
GAZİ ÜNİVERSİTESİ
Gazi
1926

NÜKLEER TEDARİK ZİNCİRİNDE EN İYİ SİBER GÜVENLİK SİSTEMİNE SAHİP ÜLKENİN SEÇİLMESİ

Merve ÇETİN

YÜKSEK LİSANS TEZİ
BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

OCAK 2020

Merve ÇETİN tarafından hazırlanan "NÜKLEER TEDARİK ZİNCİRİNDE EN İYİ SİBER GÜVENLİK SİSTEMİNE SAHİP ÜLKENİN SEÇİLMESİ" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi BİLGİ GÜVENLİĞİ MÜHENDİSLİĞİ Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Prof. Dr. Hadi GÖKÇEN

Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Doç. Dr. İbrahim Alper DOĞRU

Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Üye: Dr. Öğr. Üyesi Volkan SÖNMEZ

Bilgi Güvenliği Mühendisliği Ana Bilim Dalı, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Tez Savunma Tarihi: 30/01/2020

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Sena YAŞYERLİ

Fen Bilimleri Enstitüsü Müdürü

ETİK BEYAN

Gazi Üniversitesi Fen Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Merve ÇETİN

30/01/2020

NÜKLEER TEDARİK ZİNCİRİNDE EN İYİ SİBER GÜVENLİK SİSTEMİNE SAHİP ÜLKENİN SEÇİLMESİ

(Yüksek Lisans Tezi)

Merve ÇETİN

GAZİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

Ocak 2020

ÖZET

Bilgisayar güvenliğine olan ilginin ve akabinde bu yöndeki araştırmaların ve uygulamaların arttığı günümüzde pek çok uluslarası devlette olduğu gibi ülkemizde de gelecekte yaşanması olası tehdit senaryolarına karşı yeni düzenlemeler yapılmakta ve savunma sistemleri geliştirilmektedir. Bu düzenlemeler en nihayetinde nükleer tesislerin güvenliğini de etkileyebilecek olan bilgisayar güvenliği gereksinimlerini de karşılamalıdır. Bilgi ve bilgisayar güvenliğinin hedefinde genelde elektronik veri ve bilgisayarların siber tehditlere karşı korunması vardır. Bu tezin hedefi ise nükleer tedarik zincirinde yer alan dijital sistemlerin her türlü kötü niyetli eyleme karşı hazırlıklı olmasını sağlamak, bu amaçla yalnızca nükleer tesislerin değil nükleer güvenliği aynı seviyede etkileyebilecek tüm tedarik zincirinde siber güvenliği sağlamanın gerekliliği konusunda farkındalık kazandırmaktır. Bu tezin bilgisayar güvenliği konusunda bilgi alt yapısı oluşturulması, nükleer tedarik zincirinin işleyiş mekanizmasının ortaya konularak olası tehditlerin değerlendirilmesi ve bu hususta ortaya konulabilecek savunma sistemlerinin geliştirilmesi bakımından faydalı olacağı düşünülmektedir. Bu tezde, diğer ülke uygulamalarının ve uzman görüşlerinin aktarılması sağlanarak ülkemiz nükleer altyapısının güçlendirilmesi ve nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerini Analitik Hiyerarşi Prosesi(AHP) kullanarak sıralaması bakımından katkısı olacaktır.

Bilim Kodu : 92403
Anahtar Kelimeler : Nükleer Tedarik Zinciri, Siber Güvenlik, AHP
Sayfa Adedi : 71
Danışman : Prof. Dr. Hadi GÖKÇEN

SELECTING THE COUNTRY WITH THE BEST CYBER SECURITY SYSTEM IN NUCLEAR SUPPLY CHAIN

(M. Sc. Thesis)

Merve ÇETİN

GAZİ UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

January 2020

ABSTRACT

Today, as the interest in computer security and subsequent research and applications in this direction have increased, new regulations are being made and defense systems are being developed against future threatening scenarios in our country, as in many international states. These regulations must also meet computer security requirements, which may ultimately affect the security of nuclear facilities. Electronic data and computers are generally protected against cyber threats at the target of information and computer security. The aim of this thesis is to ensure that the digital systems in the nuclear supply chain are prepared for all kinds of malicious actions, and for this purpose, to raise awareness about the necessity of providing cyber security in the entire supply chain that may affect not only nuclear facilities but also nuclear security at the same level. It is thought that this thesis will be useful in terms of establishing an information infrastructure on computer security, evaluating possible threats by revealing the functioning mechanism of the nuclear supply chain and developing defense systems that can be revealed in this regard. In this thesis, it will contribute to the strengthening of our country's nuclear infrastructure and listing the success factors that improve cyber security in the nuclear supply chain management by using the Analytical Hierarchy Process (AHP) by providing the transfer of other country practices and expert opinions.

Science Code : 92403
Key Words : Nuclear Supply Chain, Cyber Security, AHP
Page Number : 71
Supervisor : Prof. Dr. Hadi GÖKÇEN

TEŞEKKÜR

Bu tez çalışmasının hazırlanma sürecinde bilgi ve tecrübelerinden yararlandığım danışman hocam Sayın Prof. Dr. Hadi GÖKÇEN'e en içten duygularımla teşekkür ederim. Tüm hayatım boyunca maddi ve manevi destekleri ile yanımda olan sevgili eşim Yasin ÇETİN'e, iş arkadaşlarıma ve biricik aileme teşekkür ederim.

İÇİNDEKİLER

Sayfa

ÖZET…….. iv
ABSTRACT..... v
TEŞEKKÜR..... iv
İÇİNDEKİLER v
ÇİZELGELERİN LİSTESİ..... vii
ŞEKİLLERİN LİSTESİ..... viii
SİMGELER VE KISALTMALAR..... ix
1. GİRİŞ …… 1
2. LİTERATÜR ÇALIŞMALARI VE TARTIŞMA 5
3. MATERYAL VE METOD..... 11
3.1. Nükleer Tedarik Zinciri Yönetimi 11
3.1.1. Nükleer tedarik zincir..... 13
3.2. Nükleer Tedarik Zincirinde Siber Güvenlik 14
3.2.1. Nükleer tesislerde siber güvenlik..... 22
3.2.2. Nükleer ihracat kontrol rejimi ve siber güvenlik 23
3.2.3. Araştırma merkezleri ve laboratuvarları ve siber güvenlik..... 25
3.2.4. Acil müdahale organizasyonları ve siber güvenlik 26
3.2.5. Taşımacılık organizasyonları ve siber güvenlik..... 27
3.3. Dünyadaki Uygulamalar 29
3.3.1. Güney Kore 29
3.3.2. Rusya Federasyonu 30
3.3.3. Çin Halk Cumhuriyeti 31
4. ANALİTİK MODEL TABANLI BİR UYGULAMA..... 33
4.1. Çok Ölçütlü (Kriterli) Karar Verme..... 33
4.2. Mevzuat geliştirme..... 34
4.2.1. Estonya siber güvenlik yasaları..... 34
4.2.2. Avusturalya siber güvenlik yasaları 35
4.2.3. Çin siber güvenlik yasaları..... 36
4.2.4. Fransa siber güvenlik yasaları..... 36
4.2.5. Finlandiya siber güvenlik yasaları 37

Sayfa

4.3. Örnek Uygulama 38
5. SONUÇ 59
KAYNAKLAR 65
EKLER……..... 69
EK-1. Nükleer tedarik zincirinde siber güvenliğe ilişkin anket……. 70
ÖZGEÇMİŞ 71

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

Çizelge 2.1. Literatür karşılaştırması 8
Çizelge 4.1. A Matrisi 41
Çizelge 4.2. Önem Skalası 42
Çizelge 4.3. Normalize matris (C Matrisi) 43
Çizelge 4.4. W Matrisi 44
Çizelge 4.5. RI Değerleri 46
Çizelge 4.6. Nükleer güvenlik mevzuatının özgünlüğü 48
Çizelge 4.7. Nükleer mevzuat içerisindeki siber güvenlikle ilgili referanslar 48
Çizelge 4.8. Mevzuat geliştirme için ikili karşılaştırma matrisi 48
Çizelge 4.9. Mevzuat kriteri için normalize edilmiş matris 49
Çizelge 4.10. Saldırı Öncesinde Risk Yönetimi 49
Çizelge 4.11. Nükleer tesisler için siber tehdit değerlendirmesi 50
Çizelge 4.12. Nükleer tesisler için siber TET 50
Çizelge 4.13. Saldırı öncesinde risk yönetimi kriteri için ikili karşılaştırma matrisi 50
Çizelge 4.14. Saldırı öncesinde risk yönetimi kriteri için normalize edilmiş matris 51
Çizelge 4.15. Eğitim ve farkındalığın artırılması 51
Çizelge 4.16. Eğitim ve farkındalığın arttırılması kriteri için karşılaştırma matrisi 52
Çizelge 4.17. Eğitim ve farkındalığın arttırılması kriteri için normalize matrisi 52
Çizelge 4.18. Savunma sistemi kriteri 53
Çizelge 4.19. Savunma Sistemi kriteri için ikili karşılaştırma matrisi 53
Çizelge 4.20. Savunma Sistemi kriteri için normalize matris 54
Çizelge 4.21. Acil müdahale ve siber olaya karşılık verme 54
Çizelge 4.22. Acil müdahale ve siber olaya karşılık verme karşılaştırma matrisi 54
Çizelge 4.23. Acil müdahale ve siber olaya karşılık verme normalize matris 55
Çizelge 4.24. Olay sonrası müdahale 55
Çizelge 4.25. Olay sonrası müdahale kriteri için ikili karşılaştırma matrisi 55
Çizelge 4.26. Olay sonrası müdahale kriteri için normalize matris 56
Çizelge 4.27. L sütun Vektörü 57

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil 3.1. Tipik nükleer tedarik zinciri katmanları 14
Şekil 3.2. Nükleer tedarik zincirinde siber risklerle mücadele..... 20
Şekil 3.3. Başarılı TIDs kullanımı için başarılması gereken 5 rol 21
Şekil 4.1. AHP formülasyon 40
Şekil 5.1. Siber güvenliğe ilişkin Kurumların rolleri..... 62
Şekil 5.2. Siber güvenliğe ilişkin Kurumların ve NTZ paydaşların tasarlanan rolleri ... 63

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılan bazı simgeler ve kısaltmalar açıklamaları ile birlikte aşağıda verilmiştir.

