

Ramazan Yaman Fen Lisesi Gençlik Çalıştayı

Milli Güvenlik Komitesi Çalışma Rehberi

Komite Başkanları: Defne Yaman, Ulaş Gega

İÇİNDEKİLER:

- 1. Komite Divanından Mektup**
- 2. Komite Gündemi**
- 3. Milli Güvenlik Nedir?**
- 4. Sınır Güvenliği Nedir?**
- 5. Milli Güvenlik Hakkında Bilinmesi Gereken Kavramlar**
- 6. Örnek Konu Başlıkları**
 - a) Siber Güvenlik*
 - b) Terörle Mücadelede Güvenlik*
 - c) Göç Krizleri ve Milli Güvenlik*
 - d) Hibrit Savaş ve Yeni Güvenlik Anlayışı*
 - e) Yapay Zekâ ve Otonom Silah Sistemleri*
 - f) Enerji Güvenliği ve Jeopolitik Rekabet*
- 7. Gelişmiş Ülkelerin Milli Güvenlik Yaklaşımları**
- 8. Kaynakça**

2026

Komite Divanından Mektup:

Sayın Katılımcılar,

Ramazan Yaman Fen Lisesi Gençlik Çalıştay'na ve komitemize hoş geldiniz. Burada sadece güncel sorunları tartışmayacak, geleceğin stratejilerini birlikte kurgulayacağız. Divan olarak, fikirlerinizi özgürce savunacağınız ve çokça öğreneceğimiz bir süreç dileriz. Tartışmaların harareti, çözümlerin ise netliğiyle dolu harika bir çalıştay bizi bekliyor. Komite içinde etkili bir tartışma ortamı oluşabilmesi için çalışma rehberini okuyarak gelmenizi rica ediyoruz. Herhangi bir sorunuz olursa bize defnee.ymn@gmail.com veya gegaulas@gmail.com mail adreslerinden ulaşabilirsiniz.

Sevgilerimizle.

Komite Gündemi : Günümüzde milli güvenlik; terörizm, siber saldırılar, sınır güvenliği ve toplumsal istikrar gibi birçok farklı alanda tehditlerle karşı karşıyadır. Bu komitede, bu tehditlere karşı alınabilecek önlemler tartışılacaktır.

Milli Güvenlik Nedir?

Milli güvenlik, bir devletin anayasal düzenini, egemenliğini, toprak bütünlüğünü, siyasi bağımsızlığını ve toplumun refahını; iç ve dış kaynaklı her türlü tehdide karşı korumaya yönelik geliştirdiği politika, strateji ve uygulamaların bütünüdür. Bu kavram yalnızca askeri tehditlerle sınırlı olmayıp; terörizm, siber saldırılar, ekonomik istikrarsızlık, enerji arz güvenliği, kitlesel göç hareketleri ve toplumsal huzuru bozabilecek unsurlar gibi çok boyutlu riskleri de kapsar.

Modern güvenlik anlayışında milli güvenlik, devletin sert gücünün (askeri ve kolluk kuvvetleri) yanı sıra yumuşak güç unsurlarını (diplomasi, ekonomi, eğitim ve teknoloji) da içeren bütüncül bir yapı olarak ele alınmaktadır. Bu bağlamda milli güvenlik; sadece tehditlere karşı savunma geliştirmeyi değil, aynı zamanda riskleri önceden öngörmeyi, krizleri yönetmeyi ve sürdürülebilir bir güvenlik ortamı oluşturmayı amaçlayan dinamik bir süreçtir.

Sınır Güvenliği Nedir?

Sınır güvenliği, bir devletin toprak bütünlüğünü korumak, yasa dışı geçişleri engellemek ve ulusal güvenliğini sağlamak amacıyla sınır hatlarında aldığı fiziksel, teknolojik ve idari önlemler bütünüdür. Modern dünyada sınır güvenliği sadece

fiziki bir koruma değil; göç yönetimi, kaçakçılıkla mücadele, terörizmin önlenmesi ve ekonomik istikrarın korunması gibi çok boyutlu bir stratejiyi ifade eder. Sınır Güvenliğinin Temel Bileşenleri Fiziki Önlemler: Sınır hattı boyunca inşa edilen duvarlar, tel örgüler, hendekler ve gözetleme kuleleri gibi somut engellerdir. Teknolojik Sistemler: Yapay zeka destekli MİA Teknoloji ve ZNA Teknoloji gibi kuruluşlar tarafından sağlanan; termal kameralar, sensörler, insansız hava araçları (İHA) ve gerçek zamanlı veri analiz sistemlerini kapsar. Askeri ve İdari Güçler: Sınır birlikleri ve muhafızları aracılığıyla yürütülen devriye ve denetim faaliyetleridir. Türkiye'de kara sınırlarının korunması ve güvenliği, 3497 sayılı kanun uyarınca Kara Kuvvetleri Komutanlığı sorumluluğundadır.

