçevesi, emniyet ve güvenliğin her birini tek başına ele alan ayrı çerçevelerden daha etkili bir entegre yönetim zemini sunabilir." — Schulman

BÖLÜM 10 — Emniyet ve Güvenliğin Arayüzü: İşyeri

George Boustras | European University Cyprus | Araştırma hipotezi: Emniyet ve güvenlik işyerinde ortak bir arayüz oluşturmaktadır

Fiziksel Çevre Değişimleri

- 9/11 sonrası: 40.000+ müdahaleci etkilendi. Asbestos içeren toksik bulut → solunum hastalıkları
- PTSD, depresyon ve stres hastalıkları: uzun vadeli işyeri etkisi + sosyal sigorta maliyeti
- Organizasyonel güven krizleri: Çalışanlar güvenli ortam sağlamak için işvereni sorumlu tutar
- Düşük riskli ofis ortamları bile güvenlik ve emniyet görevlerini giderek birleştiriyor
- Teröristler amblematik işyerlerini medya etkisi için seçiyor
- Kişisel hazırlık düzeyi düşük: Saldırı deneyimi olan ülkelerde bile nüfusun %50'sinden azı önlem almış

Siber Güvenlik → İşyeri Emniyeti

- Siber saldırılar veri kaybının ötesine geçer: fiziksel hasar, operasyonel devre dışı kalma
- Kritik altyapı bağımlılığı: Enerji şebekeleri, hastaneler, trafik sistemleri — birbirine bağlı 'sistemlerin sistemi'
- Domino etkisi örneği: Güney Londra güç kesintisi → trafik lambası arızası → kaos
- Nükleer tesis siber güvenliği: 2016 Brüksel saldırılarının ardından Belçika'daki nükleer tesislere hazırlık raporu ortaya çıktı
- Bağlantısallık paradoksu: Dijital entegrasyon hem üretkenliği hem güvenlik açığını artırıyor
- Ortak faktör: Siber saldırılar ve radikalizasyonun her ikisi de insan faktörü tarafından yönlendiriliyor

Radikalizasyon & Finansal Kriz

- Radikalizasyon → işyeri güvenliği: 'Yerli, radikalize olmuş gençlik' artık işyerinde de var
- Dini/siyasi ayrımcılık → kişisel şikayet → radikalizasyon zinciri
- İşyeri zorbalığı hem psikososyal sorun (emniyet) hem güvenlik riski yaratır
- 2008 finansal krizi → işsizlik, geçici iş, düşük ücret → psikolojik sıkıntı → iş kazaları artışı
- Finansal kriz → aşırı siyasi partilerin yükselişi → toplumsal kutuplaşma → güvenlik tehdidi
- Ortak etken: Sosyal dışlanma hem emniyet hem güvenlik olaylarının ortak öncülüdür
- Sonuç: Yeni bilim dalı

Temel fark: Emniyet = işveren/yöneticiye yasal yükümlülük; Güvenlik = devlet otoritesi omurga, bireysel sorumluluk gerekçesi farklı.

Araştırma ve Yönetim Zorlukları: Kitabın Sentezi [1/2]

Tanımların Yönetimsel Sonuçları

Önlenmek İstenen Olarak Tanım

- Her iki alan da zarara karşı özgürlük hedefler — kayıp önleme ortak paydası
- Kasıtlılık ayrım noktası: çoğunluğun (Blokland, Leveson, Boustras) görüşü
- Daha nüanslı görüş (Jore, Brooks, La Porte): "kötü niyetin önceliği" daha hassas ölçüt
- Ortak tanım arayışı gerçekçi değil: bağlam, tehlike türü, düzenleyici çevre farklı

Risk — Ortak Çerçeve mi?

- Leveson + Bongiovanni: Kavramsal tartışma önemli değil; sistem kontrolü kaybı ikisini de kapsar
- Blokland & Reniers: ISO 31000 zemin olabilir ama sınırlı
- Tehlike: Risk çerçevesi mutlak güvenlik vaadini ima eder → gerçekçi olmayan beklenti
- Risk yönetimi riskin kendisini ortadan kaldırmaz; sadece maruz kalmayı azaltır

Güvende mi, Güvensizde mi?

- Emniyet: Bilgi paylaşımı = iyileştirme kriteri. Araştırmacı-pratisyen işbirliği köklü.
- Güvenlik: Gizlilik = organizasyonel refleks. Araştırmacı sahaya erişim zor.
- İçeriden tehdit paradoksu: Emniyet için güvenilen kişi → güvenlik tehdidi (Germanwings)
- Sahaya erişim sorunu: Güvenlik konularında bilgi alışverişi zorlaşıyor; araştırma kalitesi düşüyor

"Emniyet ve güvenliği geniş bir risk yaklaşımıyla basitçe 'harmanlamamak' için dikkatli olmak gerekir — kavramsal zarifliğe veya halihazırda mevcut metodolojik çözümlere körü körüne sarılmaktan kaçınılmalı."