Kısaltmalar	Açıklamalar
ACSC	Avustralya Siber Güvenlik Merkezi
AHP	Analitik Hiyerarşi Prosesi
ANP	Analitik Ağ Prosesi
BİT	Bilgi İletişim Teknolojileri
CAC	Çin Siber Uzay Dairesi
CDA	Kritik Dijital Varlıkları
CEA	Fransız Alternatif Enerjiler ve Atom Enerjisi Komisyonu
CERN	Avrupa Nükleer Araştırma Merkezi
CERT	Bilgisayar Acil Durum Müdahale Ekibi(Avustralya)
CIAE	Çin Atom Enerjisi Enstitüsü
CIIP	Critical Information Infrastructure Protection
CSC	Siber Tedarik Zinciri
CSWG	Sözleşme Güvenliği Çalışma Grubu (CSWG)
IEM	Yıllık Bilgi ve Değişim Toplantısı
JAEA	Japon Atom Enerjisi Ajansı
JRC	Ortak Araştırma Merkezleri(AB)
KAERI	Güney Kore: Kore Atom Enerjisi Araştırma Enstitüsü
KIT	Karlsruhe Teknoloji Enstitüsü
LEEM	Lisans ve Uygulama Uzman Toplantısı
MAİ	Merkezi Alarm İstasyonu
NDK	Nükleer Düzenleme Kurumu
NISS	NSG Bilgi Paylaşım Sistemi
NSYÖA	Nükleer Silahların Yayılmasının Önlenmesi Anlaşması
NTG	Nükleer Tedarikçiler Grubu
NTZ	Nükleer Tedarik Zinciri
NWS	Nükleer Silah Sahibi Ülkeler
ONR	İngiltere Düzenleyici Kurumu

Kısaltmalar	Açıklamalar
RESA	Radyasyon Erken Uyarı Sistemi Ağı
SFSCM	Sustainable Food Supply Chain Management
TAEK	Türkiye Atom Enerjisi Kurumu
TID	Tamper Indicating Devices
URAP	Ulusal Radyasyon Acil Durum Planı
VZA	Veri Zarflama Analizi
ZK	Zangger Komitesi

1. GİRİŞ

Bilindiği üzere günümüzde siber güvenlik, ulusal ve uluslararası pek çok alanda odak noktası haline gelmiştir. Her geçen gün yüz değiştiren tehdit senaryolarına karşı yeni savunma sistemleri geliştirilmektedir. Söz konusu düzenlemelerle birlikte nükleer tedarik zincirinin her bir halkasını ilgilendiren siber güvenlik gereklilikleri ortaya çıkmaktadır. Bu tezin öncelikli gayesi nükleer tedarik zincirinde yer alan dijital öğelerin sabotaj, veri hırsızlığı vb. kötü niyetli faaliyetlere karşı korunması ve bu amacın akabinde bu kötü niyetli faaliyetler karşısında farkındalığın arttırılmasıdır. Bununla birlikte seçilen dört ülkenin nükleer tedarik zinciri için analitik model tabanlı bir uygulama kullanılarak nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörleri sıralanması ve en iyi siber güvenlik sistemine ait ülkenin seçilmesidir.

Nükleer sanayi; uzun zamandır sahte parçalar ve tedarik edilen ürünlerin kalite kontrolü konusunda endişeliydi. Ancak günümüz dünyasında artık bilgisayar teknolojilerinin gelişmesiyle birlikte kalite kontrolünün yanı sıra bu endüstri de siber açıdan risk altındaki parça ve hizmetlerin olasılığı da göz önünde bulundurmalıdır. Dolayısıyla tedarik zincirine yönelik siber saldırılar nükleer sanayide kalite kontrolünden daha önemli bir problem haline gelmiştir.

Ülkemizin de üye olduğu Uluslararası Atom Enerjisi Ajansı (UAEA) , BM altında kurulmuş ve nükleer konularda üye ülkelere düzenleyici faaliyetler konusunda yol gösteren bir kurumdur. Mevcut durumda, “Nükleer Tedarik Zincirinde Siber Güvenlik” konusu da hem UAEA‘ nın hem de uluslararası camianın yeni yeni üzerine eğildiği bir konu olma özelliğindedir. Dolayısıyla böyle bir konunun çalışılması hem ulusal hem de uluslararası alanda önem arz etmektedir. Nükleer alandaki siber güvenliğe ilişkin çalışmalar nükleer tesis odaklıdır [1-3], yine literatürde nükleer tedarik zinciri konusunda çalışmalar mevcuttur [4] ancak odağında siber güvenlik bulunmamaktadır. Siber tedarik zinciri veya tedarik zincirinde siber güvenlikle ilgili çalışmalar mevcuttur [5-6] ancak nükleer bu konulara dahil edilmemiştir. Bu tezde ele alınan Nükleer Tedarik Zincirinde Siber Güvenlik konusu hem bu üç ayrı disiplini tek bir çatı altında toplayarak konuyu etraflıca ele aldığı için özgün bir çalışmadır, hem de çok ölçütlü karar verme konusunu bu başlıkla birleştirdiği için daha önce çalışılmamış bir konudur ve literatüre bilimsel bir katkısı olacağı açıktır.

UAEA'nın siber alandaki çalışmalarının amacı, Tedarik Zinciri için bilgisayar güvenliğini araştırmak, özellikle tedarik sırasında tehlikeye düşerse nükleer güvenliği olumsuz etkileyebilecek ürün ve hizmetlerin bilgisayar güvenliğini uygulamak ve değerlendirmek şeklindedir.

Bu tezde dünyanın çeşitli yerlerinden ülke uygulamalarına [7-9] ve uzman değerlendirmelerine yer verilmiştir. Böylece bu çalışmanın Türkiye'nin nükleer altyapısının güçlendirilmesine de fayda sağlayacağı düşünülmektedir. Siber güvenliğe dair tecrübeyi arttırması, siber güvenlik ile tedarik zinciri yönetimi arasında köprü kurulması ve oluşturulan analitik model tabanlı uygulama ile nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerinin sıralanması bakımından nükleer tedarik zincirinde siber güvenliğin sağlanmasına ilişkin hazırlanan bu tezin ülkemizin yakın zamanda yöneteceği nükleer tedarik zinciri yönetimine katkı sağlayacağı açıktır.

Bu tez, genel başlıkları siber güvenliğe dair, plan ve programların gereksinimleri, ulusların deneyimleri [5-6,10], Uluslararası Atom Enerjisi Ajansının (UAEA) önerileri [4,11-13] ve siber güvenlik ile alakalı ülkemiz mevzuatındaki yapılabilecek iyileştirmeler [14] konusunda bilgi vermektedir. Ayrıca dünden bugüne tedarik zincirindeki öğelere yönelik düzenlenen siber saldırılara ve bu saldırı etkilerine yer verilmiştir.

Bu tez esasen üç ana başlık altında anlatılmış olup ilk olarak literatürde yapılan çalışmalara, Sonraki ana başlık olan materyal ve metot kısmında, tedarik zinciri ve tedarik zinciri yönetimi başlığı altında temel kavramlara [15], tedarik zinciri, tedarik zinciri yönetimi ve nükleer tedarik zincirini oluşturan hususlara yer verilmiştir.

Sonrasında nükleer tedarik zinciri yönetimi konusu ele alınmış, bir önceki ana başlıkta anlatılanlardan ayrı olarak tedarik zinciri yönetimi konusu UAEA bakış açısı ile nükleer alanda ele alınmıştır. Akabinde nükleer tedarik zincirinde siber güvenlik ve temel tanımlar bölümünde ise nükleer tesislerde siber güvenlik, nükleer ihracat kontrol rejimi ve siber güvenlik, araştırma laboratuvarları ve siber güvenlik, nükleer tedarikçiler ve alt tedarikçilerde siber güvenlik ilişkisi, düzenleyici kurumlar ve siber güvenlik, teknik destek kuruluşları ve siber güvenlik, acil müdahale organizasyonları ve siber güvenlik, taşımacılık organizasyonları ve siber güvenlik konularına değinilmiştir. Sonraki alt başlıkta Çin, Rusya ve Güney Kore'nin uygulamalarına değinilmiştir.