Milli Güvenlik Hakkında Bilinmesi Gereken Kavramlar:

- 1) **Egemenlik**: Bir ülke üzerinde en üstün ve bağımsız otoriteyi kullanma yetkisidir. İç egemenlik (hukuki ve siyasi otorite) ve dış egemenlik (uluslararası alanda bağımsızlık) olmak üzere iki boyutta ele alınır.
- 2) **Ulusal Çıkar**: Devletin varlığını sürdürmesi, refahını artırması ve uluslararası sistemde konumunu güçlendirmesi için korunması gereken temel hedefler bütünüdür. Milli güvenlik politikalarının belirlenmesinde ana referans noktasıdır.
- 3) **Tehdit ve Risk Analizi**:
 - **Tehdit**: Devletin değerlerine zarar verme potansiyeline sahip aktör veya durum
 - **Risk**: Bu tehdidin gerçekleşme olasılığı ile muhtemel etkisinin birleşimi. Modern güvenlik çalışmaları, bu iki kavram üzerinden strateji üretir.

4) Caydırıcılık: Devletin sahip olduđu askeri, ekonomik veya teknolojik kapasite aracılıđıyla, potansiyel rakiplerin saldırı niyetini engellemeye yönelik stratejik yaklaşımdır. Özellikle nükleer strateji bağlamında gelişmiştir.

5) Güç ve Milli Güç Unsurları: Devletin uluslararası sistemde etkide bulunma kapasitesi;

- **Sert güç** (askeri kapasite),
- **Yumuşak güç** (kültürel ve diplomatik etki),
- **Akıllı güç** (her ikisinin dengeli kullanımı)

şeklinde sınıflandırılır.

6) Güvenlik İkilemi:

Bir devletin güvenliğini artırmaya yönelik attığı adımların, diğer devletler tarafından tehdit olarak algılanması ve karşılıklı güvensizlik ortamı yaratması durumudur. Uluslararası ilişkiler teorisinde önemli bir kavramdır.

7) İç Güvenlik ve Dış Güvenlik:

- **İç güvenlik:** Kamudüzeni, toplumsal istikrar ve hukuk düzeninin korunması
 - **Dış güvenlik:** Devletin dış tehditlere karşı korunması
- Günümüzde bu ayrım giderek belirsizleşmektedir.

8) Asimetrik Tehditler: Devlet dışı aktörlerin (terör örgütleri, siber saldırganlar vb.) geleneksel olmayan yöntemlerle oluşturduğu tehditlerdir. Modern güvenlik anlayışının merkezinde yer alır.

9) Siber Güvenlik: Bilgi ve iletişim sistemlerinin korunmasına yönelik strateji ve uygulamaları kapsar. Kritik altyapıların korunması açısından milli güvenliğin ayrılmaz bir parçası haline gelmiştir.

10) İstihbarat ve Erken Uyarı Sistemleri: Tehditlerin önceden tespit edilmesi amacıyla veri toplama, analiz etme ve karar alıcılara sunma süreçlerini içerir. Stratejik karar alma mekanizmalarının temelini oluşturur.

11) Kriz ve Risk Yönetimi: Beklenmedik veya yüksek etkili olaylara karşı devletin hızlı, koordineli ve etkili tepki verme kapasitesidir. Afetler, savaşlar ve ekonomik krizler bu kapsamda değerlendirilir.

12) İnsan Güvenliği: Geleneksel devlet merkezli güvenlik anlayışının ötesine geçerek bireyin yaşam, sağlık, özgürlük ve refahını merkeze alan yaklaşımdır. Modern güvenlik çalışmalarında önemli yer tutar.

Örnek Konu Başlıkları:

a) Siber güvenlik: Ulusal düzeyde siber güvenlik, bir ülkenin devlet kurumlarını, kritik altyapılarını ve vatandaşların dijital verilerini siber tehditlere karşı korumak amacıyla geliştirdiği politika, kurum ve teknolojilerin bütünüdür. Bu kapsamda devlet, siber saldırıların önlenmesi, tespit edilmesi ve etkilerinin en aza indirilmesi için hem teknik hem de hukuki önlemler alır; enerji, ulaşım, sağlık ve bankacılık gibi hayati sektörlerin kesintisiz çalışmasını güvence altına almaya çalışır. Aynı zamanda siber olaylara hızlı müdahale edebilmek için özel merkezler kurulur ve yerli siber güvenlik teknolojilerinin geliştirilmesi

desteklenir. Böylece hem ulusal güvenlik hem de dijital egemenlik korunarak ülkenin bilgi sistemleri dış tehditlere karşı daha dirençli hale getirilir.