Toplumsal Yakınsama ve Global Araştırma Gündemi [2/2]

Risk Toplumu ve Kurumsal Çerçeve

- Emniyet ve güvenlik artık neo-liberal etkiden (deregülasyon, özelleştirme, dış kaynak kullanımı) bağımsız ele alınamaz
- Bireylerin hedefleri artıyor, aynı anda daha çok kaybedecekleri var; kurumsal güven azalıyor
- HRO teorisi (1990'lar), dikkatli örgütlenme, dayanıklılık mühendisliği: 'Sürprizlere hazırlıklı ol', 'Beklenmedik olanı yönet'
- Radikal ölçekte küresel risk dinamikleri organizasyonel pratikleri şekillendiriyor — bu bağlantı yeterince araştırılmadı

Yeni Aktörler Araştırmaya Dahil Edilmeli

- Brooks & Coole: Emniyet ve güvenlik profesyonelleri ayrı topluluklar → her ikisi de araştırmaya katılmalı
- Wipf: 'Saldırgan' güvenlik analizinde aktör — emniyet perspektifinde var olmayan aktör
- Bongiovanni: Son kullanıcı (yolcu) → havacılık emniyet yönetiminde büyük ölçüde görmezden geliniyor
- Gelecek araştırma: Hem güvenlik hem emniyet araştırmacılarını içeren ekipler → önyargı azaltma

Ölçek Sorunu: Mikro'dan Makro'ya

- Pettersen & Bjørnskau: AB güvenlik düzenlemeleri havacılık çalışanlarının çalışma koşullarını → emniyeti etkiliyor
- Schulman: Güvenlik açıkları organizasyon sınırının ötesinde → tek örgüt müdahalesi yetersiz
- Boustras: Radikalizasyon uluslararası mesele → işyeri bireysel riski → ölçekler arası bağlantı
- Brüksel havalimanı krizi: Kriz ekibi dışarıdan ulaşamadı — güvenlik devlet sorumluluğunda, yönetim sınırı belirsiz

Kitabın Ortak Araştırma Gündemi Önerileri

- Makro-global yaklaşım: Risk toplumu dinamiklerinin örgütsel emniyet/güvenlik pratiklerine gizli etkileri
- Saha erişim sorunu: Güvenlik araştırması için ortam oluşturulması zorunlu
- Çoklu ölçek ve boyut: Bireysel, örgütsel, sektörel, ulusal, uluslararası düzeyler eş zamanlı
- La Porte'un önerisi: Liderler 'gözetim seyreltmesine' direnç göstermeli; emniyet ve güvenlik koruyucularını onurlandırmalı

"Emniyet ve güvenlik, küresel risk dinamiklerinin örgütsel pratiklere gizli ve beklenmedik etkilerini ortaya çıkarmada ortak bir araştırma gündeminde buluşuyor."

Genel Sentez — 11 Bölümden 11 Temel Çıkarım

1. Birleşik tanım arayışı gerçekçi değil; bağlama göre farklı tanımlar geçerli (Bieder & Gould)
2. Risk: Ortak çerçeve sunar, ama 'her şeyin çözümü' değil (Blokland & Reniers)
3. STAMP/STPA: Bütünleşik analiz için en güçlü mühendislik aracı (Leveson)
4. Oyun teorisi: Güvenlik olaylarını modelliyor, emniyet-güvenlik ikisini bağlıyor (Wipf)
5. Güvenlik kültürü: Vaat edici ama operasyonelleştirme eksik; teoride ayrı, pratikte birlikte (Jore)
6. Tasarım odaklı yaklaşım: Kullanıcı deneyimi hem emniyet hem güvenliği birleştirir (Bongiovanni)
7. Mesleki ayrışma belirgin: OHS ve kurumsal güvenlik bilgi tabanları farklılaşıyor (Brooks & Coole)
8. Yol bağımlılığı kritik: Kim önce geldi → gerilimlerin biçimini belirler; sürprizlere hazır ol (La Porte)
9. HRO çerçevesi umut verici: Emniyet-güvenlik entegrasyonu için zemin sunuyor (Schulman)
10. İşyeri arayüzü: Siber, radikalizasyon, finansal kriz — yeni emniyet-güvenlik kesişim alanı (Boustras)

Teşekkürler

The Coupling of Safety and Security
Exploring Interrelations in Theory and Practice

Bieder & Pettersen Gould (Eds.) | SpringerBriefs in Safety Management | Springer 2020 | Open Access

- 23 slayt, 11 bölüm, 12 yazar, 3 eksen: Kavramsal | Teknik/Metodolojik | Yönetim/Pratik
- Emniyet (Safety) ≠ Güvenlik (Security) — ancak modern risk ortamında bütünleşik yönetim zorunlu
- Ortak araştırma gündemi: Küresel risk dinamikleri, çok ölçekli yaklaşım, disiplinlerarası ekipler

https://doi.org/10.1007/978-3-030-47229-0 | Creative Commons Attribution 4.0 | Ücretsiz erişim: link.springer.com