Son ana başlıkta, seçilen dört ülkenin nükleer tedarik zinciri için analitik model tabanlı bir uygulama ile AHP yöntemi kullanarak nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerini sıralanmış ve A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir.) arasından en etkin siber güvenlik sistemine sahip ülke seçilmiştir.

2. LİTERATÜR ÇALIŞMALARI VE TARTIŞMA

Ürün yaşam döngüsünün iyice kısaldığı, hızlı tüketim çağında ve bu rekabetçi işletme koşullarında, işletmelerin artan müşteri taleplerine beklenildiği gibi cevap vermesi, bu süreçte yaşanan iletişim ve ulaşımdaki teknik gelişmelerle birlikte ortaya çıkan tedarik zincirinin halkalarının artışına yeni bir yönetimsel bakış getirmesi oldukça zordur.

"Bu zorluğa ek olarak, bilgi ve iletişim teknolojilerinde yaşanan gelişmeler uluslararası rekabeti arttırmakta ve daha önce göz önünde bulundurulmamış yeni tehlikeleri de beraberinde getirmektedir. Şüphesiz çağımızda bu tehditlerin başında siber tehditler gelmekte ve bu tehditler bilgisayar güvenliğinin önemini arttırmaktadır.

"Tedarik zinciri yönetiminde bilgisayarlar e-ticaret ile kullanılmaya başlamış bugün ise tedarik zinciri yazılımlarının kullanıldığı kurumsal bilgi sistemleri gelişimine devam etmektedir" [15].

"İnternet sayesinde herhangi bir değerli ticari bilgiye herhangi bir yerden ve herhangi bir zamanda kolayca ulaşılabilir" [15]. ERP (Kurumsal Kaynak Planlama) yazılımlarının ve yöneticiye karar vermede destek sağlayan karar destek sistemlerinin kullanımı giderek artmaktadır. Bu durum aynı zamanda bilgi güvenliğini de tehlikelere açık hale getirmektedir.

İşletmelerin rekabetçi yapılarını sürdürebilmelerinde önemli olan diğer bir husus ise siber olaylar ile mücadeledir. Siber tehditlerin pek çok güdüleyicisi bulunmaktadır. Bu motivasyonlardan biri de işle ilgili rakip firmayı alıkoymak ve engellemektir. Günümüzde rakip firmalar bu motivasyonla siber araçları tehdit olarak kullanabilmektedir. Özellikle nükleer alana yönelik siber saldırı senaryolarına ilişkin örneklerde rekabet amacıyla bir firmanın diğerinden gerekli bilgileri topladığı, sistemde kimliğini gizleyerek kötücül yazılımlarla siber saldırıyı uygun vakit bulduğunda gerçekleştirdiği veya rakip firmaya firmanın ya da tesisin bir çalışanı imiş gibi girerek iç tehdit rolü oynadığı görülmektedir.

Bilişim teknolojilerinin kullanımının hızla artması beraberinde siber riskleri getirmiş ve doğal bir sonuç olarak siber güvenliğe verilen önem ve akabinde akademik olarak bu konuda yapılan çalışmaların sayısı artmıştır.

Nükleer tesislerde siber güvenliğe ilişkin makaleler literatürde yerini almış, Bıçakçı'nın Türkiye'de Siber Güvenlik ve Nükleer Enerji başlıklı çalışmasında siber saldırılara ve sonuçlarına değinilirken [2,16], bu siber tehditleri engellemeye yönelik tedbirlere ve savunma metotlarına UAEA kaynaklarında detayları ile yer verilmiştir [11]. Bu tezde de bu kaynaklardan faydalanılmıştır.

UAEA nükleer alanda pek çok konuda üye ülkelere rehberlik sağladığı gibi siber alanda olası tehditlerle başa çıkabilmek için düzenleyici kurumlara yayınladığı dokümanlarla rehberlik sağlamaktadır. UAEA 2016 yılında yayınladığı Conducting Computer Security Assessments ve henüz yayınlamadığı taslak dokümanı Computer Security for Nuclear Security (NST 045/NSGC 9 Draft) başlıklı dokümanlarında siber güvenlik değerlendirilmesinin nasıl yürütüleceğinden ve nükleer tesislerdeki siber güvenliğin uygulamasından bahsetmektedir [12-13]. Ayrıca NST 045 dokümanında strateji geliştirme ve uygulama konusuna yer verilmiştir.

1982 yılında Rusya'nın Kanada'da bulunan bir şirketten doğalgaz boru hatlarının kontrol edilmesinde kullanıldığı düşünülen bir yazılımı çalması tarihe ilk siber saldırı olarak geçmiştir. Nükleer açıdan siber olayları değerlendirdiğimizde, tarih 2010'u gösterdiğinde İran'daki nükleer tesislerdeki SCADA sistemlerine gerçekleştirilen Stuxnet saldırısı büyük yankı uyandırmıştır. Nükleer alanda daha önce duyduğumuz siber saldırılar ise; Amerika Birleşik Devletleri'ndeki (ABD) David Besse Nükleer Enerji Santrali saldırısı, Browns Ferry Nükleer Enerji Santrali saldırısı, Hatch Nükleer Enerji Santrali saldırısı şeklinde sayılabilir [2].

Bu teze bilgileri ile ışık tutan UAEA' nın Nükleer Tesislerde Siber Güvenlik [1] isimli kılavuzunda; düzenleyici kurumların siber güvenlik planını nasıl kuracağı, geliştireceği ve ilgili mevzuatın nasıl yapılanacağı ele alınmaktadır.

UAEA'nın Nükleer Tesislerde Siber Güvenlik [1] isimli kılavuzu ile hedeflenen düzenleyici kurumlar tarafından hazırlanacak olan nükleer tesisteki tüm güvenlik planında siber güvenliğin göz önünde bulundurulması ve bu kılavuzlar ışığında siber güvenlik planının ya da stratejisinin nükleer tesislere uyarlanması için rehberlik etmektir.

Bunun için bu dokümanda nükleer düzenleyici kurumlara yönelik bazı yaklaşım önerileri, yapılar ve nükleer tesisler için tasarlanmış uygulama prosedürleri bulunmaktadır. Bu kılavuzun diğer bir hedefi ise hali hazırda bir program var ise o programdaki denge problemlerini ve riskleri azaltmaktır [1]. Bu sebeple ülkemizde de bilgisayar güvenliğine ilişkin yasal düzenlemelerin hazırlanmasında ve iyileştirilmesinde, yükümlülüklerin belirlenmesinde bu doküman ve tezin faydalı olduğu düşünülmektedir.

Tezde faydalanılan bir diğer kaynak olan ajansın "Siber Güvenlik Olaylarına Karşılık Verme" başlıklı taslak doküman ise, nükleer-siber güvenlik olayı müdahale planının geliştirilmesi için rehberlik etmektedir. UAEA 2011 yılında bu konuda çalışmaya başlamıştır. NSS17, 2011 yılında basımı gerçekleştirilen dokümanı ilk yayımlanmış dokümandır. Bu tezde şu an taslak doküman olan ve hala çalışmaları devam eden yayınlardan da faydalanılmıştır.

Tezde ayrıca diğer ülkelerin siber güvenlik konusundaki uygulamalarına yer verilmiş, düzenlemeleri incelenmiştir. Gözden geçirilen tüm bu araştırmalar ve yayınlar sayesinde nükleer tedarik zincirindeki bilgisayar sistemlerinin hırsızlık ve sabotaj benzeri kötü niyetli eylemlere karşı korunmasıyla ilgili farkındalık uyandıracak, bilgi güvenliğine ilişkin stratejik plana ve mevzuata katkı yapabilecek bir tez hazırlanmıştır.

Literatürde yer alan çalışmaların karşılaştırılması ve bu tezin literatüre katkısı aşağıdaki tablo ile verilmiştir:

Çizelge 2.1. Literatür karşılaştırması

1.Disiplin	2. Disiplin	Çalışmalar
Nükleer	Tedarik Zinciri	IAEA. (2016). Procurement Engineering and supply chain guidelines in support of operation and maintenance of nuclear facilities. International Atomic Energy Agency.
Siber Güvenlik	Tedarik Zinciri	* Rongping, M. ve Yonggang, F. (2014). *Security in the cyber supply chain: A Chinese perspective.* Technovation, 34. * Kim, K.C. (2014). Issues of cyber supply chain security in Korea. Technovation, 34. * Security issues in the security cyber supply chain in South Africa * Windelberg, M. Objectives for managing cyber supply chain risk
Nükleer	Siber Güvenlik	* IAEA, 2011a, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No.17, International Atomic Energy Agency, Vienna * ISS&NTI (2017). Cyber Security at Nuclear Facilities: National Approaches,The Nuclear Threat Initiative. http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf?_=1466705014 adresinden erişilmiştir. * IAEA, 2011b, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC /225/Rev5), IAEA Nuclear Security Series No.13, International Atomic Energy Agency, Vienna
Nükleer Tedarik Zincirinde Siber Güvenlik		* IAEA Consultancy Meeting 13-16 Feb 2017(Computer Security In The Nuclear Supply Chain Draft Working Material) 1 Bu konu özelinde yayımlanmış bir çalışmaya rastlanmamıştır 2 Ayrıca ne siber güvenlik konusunda ne de nükleer alanda AHP gibi çok ölçütlü karar verme metodunun kullanıldığı bir çalışmaya rastlanmamıştır.