ULUSAL SIBER GÜVENLİK ANALİZ RAPORU

Stratejik Bileşenler ve Tehdit Yönetimi

1. Ulusal Siber Güvenlik Sistemi

Bileşen	Fonksiyon ve Amaç
Kritik Altyapı Yönetimi	Enerji, ulaşım ve finans gibi hayati sektörlerin siber saldırılara karşı korunması ve kesintisiz hizmetin devamlılığı.
Tespit ve Müdahale	Siber olaylara anında müdahale kapasitesinin artırılması ve saldırı etkilerinin minimize edilmesi süreci.
Dijital Egemenlik	Milli ve yerli siber güvenlik teknolojilerinin teşvik edilmesiyle dışa bağımlılığın azaltılması.
Hukuki Çerçeve	Siber suçlarla mücadele ve dijital verilerin korunmasına yönelik yasal düzenlemelerin tesisi.

Siber güvenlik neden önemlidir?

Günümüzde neredeyse her şey internet üzerinden yürüdüğü için (bankacılık, sosyal medya, eğitim, devlet işlemleri), kişisel ve kurumsal veriler sürekli risk altındadır. Siber güvenlik bu verilerin güvenliğini sağlar.

Temel Amaçları

- Bilgi gizliliğini korumak (kişisel verilerin başkalarının eline geçmemesi)
- Verilerin bütünlüğünü sağlamak (verilerin değiştirilmemesi)
- Sistemlerin kesintisiz çalışmasını sağlamak (erişilebilirlik)

b) Terörle Mücadelede Güvenlik: Devletin ve ilgili kurumların terör örgütlerinin faaliyetlerini önlemek, vatandaşların can ve mal güvenliğini korumak ve kamu düzenini sağlamak amacıyla yürüttüğü önleyici, koruyucu ve caydırıcı tüm politikaları ifade eder. Bu güvenlik anlayışı sadece olay olduktan sonra müdahale etmeyi değil, aynı zamanda terörün ortaya çıkmasını engelleyecek sosyal, ekonomik, istihbari ve hukuki tedbirleri de kapsar. Bu süreçte istihbarat

faaliyetleriyle olası tehditler erken aşamada tespit edilmeye çalışılırken, sınır güvenliği, kritik tesislerin korunması ve toplum içinde güvenlik bilincinin artırılması gibi uygulamalar da devreye girer. Böylece hem devletin istikrarı hem de toplumun huzuru korunarak terörün oluşturabileceği zararların önüne geçilmeye çalışılır.

Türkiye'de terörle ilgili veriler genellikle İçişleri Bakanlığı, Emniyet Genel Müdürlüğü ve Millî İstihbarat Teşkilatı (MİT) gibi kurumların yıllık raporları üzerinden değerlendirilir. Genel çerçevede Türkiye, uzun yıllardır hem bölücü terör örgütleri (özellikle PKK) hem de küresel bağlantılı terör örgütleri (örneğin DEAŞ) ile mücadeleden ülkeler arasında yer alır. Son yıllarda güvenlik operasyonlarının artmasıyla birlikte şehir merkezlerindeki büyük ölçekli terör saldırılarının belirgin şekilde azaldığı, ancak kırsal alanlarda ve sınır bölgelerinde güvenlik operasyonlarının devam ettiği görülmektedir. Türkiye'de terörle mücadele kapsamında binlerce operasyon düzenlenmekte, örgütlerin lojistik ağları, finans kaynakları ve eleman kazanma faaliyetleri hedef alınmaktadır. Ayrıca yüzlerce terör bağlantılı kişi hakkında adli işlem yapılmakta, yurt içi ve yurt dışında koordineli güvenlik çalışmaları yürütülmektedir. Resmî verilere göre devletin amacı, terör olaylarını sadece bastırmak değil, aynı zamanda önleyici güvenlik stratejileriyle terör oluşumunu kaynağında engellemek olarak ifade edilmektedir.



c) Göç Krizleri ve Milli Güvenlik: Savaşlar, siyasi baskılar, ekonomik çöküşler ve doğal afetler nedeniyle milyonlarca insanın yerinden edilmesiyle oluşan, ev sahibi ülkelerde altyapı, ekonomik uyum, sosyal kutuplaşma ve güvenlik sorunlarını tetikleyen karmaşık durumlardır

Türkiye, jeopolitik konumu nedeniyle tarihsel olarak hem transit hem de hedef ülke niteliği taşıyan bir göç rejimine sahiptir. Özellikle 2011 sonrası Suriye iç savaşıyla birlikte kitlesel zorunlu göç hareketleri artmış, Türkiye milyonlarca sığınmacıya ev sahipliği yapan ülkelerden biri hâline gelmiştir. Bu durum, kamu hizmetleri üzerinde baskı oluştururken aynı zamanda iş gücü piyasası, şehirleşme ve sosyal uyum süreçlerinde yapısal değişimlere yol açmıştır. Türkiye'nin göç yönetimi politikaları, insani yükümlülükler ile ulusal kapasite ve toplumsal uyum arasında denge kurma çabası üzerinden şekillenmektedir.

1. Türkiye'deki Geçici Koruma Kapsamındaki Nüfus Gelişimi

Yıl	Kayıtlı Suriyeli Sayısı	Nüfus Oranı (%)	Temel Politika Yaklaşımı
2011	8.000	<%0.1	Açık Kapı / Misafir Odaklı
2014	1.500.000	%1.9	Geçici Koruma Statüsü
2018	3.600.000	%4.4	Sosyal Uyum ve Entegrasyon
2023	3.300.000	%3.8	Gönüllü Geri Dönüş ve Sınır Kontrolü

Açık Kapı Politikası: Açık kapı politikası, bir devletin sınırlarına gelen ve genellikle savaş, çatışma veya ağır insani krizlerden kaçan kişileri önceden sıkı bir engelleme yapmadan ülkeye kabul etmesi anlayışıdır. Açık kapı politikası insani açıdan doğrusada, uzun vadede Türkiye'nin sosyal ve ekonomiyapısı açısından sürdürülebilir midir?

Türkiye bağlamında açık kapı politikası özellikle Suriye iç savaşı sonrası uygulanmış ve güvenlik riski taşıdığı değerlendirilen kişilere karşı bile, genel olarak “sığınmacılara sınırların açık tutulması” yaklaşımını ifade etmiştir. Bu politika, insani sorumluluk ve uluslararası koruma ilkeleri çerçevesinde değerlendirilirken; aynı zamanda ekonomik yük, sosyal uyum ve güvenlik gibi alanlarda tartışmalara da yol açmaktadır.

2. Açık Kapı Politikasının Çok Boyutlu Etki Analizi

Etki Alanı	İnsani ve Stratejik Kazanımlar	Yapısal ve Güvenlik Sorunları
Ekonomi	İş gücü arzı, üretim artışı.	Kamu harcamalarında artış, kayıt dışı istihdam.
Sosyal Yapı	Kültürel etkileşim.	Sosyal kutuplaşma, demografik kaygılar.
Güvenlik	Yumuşak güç kullanımı.	Sınır güvenliği riskleri, asayiş sorunları.

d) Hibrit Savaş ve Yeni Güvenlik Anlayışı: Hibrit savaş kavramı nizami ve gayrinizami savaşın iç içe girdiği kompleks bir savaş formunu ifade etmektedir. Kavram savaş alanlarının ve araçlarının değişen, gelişen ve iç içe giren kapsamına dikkat çekmektedir.

En önemli yönlerinden biri, hibrit savaşın düşük maliyetle yüksek etki yaratabilmesidir. Bir ülke doğrudan ordu kullanmadan, siber saldırılarla altyapıyı zayıflatabilir, sosyal medya üzerinden bilgi kirliliği oluşturabilir ya da ekonomik baskılarla bir devleti zor durumda bırakabilir. Bu durum, savaşın alanını genişletir ve tehditleri daha karmaşık hale getirir.

Bir diğer önemli nokta, toplumların hedef haline gelmesidir. Hibrit savaşta amaç sadece devlet kurumlarını değil, halkın güven duygusunu, birlik hissini ve karar alma mekanizmalarını etkilemektir. Bu da bilgi savaşını ve psikolojik etkiyi çok kritik hale getirir.