Ülkemizin de üye olduğu Uluslararası Atom Enerjisi Ajansı (UAEA), 169 üyesi olan BM altında kurulmuş ve nükleer konularda üye ülkelere düzenleyici faaliyetler konusunda yol gösteren bir kurumdur. UAEA üye ülkelerle işbirliği sağlar ve Ülkemizin nükleer alanda uyduğu standartlar, uyguladığı mevzuat hükümlerinde UAEA' nın dokümanlarından

faydalanılmaktadır. UAEA'nın "IAEA SAFETY GLOSSARY" dokümanında nükleer güvenlik ve nükleer emniyet kavramları aşağıdaki gibi tanımlanmıştır [17]:

Nuclear safety:

The achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation risks.

Often abbreviated to safety in IAEA publications on nuclear safety. Safety means nuclear safety unless otherwise stated, in particular when other types of safety (e.g. fire safety, conventional industrial safety) are also being discussed. See protection and safety for a discussion of the relationship between nuclear safety and radiation protection.

Nuclear security:

1. The prevention and detection of, and response to, criminal or intentional unauthorized acts involving nuclear material, other radioactive material, associated facilities or associated activities.

2. The prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive material or their associated facilities.

Ülkemizde nükleer alanda düzenleyici kurum olarak görev yapan Kurum Nükleer Düzenleme Kurumu'nun uyguladığı mevzuatta, Nükleer Tesislerin ve Nükleer Maddelerin Fiziksel Korunması Yönetmeliği'nde, nükleer emniyet ve nükleer güvenlik tanımları ise aşağıdaki gibi tanımlanmıştır [18].

Nükleer emniyet, nükleer madde ve nükleer tesisleri hedef alan hırsızlık, sabotaj, yetkisiz erişim ve diğer kötü niyetli girişimleri engellemek, tespit etmek ve gerektiğinde karşılık vermek üzere gerekli fiziksel koruma önlemlerinin alınmasını ve etkinliğinin sürdürülmesini,

Nükleer güvenlik, Nükleer tesislere ilişkin faaliyetler sırasında birey, toplum ve çevrenin radyasyondan korunmasını sağlamak üzere uygun koşulların oluşturulması, kazaların önlenmesi veya kaza sonuçlarının hafifletilmesini" ifade etmektedir.
Dolayısıyla Nükleer Düzenleme Kurumunun tabi olduğu mevzuatta "security" kavramı "emniyet", "safety" ise "güvenlik" olarak çevrilmiştir. Bununla birlikte uluslararası literatürde "cyber security" olarak geçen kavram Türkçe kaynaklarda "siber güvenlik" olarak çevirilmiştir.

Türkçe kaynaklardaki çeviri ile mevzuatta yer alan hükümlerin farklılığından doğacak karışıklıkların önüne geçmek amacıyla bu tezde uluslararası literatürde "security" olarak anılan hususlar "güvenlik", "safety" kavramı ise "emniyet" olarak kullanılmıştır. Mevzuattan yapılan alıntılarda ise orijinal metindeki hali korunarak alıntı yapılmıştır.

3. MATERYAL VE METOD

Tedarik zinciri denilince ilk akla gelen sırasıyla hammaddenin sağlanması, o hammedeler kullanılarak mamul ve yarı mamullerin üretilmesi, montajı, son ürünün o ürünü talep eden müşterilere ulaştırılması ve bu süreçte yer alan üreticilerin, dağıtıcıların oluşturduğu bir değerler kümesidir. Bu zincirin her bir faaliyetinde kullanılan araçlardan birisi de bilgi sistemleridir.

3.1. Nükleer Tedarik Zinciri Yönetimi

"Tedarik Zinciri Yönetimi, hammadde temininden üretime ve dağıtımla son müşteriye kadar bir malın ulaşabilmesi için bir değer zincirinde yer alan tedarikçi, üretici, dağıtıcı, perakendeci ve müşteriler arasında malzeme/ürün, para ve bilginin yönetimidir" [19]. Tedarik zinciri yönetiminde diğer unsurlar ve bilgi yönetimin önemli olduğu kadar bilgi güvenliğinin yönetilmesi de önemlidir. Tedarik zinciri, tedarikçiler müşterilerden uzakta olduğu zaman aradaki mesafeyi kapatmaya yaramaktadır. Bu konuda en önemli araç kullanılan bilişim teknolojileridir" [15].

Bilişim teknolojilerinden faydalanırken bilginin geçerliliği, bütünlüğü ve erişilebilirliği korunmalıdır. Bu hususta bilgi teknolojilerinin kullanımıyla birlikte saldırılara açık hale gelen tedarik zincirinin siber tehditlere karşı etkin bir savunma mekanizması geliştirmesi ve tedarik zincirini oluşturan her bir halkada bu siber güvenlik kültürüne gereken önem verilmelidir. Tedarik zincirinin herhangi bir halkasında oluşacak bilgi güvenliği zafiyeti tüm sistemi etkileyecektir.

Günümüz iş dünyasında giderek zorlaşan rekabet koşulları, küreselleşme ve sürekli gelişen ve değişen bilgi ve iletişim teknolojileri, firmaların varlıklarını sürdürebilmelerini oldukça zorlaştırmaktadır. Gelecekte firmaların diğer şirketlere üstünlük sağlayabilmeleri ve ayakta kalabilmeleri, Tedarik Zinciri Yönetiminde ne kadar başarılı olduklarıyla ölçülecektir. Tedarik zinciri yönetimi işletmelerin faaliyetlerinin başarılı olmasında önemli bir rol oynamaktadır. İhtiyaç olan doğru ürünü doğru zamanda doğru yerde temin etmelerinde etkin bir yol izleyebilmesi için tedarik zinciri yönetimi üzerine yoğunlaşmaktır. Söz konusu çabanın odağında ise tedarik sürecinin güvenli yönetilmesi yer almaktadır.

Tedarik zinciri hammadde siparişinden teminine, üretiminden yeni ürünlerin müşterilere ulaştırılmasına varıncaya kadar süregelen faaliyetler zinciridir. Tedarik zinciri yönetimi ise; her bir öğenin iletişimini temin ederek, toplam maliyetleri minimize edecek ve toplam faydayı maksimize edecek tüm yaklaşımların ve modellerin ortaya konmasıdır.

Tedarik zinciri yönetiminde; karar vericinin karşılaştığı problemlerden ilki tedarikçi seçimi problemidir ve literatürde tedarikçi seçimine ilişkin analitik model tabanlı pek çok çalışma mevcuttur. Tedarikçi seçiminde tedarik edilen malın kalitesi fiyatı temin zamanı vb. dikkat edilen pek çok husus vardır. Ancak bunların yanı sıra tedarikçinin güvenliği de tedarik zincirinin güvenli olması açısından dikkat edilmesi gereken bir hususdur.

Tedarik zincirinde temel amaçlardan biri; müşterinin isteklerine uygun, en kaliteli malın en hızlı şekilde müşteriye ulaştırılmasıdır Bu yüzden doğru tedarikçilerle çalışılması önem arz etmektedir.

Tedarik zinciri, hammaddenin sipariş edilmesi ile başlayan, temin edilmesi, üretimde kullanılması, yeni ürün üretilmesi ve yeni ürünlerin müşterilere ulaştırılması aşamalarıyla devam eden zincirleme bir faaliyetler sürecidir. Tedarik zinciri yönetimi ise; her bileşenin bağlantılarını sağlayarak, toplam maliyetleri minimize edecek yaklaşımların ve modellerin oluşturulmasıdır.

Tedarik zinciri yönetiminde; karar vericinin karşılaştığı ilk engel, tedarikçi seçimi problemidir. Bir işletmenin günümüz rekabet koşullarında ayakta kalması ve sektöründe büyüyerek faaliyetlerini devam ettirebilmesi için doğru kaynaktan, istediği ürüne, en düşük maliyetle ulaşabilmesi gerekir. Ortaya çıkaracağı sonuçları bu denli önemli olan bir problemin çözüme kavuşturulması için karar verici, sezgileri kadar matematiksel ve objektif yöntemlere de başvurmalıdır. Bu hedef doğrultusunda karar verici ihtiyacını en doğru şekilde tanımlamalıdır. Önceliklerini kısıtlarını ve göze alabileceği risklerini iyi belirlemedir. Bu aşamadan sonra çözüm işleminin son basamağı ise olan doğru tedarikçi seçimi yöntemini bulup uygulamasıdır.

Bir işletmenin günümüz rekabet koşullarında ayakta kalması ve sektöründe büyüyerek faaliyetlerini devam ettirebilmesi için doğru kaynaktan, istediği ürüne, en düşük maliyetle ulaşabilmesi gerekir. Ancak konu nükleer alan olduğunda nükleer güvenlik hususu söz konusu diğer tüm amaçların önüne geçmektedir.

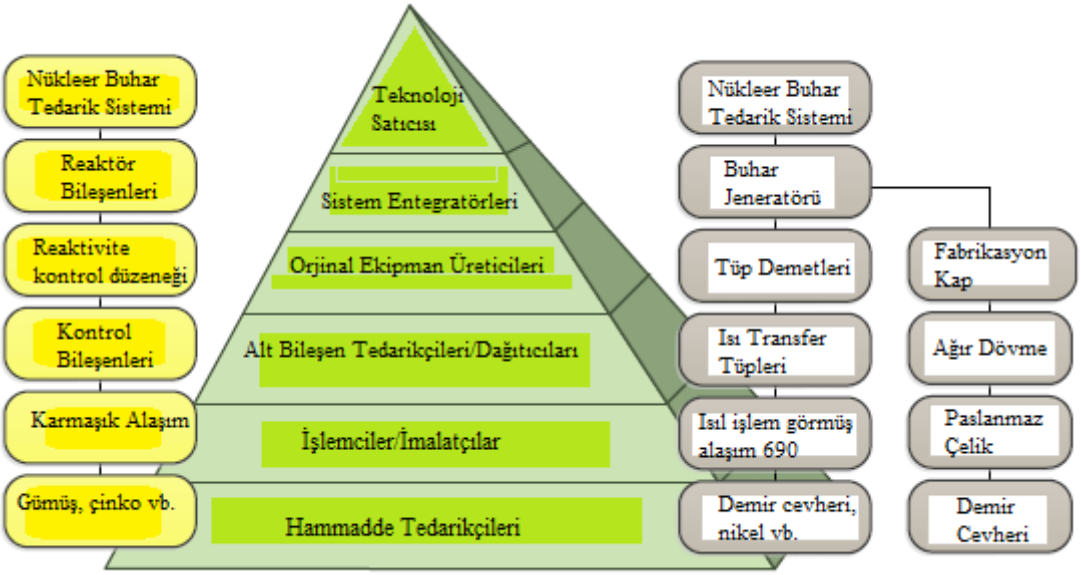
Ortaya çıkaracağı sonuçları bu denli önemli olan bir problemin çözüme kavuşturulması için karar verici, sezgileri kadar matematiksel ve objektif yöntemlere de başvurmalıdır. Bu hedef doğrultusunda karar verici ihtiyacını en doğru şekilde tanımlarken, nükleer güvenliği göz ardı etmemeli ve önceliklerini kısıtlarını ve göze alabileceği risklerini iyi belirlemedir.

Günümüzün rekabetçi işletme koşullarında ayakta kalmak için işletmeler tedarikçi seçimi yaparken maliyeti düşürmeye ve kaliteli malzeme tedariğine yönlenmektedirler. İşletmelerin unutmaması gereken en önemli husus belki de bu zincirin tek bir bütün olduğunun değerlendirilmesi ve sürecin gerçek kapasitesinin ancak tedarikçiden üreticiye tüm halkalardaki yetersizliğin takip edilerek bulunacağı ve önleneceğidir.

3.1.1. Nükleer tedarik zinciri

Ülkemizin de üye olduğu Uluslararası Atom Enerjisi Ajansı (UAEA) , 169 üyesi olan BM altında kurulmuş ve nükleer konularda üye ülkelere düzenleyici faaliyetler konusunda yol gösteren bir kurumdur. UAEA üye ülkelerle işbirliği sağlar ve ülkemizin nükleer alanda uyduğu standartlar, uyguladığı mevzuat UAEA' nın dokümanları örnek alınarak hazırlanmaktadır. UAEA, nükleer teknoloji uygulamaları, nükleer güvenliki ve nükleer güvenlik alanlarında faaliyet göstermektedir.

UAEA'nın tanımına göre; "Nükleer tesisler bağlamında, tedarik zinciri yönetimi, sadece bir ihale şartnamesi vermenin ve tekliflere cevap vermenin nispeten pasif bir rolünün aksine, bir işletme organizasyonundaki tedarik ve tedarik zinciri organizasyonları için aktif bir rol ifade eder. Dış tedarikçiler ile ve işletme organizasyonunun içinde değişen ilişkileri ve buna karşılık gelen süreçleri içerir. Tipik nükleer tedarik zinciri kademeleri şekilde gösterilmektedir. Yeni inşa projeleri tipik olarak birinci seviye teknoloji üreticilerinin tedarik zincirlerini nasıl kurdukları ve yönettiği ile ilgilidir, işletme tesisleri ise genellikle işlemle ilgili yedek parçalar için doğrudan seviye 3 ve altı ile ilgilenmektedir. Bu iki faaliyet her zaman birbiriyle bağlantılıdır, çünkü teknoloji satıcısı tarafından verilen kararlar ve satın alma seçimleri (örneğin, ana tedarikçilerin seçimi ve yeri) bir tesisin ömrü boyunca tedarik zinciri için etkileri olacaktır." [4]



Şekil 3.1. Tipik nükleer tedarik zinciri katmanları [4]

3.2. Nükleer Tedarik Zincirinde Siber Güvenlik

Siber güvenlik, bilgisayarlar, sunucular, mobil cihazlar vb. dijital sistemlerin, ağların ve verilerin kötü amaçlı saldırılardan korunmasıdır.

Siber saldırı, hassas bir sistemi veya hassas bilgi varlıklarını, duyarlı bir sisteme yetkisiz erişim (veya içindeki eylemler) aracılığıyla belirli bir hedefe erişim, erişimi engelleme veya yok etme amacıyla hedefleyen bireyler veya kuruluşlar tarafından gerçekleştirilen kötü amaçlı bir eylemdir. Hassas bilgi varlıkları kontrol sistemleri, ağlar, bilgi sistemleri ve diğer elektronik veya fiziksel ortamları içerir.

Bu tezin amacı tedarik zinciri süreçleri sırasında nükleer güvenliği olumsuz yönde etkileyebilecek herhangi bir ürün ve hizmet tehdit altındaysa bilgisayar güvenliğini uygulamak ve değerlendirmektir. Derinlemesine savunma ilkesi gereği nükleer tedarik zincirindeki dijital varlıklar siber tehditlere karşı korunmalıdır.

Nükleer tesisler, ekipmanı izlemek ve işletmek ve hayati bilgileri ele etmek ve saklamak için dijital ve analog sistemleri kullanır. Analog sistemler işlerini "fiziksel bağlantılı" yönergeleri izleyerek yaparlar, dijital bilgisayar tabanlı sistemler ise bellekte kayıtlı talimatları (yazılımı) izler. Ek olarak, çoğu tesis bilgisayarı sistemi, artık tesis genelinde genişleyen, güvenlik,

emniyet, kaza azaltma izleme ve acil durum hazırlık işlevlerini gerçekleştiren dijital ağlarla bağlantılıdır. Bu bağlantılar şimdi sıklıkla nükleer tesislerin dışına taşmaktadır [4].

BT endüstrisinde, bir sistemin saldırı yüzeyinin, izinsiz bir kullanıcının, saldırganın veri girmeye, veri çekmeye veya kontrol altına almaya çalışabileceği saldırı vektörleri olarak da bilinen farklı noktaların toplamı olduğu kabul edilir. Daha fazla İnternet tabanlı cihaz eklemek, saldırı yüzeyini avcılar için daha büyük hale getirebilir. Ticari endüstriyel üretim ortamlarına yönelik siber saldırılar, istenmeyen ihlaller, endüstriyel casusluk veya devlet destekli saldırılar dahil, önemli ölçüde artmıştır. Bu saldırılar planlanmamış aksama sürelerine, ekipman bulunabilirliğinde kesintilere ve üretim aksamalarına neden olabilir [4]

Bilgisayar güvenliği risklerini azaltmanın etkili bir yolu, diğer sistemlerin nükleer santral bilgisayar varlıklarını etkileme derecesini azaltmak ve diğer sistemler üzerindeki potansiyel etkilerini en aza indirmektir. Bu, teknoloji seçimleriyle veya varlıkların bağlantılarını mümkün olduğu kadar azaltarak yapılabilir. Bilgisayar güvenliği standartları, işletme ve süreç kontrol ağlarına karşı tehdit olarak üretilmiştir. Faaliyet organizasyonları, bazıları çeşitli uluslararası güvenlik standartlarına uyumu sağlamak için bilgisayar güvenlik programları oluşturmuştur. Ticari yazılım satıcıları, şirketlere bilgisayar güvenliği gereksinimlerinin karşılanmasını sağlamada yardımcı olacak araçlar üretmiştir (örneğin, veri toplama, masa üstü incelemeler, kontrol değerlendirmesi, saldırı vektör analizi, kayıt yönetimi ve dış tehdit yönetimi) [4].

Tedarik zinciri yönetiminde bilişim teknolojilerinin kullanılmasıyla işletmeler insan gücü, emek ve zamandan kar etmekte ve müşteri memnuniyetini de arttırmaktadır. Ancak konu nükleer ve nükleer tedarik zinciri olduğunda göz önünde bulundurulması gereken ilk husus nükleer güvenlik ve nükleer emniyet bunun sağlanması için de bilgi güvenliğinin korunmasıdır.

Enstrümantasyon ve kontrol (I&C) sistemleri nükleer tesislerin güvenli bir şekilde işletilmesinde kritik bir rol oynamaktadır. Dijital teknolojiler gelişmeye ve daha yetenekli hale gelmeye devam ettikçe, giderek daha fazla I&C sistemlerine dahil edilmekte ve entegre olmaktadır. Yeni nükleer tesisler ve modern nükleer tesis tasarımları, önceki I&C sistemlerinden daha az insan etkileşimi ve müdahalesini gerektirirken, çok sayıda proses verisini verimli ve aynı anda işlemek için yüksek düzeyde entegre dijital I&C sistemleri

kullanmaktadır. Dijital teknolojiler ayrıca mevcut tesislerin modernizasyonu sırasında sıklıkla I&C sistemlerine dahil edilmektedir. Ancak, I&C sistemlerinde dijital teknolojilerin uygulanması, bu sistemleri siber saldırılara karşı savunmasız hale getirmiştir [20].