Ayrıca hibrit savaş, devletlerin güvenlik anlayışını değiştirmiştir. Artık sadece sınır güvenliği veya ordu gücü yeterli değildir. Siber güvenlik sistemleri, enerji altyapısı koruması, medya okuryazarlığı ve istihbarat kapasitesi bir ülkenin güvenliği için

temel unsurlar haline gelmiştir. Son olarak, hibrit savaşın önemi uluslararası ilişkileri belirsizleştirmesidir. Saldırının kimden geldiği her zaman açık olmayabilir. Bu da devletler arasında doğrudan çatışma olmadan gerilim yaratılmasına yol açar. Hibrit savaşın “savaşılan edilmeden yürütülen savaş” olarak tanımlanması, uluslararası hukuka açısından hangisi sorunları doğurur?

e) Yapay Zekâ ve Otonom Silah Sistemleri: Yapay zeka, savaş sistemlerinde, stratejik karar verme süreçlerinde, veri geliştirme ve analizinde, çatışma simülasyonlarında, hedef tanımlama, tehdit izleme, İHA (İnsansız Hava Aracı) ve SİHA (Silahlı İnsansız Hava Aracı) sürü yönetimi, lojistik taşıma, savaşta yaralıların bakımı ve tahliyesi gibi pek çok alanda kullanılmaktadır. Yapay zekanın bu alanlarda kullanılması, operasyonel süreçlerde insan hatalarının önlenmesine ve zayıf verilere dayalı kararların engellenmesine olanak tanımaktadır. Gelecekte savaşlar tamamen “insansız” hale gelebilir mi?

f) Enerji Güvenliği ve Jeopolitik Rekabet: Enerji güvenliği, bir devletin ekonomik faaliyetlerini sürdürebilmesi ve ulusal güvenliğini koruyabilmesi için gerekli olan petrol, doğal gaz, kömür ve giderek artan şekilde yenilenebilir enerji kaynaklarına kesintisiz, güvenli ve ekonomik erişimini garanti altına almasıdır. Günümüzde enerji güvenliği, klasik bir ekonomik mesele olmaktan çıkarak doğrudan jeopolitik rekabetin merkezine yerleşmiştir. Çünkü enerji kaynaklarının dağılımı dünyada eşit değildir ve bu kaynaklar çoğunlukla politik olarak istikrarsız veya stratejik öneme sahip bölgelerde yoğunlaşmıştır. Enerji kaynaklarının eşitsiz dağılımı küresel güç dengesini nasıl etkiler?

Gelişmiş Ülkelerin Milli Güvenlik Yaklaşımları:

Gelişmiş ülkelerin millî güvenlik stratejileri, klasik askerî savunma anlayışının ötesine geçerek çok boyutlu bir güvenlik yaklaşımı üzerine kuruludur.

Amerika Birleşik Devletleri, güvenlik stratejisinde küresel güç projeksiyonunu, ittifak sistemlerini (özellikle NATO) ve teknolojik üstünlüğü merkezde tutarken; siber güvenlik, uzay savunması ve yapay zekâ destekli askerî sistemlere büyük yatırım yapmaktadır. Avrupa Birliği ülkeleri ise daha çok kolektif güvenlik, kriz yönetimi ve diplomatik çözüm mekanizmalarıyla birlikte enerji güvenliği ve göç yönetimini de millî güvenlik çerçevesine dahil etmektedir. Birleşik Krallık, istihbarat kapasitesi ve deniz aşırı operasyon kabiliyetiyle birlikte hibrit tehditlere karşı esnek savunma stratejileri geliştirmektedir. Japonya ve Güney Kore gibi Asya-Pasifik ülkeleri ise özellikle bölgesel tehdit algısı nedeniyle füze savunma sistemleri, teknoloji temelli erken uyarı sistemleri ve ABD ile askeri iş birliklerini stratejilerinin merkezine koymaktadır.

Genel olarak bu ülkelerde millî güvenlik, yalnızca askerî tehditlere karşı korunma değil; siber saldırılar, ekonomik istikrarsızlık, enerji arz güvenliği, bilgi savaşı ve iklim kaynaklı riskler gibi alanları da kapsayan bütüncül bir “ulusal dayanıklılık” yaklaşımı şeklinde ele alınmaktadır.

KAYNAKÇA: <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik- stratejisi-2024-2028.pdf>

<https://dergipark.org.tr/tr/download/article-file/4886657>

<https://dergipark.org.tr/tr/download/article-file/2643480>

https://ipv4.tasam.org/Files/Icerik/File/Hibrit_Sava%C5%9Ftan_Yeni_Nesil_bir_G%C3%BC_ve_nlik_Anla_y%C4%B1_%C5%9F%C4%B1_na_Hibr it_G%C3%BC_ve_nlik__As%C4%B1_m_%C3%96zt_%C3%BCr_k_pd_f_e00c_f266-0c5a-498e-a6b6-8ec0a4a709e3.pdf

<https://tesamstrateji.com/yazi.php?link=yapay-zekanin-silahli-catismalarda-kullanilmasi-ve-dogurdugu-etik-ve-hukuki-sorunlar>

<https://ordaf.org/ortadoguda-cok-katmanli-rekabet-ve-guc-siyaseti/>