I&C sistemlerine yapılan siber saldırılar nükleer tesislerin emniyetini ve güvenliğini tehlikeye atabilmektedirler. Nükleer maddelerin yetkisiz olarak taşınmasına veya sabotaja yardımcı olabilirler. Siber saldırıların güvenlikle ilgili I&C sistemleri üzerindeki etkileri, geçici bir süreç kontrolü kaybı veya kabul edilemez radyolojik sonuçlar gibi çok çeşitli sonuçlara yol açabilir. Halkın I & C sistemlerini etkileyen siber saldırılara karşı farkındalığı da nükleer tesislerin güvenliğine ve emniyetine zarar verebilir [20].

UAEA'nın " [11]" başlıklı klavuzu, düzenleyici kurumların yanı sıra nükleer tesis yönetimi, operasyonlar, bakım ve mühendislik personeli, I&C satıcıları, yükleniciler ve tedarikçiler, I&C tasarımcıları, araştırma laboratuvarları ve nükleer tesislerin emniyeti ve güvenliği ile ilgili diğer kuruluşlar dahil olmak üzere yetkili makamlara yöneliktir [20].

Bilgisayar güvenliği politikası, I&C sistemlerinin güvenliğini ele alan unsurlar içermeli ve sonuç olarak, politika I&C sistemi yaşam döngüsünde faaliyetlerden sorumlu olan tüm kuruluşlar için geçerli olmalıdır. Bu kuruluşlar arasında I&C sistemleri, yazılımları ve bileşenleri tasarlayan, uygulayan ve temin eden operatörler, satıcılar, yükleniciler ve tedarikçiler bulunmaktadır [20].

UAEA'nın "Computer Security of Instrumentation and Control Systems at Nuclear Facilities " başlıklı klavuzundaki tavsiyesine göre aşağıda bahsi geçen, 'satıcılar', 'yükleniciler' ve 'tedarikçiler' nükleer tesise, atanan güvenliğe uygun olarak bilgisayar güvenliğine kademeli bir yaklaşımın uygulandığı I&C sistemleri için dijital ekipman, yazılım ve hizmetler sağlayanlardır. İşletmeci, söz konusu satıcılar, yükleniciler veya tedarikçilerle bir sözleşme yürüterek aşağıdaki paragraflarında yer alan kılavuzun uygulanmasını sağlamalıdır [20].

Tedarikçi ve alt satıcı kuruluşlarının sağlam ve doğrulanabilir bilgisayar güvenlik süreçleri olmalıdır. Satıcılar, yükleniciler ve tedarikçiler, yürürlükteki tüm bilgisayar güvenlik gereksinimlerini karşılamalıdır. Bu, operatör tarafından, satıcı, yüklenici veya tedarikçinin işyerinde sağlanan destek sırasında ve satın alınan malların herhangi bir nakliyesi veya depolanması sırasında belirtilen bilgisayar güvenlik önlemlerinin uygulanmasını

içermektedir. Satıcı, yüklenici veya tedarikçinin bir bilgisayar güvenlik yönetimi süreci olmalıdır.
Bir satıcının, yüklenicinin veya tedarikçinin I&C sistemleri ile faaliyet yürüttüğü yerlerde geçerli bilgisayar güvenlik gereksinimleri, sistem, alt sistem veya bileşenin atanan güvenlik seviyesine göre operatör tarafından açıkça ve sözleşmeye bağlı olarak belirtilmelidir.

Operatörün ve tedarikçinin, yüklenicinin veya tedarikçinin güvenlik açıklarını birbirlerine rapor etmesine ve yanıt ve azaltma çabalarını koordine etmesine olanak tanıyan bir süreç mevcut olmalıdır. Satıcı, yüklenici veya tedarikçi, sözleşmeli hizmetlerinin tamamı boyunca güvenlik açıkları raporlarını almak, değerlendirmek ve nükleer tesise raporlamak için güvenilir bir mekanizmaya sahip olduğunu göstermelidir. Bu husus, kurulu ekipmanın kullanım ömrünü desteklemek için normal garanti sürelerinin ötesine geçebilir. Bu durumlarda mekanizma, satıcılar, yükleniciler veya tedarikçiler tarafından üzerinde anlaşmaya varılan sözleşme yükümlülükleri dahilinde uzun süre dahil edilmelidir.

I&C tasarım, geliştirme, entegrasyon ve bakımdan sorumlu satıcıların, yüklenicilerin veya tedarikçilerin denetlenmesi ve değerlendirilmesi yapılmalı ve sonuçlar operatöre rapor edilmelidir [20].

NST045 dokümanına göre hassas dijital varlıklar terimi (Sensitive digital assets /SDA), bu yayında bilgisayar tabanlı ve korunmaları için bilgisayar güvenlik önlemlerine ihtiyaç duyan hassas bilgi varlıklarını tanımlamak için kullanılmaktadır.

Bazen yetkili bir makam veya operatörün hassas bilgiler ve SDA'lar içeren hizmetler veya ürünler sağlamak için bir yüklenici, satıcı veya tedarikçiye ihtiyacı vardır. Bu tür düzenlemeler, lisans veya sözleşme gibi yasal anlaşmalar yoluyla yapılmalı ve uygun bilgisayar güvenliği gerekliliklerini içermelidir.

Yetkili makamlar ve operatörler, sözleşmelerini geliştirirken yüklenicilerin, satıcıların ve tedarikçilerin ürün veya hizmetleriyle ilgili benzersiz ve özel bilgilere sahip olacağını (örneğin; Orijinal sözleşme tamamlandıktan uzun süre sonra ortaya çıkabilecek ve gelişebilecek siber saldırılara karşı güvenlik açıkları hakkında) göz önünde bulundurmalıdır.

Yetkili makamlar ve operatörler, bu yükleniciler, satıcılar ve tedarikçiler için bilgisayar güvenlik planına özgü bilgisayar güvenliği gereksinimlerini ifade etmelidir. Bu, hem saha içi hem de saha dışı çalışmalar için gereksinimleri içerebilir.

Yetkili makamlar ve operatörler, örneğin sözleşmeli düzenlemeler dahilinde bilgisayar güvenliği için belirli sorumluluklar ifade etmeleri gerekebilir. Bu sözleşme düzenlemeleri aşağıdakileri içermekle birlikte bunlarla sınırlı değildir:

- Hassas bilgilerin ve diğer bilgilerin açıklanmaması
- Saklama ve imha şartları dahil olmak üzere hassas bilgiler için koruma gereksinimleri
- Bilgisayar tabanlı sistemlerde izin verilen erişim ve faaliyetlerin gerçekleştirilmesi
- Belirtilen bilgisayar güvenlik gereksinimlerine uymama cezaları
- Uzaktan erişim kısıtlamaları
- Sözleşme kapsamında sunulan hizmet ve ürünler için test gereklilikleri

Yetkili makamlar ve operatörler ayrıca müteahhitlerin, satıcıların ve tedarikçilerin nükleer güvenliği etkileyebilecek potansiyel tehditlerin ve güvenlik açıklarının tanımlanması da dahil olmak üzere bilgisayar güvenliği olaylarını zamanında bildirmelerini istemelidir. Raporlama yükümlülükleri ve protokolleri sözleşmenin bir parçası olmalıdır.

Bilgisayar güvenliği için hesap verebilirlik yüklenicilere, satıcılara ve tedarikçilere yüklenemez [13]. UAEA tarafından yayımlanan 13-16 Şubat 2017 tarihli Tedarik Zincirinde Bilgisayar güvenliği konusundaki rapora göre;

- "Nükleer güvenlik, ilgili tesis ve operasyonlardaki nükleer ve diğer radyoaktif maddeleri içeren kötü niyetli eylemleri önlemeyi, tespit etmeyi ve bunlara karşılık vermeyi amaçlamaktadır" [21].
- "Bilgisayarlar, bilişim sistemleri ve dijital bileşenler, bu tesislerde hassas bilgi yönetimi, nükleer güvenlik, nükleer güvenlik ve madde sayım ve kontrolünde sürekli genişleyen bir rol oynamaktadır." [21]

Bu tezde, siber güvenlik konusunda çeşitli ülkelerden foruma katılan uzmanların, tedarik zincirinde bilgisayar güvenliğini uygulama konusunda deneyimleri, öğrenilen dersler ve

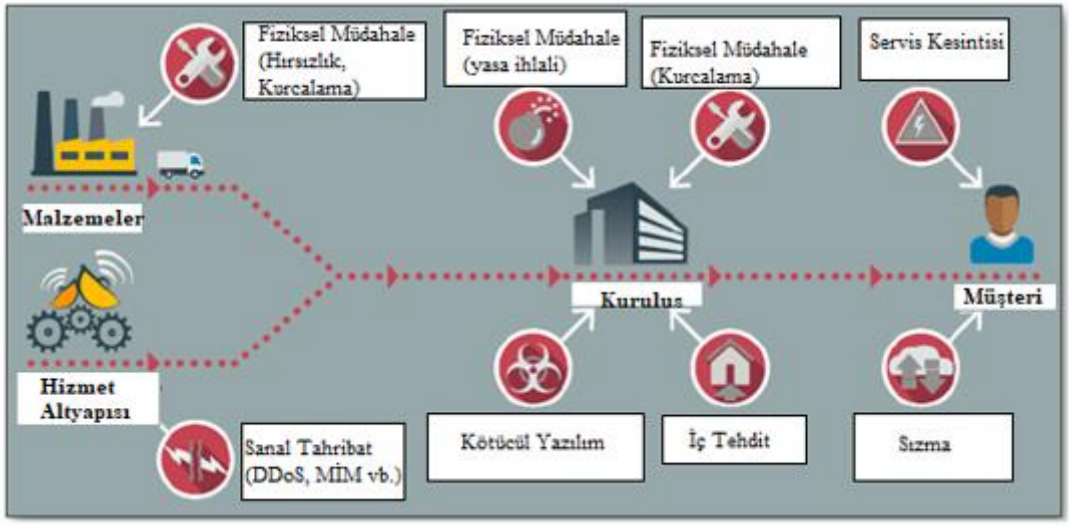
tavsiyeler hakkında yaptıkları sunumlara yer verilmiştir. Bu sunumlar, tedarik zinciri için bilgisayar güvenliği gereksinimlerinin sorunları ve zorluklarından bahsetmektedir.

Bu tezin amacı, tedarik zincirinde bilgisayar güvenliğini uygulamada tecrübe, öğrenilen dersler ve tavsiyelerin paylaşılması ve bilgisayar güvenliği gereksinimlerini ve tedarik zincirindeki zorlukları ele almak için iyi uygulamalardan, bilgisayar güvenliğinin uygulanmasında alınan derslerden ve önerilerden bahsetmektir.

Bay Matt Gibson tarafından gerçekleştirilen sunumda, raporda ifade edildiği üzere, Electric Power Research Institute (EPRI)'un siber güvenlik ve tedarik zinciri konusundaki çabalarına yer verilmiştir. EPRI topluma emniyetli, güvenilir, uygun maliyetli ve çevreye duyarlı elektrik sağlamak için güç sistemlerinin dönüşümünün daha esnek, esnek ve bağlantılı olmasını sağlayan yenilikçi çözümler sunmaktadır. Tedarik metodolojilerinin sayısız çeşidi vardır. Nükleer tesislerle ilgili bu yöntemlerden biri EPRI tarafından sağlanmaktadır. Metodoloji, siber güvenliği ve piyasaya hazır ticari veya özel geliştirme bileşenlerini ve sistemlerini içeren üç satın alma türünü ana hatlarıyla açıklamaktadır [21]. Üç satın alma türü:

- Katalog Satın Alma
- Basit Tedarik
- Karmaşık Tedarik

Yine raporda AREVA, DOE, CNL ve İngiltere tarafından yapılan sunumlara yer verilmiştir. AREVA'nın ilgili standartları (IEC 62443, ISO 27036), araştırma faaliyetleri (SMARTEST) ve tedarik zincirini korumak için Tamper Gösterge Cihazlarının kullanımı tartışılmıştır. Söz konusu sunumda nükleer tedarik zincirinde siber risklerle mücadele aşağıda verilen resimde özetlenmiş ve Tamper Indicating Devices (TID)aygıtlarından bahsedilmiştir [21].



Şekil 3.2. Nükleer tedarik zincirinde siber risklerle mücadele

“NPP için tedarik zincirindeki ihlaller yaşam, çevre ve altyapı üzerinde ciddi etkiye neden olabilir. Tedarik zinciri güvenliği için belirtilen standartlar:

- ISO 27036
- IEC 62443
- ISO / IEC 27002
- Amerika Birleşik Devletleri Nükleer Düzenleyici Kuruluşu düzenlemeleri” [22]

Bilgi Teknolojisi (BT) sistemlerinin vaktinden önce Endüstriyel Kontrol Sistemlerine dahil edilmesi, siber güvenlik açıklarını ve siber saldırı olasılığını artırır. Bir saldırganın erişim elde etmek için kullanabileceği 5 ana vektör:

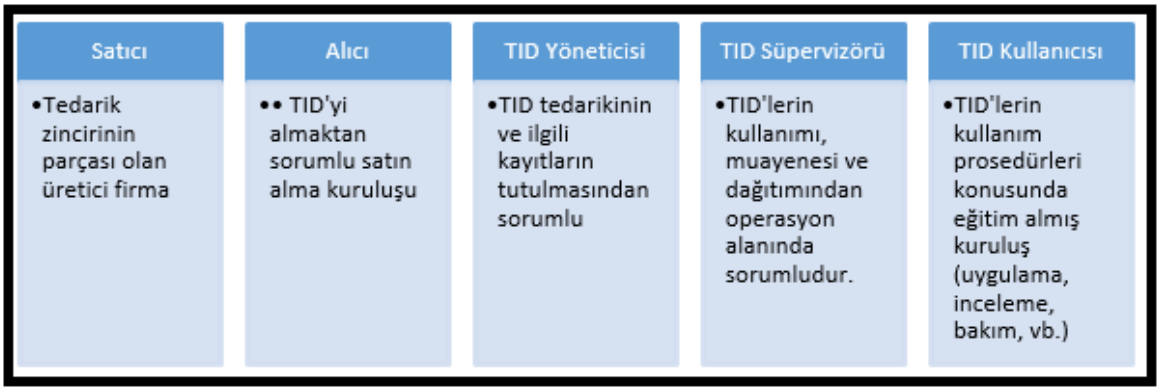
- Doğrudan ağ bağlantısı,
- Kablosuz ağ özelliği,
- Taşınabilir ortam ve ekipman,
- Tedarik zinciri
- Doğrudan fiziksel erişim şeklindedir.

Güvenlik kontrolleri, bir saldırganın erişim elde etmek için kullanabileceği 5 ana vektörü ortadan kaldırarak bu Kritik Dijital Varlıkları (CDA) korumanın bir yoludur. Ancak bu

durumda bir takım risk ve fırsatlar mevcuttur.” [22] Risk (Zorluk), gerekli teknik işlevlerden yoksun olduğu için tüm CDA'lar çeşitli güvenlik kontrollerini desteklemez.

Fırsat, bu tür CDA'larla ilgili zaafiyetleri başarılı bir şekilde azaltabilen alternatif bir denetim, dış müdahale gösteren aygıtları (Tamper Indicating Devices/TID) kullanarak bir program uygulamaktır.

TID aygıtları, özel nükleer maddelerin madde kontrol ve sayımında ve siber kaynaklı kurcalama izlerini izlemede görevli personele yardımcı olmak amaçlı ek bir savunma katmanı getirmede kullanılırken yetkisiz erişimi durdurmak ve önlemekte kullanılmaz. TID'leri uygulamak için önce sahaya özgü ihtiyaçları, endişeleri ve koşulları göz önünde bulunduran bir programın geliştirilmesi gerekmektedir.



Şekil 3.3. Başarılı TIDs kullanımı için başarılması gereken 5 rol [22]

Nükleer Güç Santrali Tedarik Zincirinde TIDs Kullanımı tedarikçi sahasında ve taşıma sırasında olmak üzere iki şekildedir. İlki, tedarikçi sahasında güvenlik testlerinin sonuçlarını garanti etmek için tasarım ile uygulanan TID'lerdir.

İkincisi ise taşıma sırasında malzemeyi taşırken, Nükleer Güç Santrali ürünün kurcalanmadan kalmasını sağlamalıdır. Gerçek zamanlı TID'lerin kullanılması, örneğin hem güvenli tedarik zinciri korumasını hem de kurcalama tespitini sağlayabilmektedir [22] Bahsi geçen rapora göre, İngiltere Düzenleyici Kurumu (ONR), UAEA NSS yayınlarıyla tutarlı bir çerçeve geliştirmiştir. İngiltere düzenleyici çerçevesinin Temel İlkeleri, Teslimat İlkeleri ve Teknik Değerlendirme Kılavuzları vardır. Bu çerçeve, operatörlerin uyumlu programlar geliştirmeleri için yeterli ayrıntı sağlamaktadır. Güvenlik ve sözleşmeleri içeren

metodolojiler hakkında tartışma için ulusal bir forum sağlayan bir Sözleşme Güvenliği Çalışma Grubu (CSWG) da bulunmaktadır.

3.2.1. Nükleer tesislerde siber güvenlik

Her geçen gün gelişen ülkemizin ekonomisi büyüdükçe buna bağlı olarak enerjiye olan talebimiz ve akabinde elektrik tüketimi artan bir ivme göstermektedir. Ülkemiz elektrik tüketim talep artışında dünyada ilk sıralarda yerini almaktadır. Yükselen bu talep sebebiyle ülkemizin hedefinde enerji tedarikinde dışa bağımlılığın en alt düzeye indirilmesi, yeni ve yenilenebilir kaynaklara yönelme şüphesiz yerini almaktadır. Bu hedefin odağında ise nükleer güç santralleri bulunmaktadır [14].

Nükleer güç santrallerinin kullanım alanları arasında elektrik üretimi dışında sanayi, tıp ve tarım gibi alanlar da mevcuttur. Nükleer güç santrallerinin inşaat ve işletme aşamasında bu büyük proje pek çok sektörü direkt ve dolaylı yoldan etkileyecektir. Nükleer güç santralleri sayesinde Türkiye'de kalite yönetim standartlarının uygulanması, standartlara uygunluk denetimi ile güvenlik ve emniyet kültürünün gelişmesine de sağlayacağı katkı ekonomi, teknoloji ve istihdama sağlayacağı katkı kadar önemlidir. Dolayısıyla en az tesisin tasarımı ve işletilmesi kadar bu santrallerin nükleer güvenliğini garanti altına almak da önemli bir husustur.

Dijital sistemlerin her türlü kötü niyetli eyleme karşı korunması için kapsamlı bir siber güvenlik programı oluşturulmalıdır. Nükleer tesislere özgü bazı özel hususlar ortaya çıkabilmektedir. Bu hususlar:

- Nükleer tesisler, bilgisayar sistemleri veya kılavuzlarını dolaylı veya direk düzenleyebilen ulusal düzenleyici kurumlar tarafından belirlenen gereksinimlerle uyumlu olmak zorundadır.
- Nükleer tesisler diğer endüstrilerde genellikle dikkate alınmayan ek tehditlere karşı korunmak zorundadır. Böyle tehditler ayrıca nükleer sanayinin hassas doğası sebebiyle azaltılmak zorundadır [14].

3.2.2. Nükleer ihracat kontrol rejimi ve siber güvenlik

Ülkemizin de üye olduğu ve her sene bildriimde bulunduğu Zangger Komitesi (ZK) 1971 yılında nükleer malzemelerin nükleer silah üretimi için değil aksine endüstride barışçıl amaçlarla kullanımını desteklemek amacıyla kurulmuş olup bundan dört yıl sonra aynı şekilde Nükleer Tedarikçiler Grubu (NTG) kurulmuştur. 2000 yılında ülkemizin de üye olduğu NTG katılımcı ülkelerile her yıl iki kez düzenli toplantı gerçekleştirmekte ve bu toplantılar aracılığı ile nükleer malzemeler ile çift kullanımlı malzemelerin ihracatına ilişkin olarak ihracat kontrol listelerini belirlemektedir.

“NSG Bilgi Paylaşım Sistemi (NISS), Yıllık Bilgi ve Değişim Toplantısı (IEM) ve Lisans ve Uygulama Uzman Toplantısı (LEEM), NSG rejimi kapsamında işletilen bilgi paylaşım sistemlerinin unsurlarıdır. NISS, doğru bilgileri zamanında paylaşma ihtiyacına yanıt olarak yaratılmıştır. ABD Enerji Bakanlığı, NSG'nin tüm üye ülkeleri arasında bilgisayarlı bir bilgi paylaşım sistemi olan NISS'in gelişimine sponsor olmuştur. Üye devletlere çok çeşitli teknolojik bilgi ve politika seçeneklerine hızlı erişim izni verilmesi, NSG'nin etkinliğine katkıda bulunmuştur. Bu, bilgisayarlı ve sistemik bir bilgi paylaşım sistemi olduğundan, güvenli elektronik postalama sağlayabilir. Bu posta sistemi sadece belge ve kayıt sağlamakla kalmayıp aynı zamanda gayri resmi bir iletişim kanalı haline gelmiştir NISS, ortalama iki gün içinde NSG üye ülkelerine ihracat reddi bildirimlerini bildirerek bir inkâr raporlaması aracı olarak çalışmaktadır. Ayrıca, bu sistemden alınan veriler, proliferatörlerin etkileşim modellerini belirlemeye ve korunan maddelerin uygunluğa ilişkin endişelerin bulunduğu ülkelere ihraç edilmesi de dahil olmak üzere anormal vakaları tespit etmeye elverişlidir (ABD Genel Muhasebe Ofisi 2002).” [23]

ABD hükümetinin bilgisayarlı bir bilgi paylaşım sistemi kurma sponsorluğu, NSG'nin güvenli bir ağ veritabanına sahip olmasını ve üye ülkelere gerçek zamanlı bilgi sağlamasını sağlar. Amerika Birleşik Devletleri'ndeki Los Alamos Ulusal Laboratuvarı NISS'i kurdu ve NISS'in yukarıda açıklandığı gibi faydaları arasında, inkâr bilgisi ve proliferasyona duyarlı malzemelerin ve teknolojinin aktarılması gibi bilgilerin hızlı bir şekilde yayılması ve düzensiz ve yasadışı eşya ticaretini önlemek de vardır [23].

Olası bir tehlike durumunda en yakın zamanda NISS takımına haber verilmesi gerekmekte ve NISS takımının sizin NISS sertifikanızı iptal etmesi gerekmektedir. Yine ihracat kontrol

rejiminde olduğu gibi benzer şekilde nükleer madde sayım kontrol için de web tabanlı sistemler kullanılmaktadır.

Nükleer silahların yayılmasının önlenmesine yönelik Türkiye Cumhuriyetinin taraf olduğu ikili veya çok taraflı uluslararası anlaşmalar ile üyelik yükümlülüklerin yerine getirildiğinin teyit edilmesine nükleer güvence denilmektedir. 5 Mart 1970 yılında yürürlüğe giren ve Ülkemizde de 1979 yılında Parlamentomuz tarafından onaylanan Nükleer Silahların Yayılmasının önlenmesi Antlaşmasının amacı, nükleer silahların yayılmasını önlemek ve nükleer teknolojiyi barışçıl amaçlar için kullanmaktır. Ayrıca Uluslararası Atom Enerjisi Ajansı sorumluluğu altında güvence denetimi sisteminin kurulmasını içerir. Antlaşmaya 191 ülke taraftır. Hindistan, İsrail ve Pakistan bu antlaşmaya taraf değildir. 1 Ocak 1967 tarihinden önce nükleer silah ve patlayıcıya sahip olan ülkeler nükleer silah sahibi ülkeler olarak (NWS) kabul edilmiştir.

Nükleer silah sahibi olmayan ülkemiz NSYÖA'nın 3.maddesinin bir gereği olarak, Uluslararası Atom Enerjisi Ajansı ile 1 Eylül 1981 tarihinde "Güvence Denetimi Anlaşması'nı imzalamıştır. UAEA'nın ülkemiz sınırları içinde, yetki veya kontrolü altında bulunan bütün barışçıl nükleer faaliyetlerde kullanılan kaynak veya özel bölünebilir nükleer maddelerin nükleer silahlara veya diğer nükleer patlayıcılara dönüştürülmediğini doğrulamak amacıyla denetim yapma yetkisi vardır.

Devletler ve UAEA arasında zamanında iletişim için güvenli kanal oluşturan UAEA Güvence Devlet Bildirimleri Portalı (THE IAEA SAFEGUARDS STATE DECLARATIONS PORTAL) kullanılmaktadır. Portal, Devletlere ve bölgesel yetkililere deklarasyonlar ve Safeguard Dairesi ile iletişim kurmak. için güvenli ve etkin yöntem sunmaktadır [24].

Portal katmanlı bir yaklaşım kullanarak, iki faktörlü kimlik doğrulama ve uçtan uca şifreleme ile bilgi korumada en son kontrolleri uygular. Portal, aşağıdakilerin sunulması için kullanılabilir:

- Nükleer Madde Sayım Raporları,
- Ek Protokol Beyanları,
- Fesih, muafiyet talepleri ve önlemlerin yeniden uygulanması,

Bu Portal, Devlet veya bölge makamları ile IAEA Güvenlik Bölümleri arasında Güvenli Bilgi alışverişi için web tabanlı bir sistemdir. Eyalet Deklarasyon Portalı'na kayıt ve erişim, IAEA Üye Devletlerinin Tüm Daimi Görevlerindeki personel ve IAEA Üye Devletlerindeki yetkili makamlardaki kişilerle sınırlıdır [25].

3.2.3. Araştırma merkezleri ve laboratuvarları ve siber güvenlik

Dünyada başta Avrupa Nükleer Araştırma Merkezi (CERN)), Çin Atom Enerjisi Enstitüsü (CIAE, Çin H.C.), Bhabha Atom Araştırma Merkezi (Hindistan), Kurchatov Ulusal Araştırma Enstitüsü (Rusya F.), Karlsruhe Teknoloji Enstitüsü (KIT) (Almanya), Fransız Alternatif Enerjiler ve Atom Enerjisi Komisyonu (CEA, Fransa), Japon Atom Enerjisi Ajansı (JAEA, Japonya), Ortak Araştırma Merkezleri (JRC, AB), Argonne ve Los Alamos Ulusal Laboratuvarları (ABD), Kore Atom Enerjisi Araştırma Enstitüsü (KAERI, Güney Kore) olmak üzere pek çok AR-GE Merkezi nükleer alanda faaliyet göstermektedir.

Örnek olarak; Çin Atom Enerjisi Enstitüsü (CIAE); Nükleer fizik, Nükleer kimya ve radyokimya, Reaktör mühendisliği, Hızlandırıcı teknolojisi, İzotop teknolojisi, Radyasyon metrolojisi, Nükleer güvence teknolojisi ve radyasyondan korunma teknolojisi vb. konularda çalışmalar yürütmektedir [26].

Dünyanın en büyük parçacık fiziği araştırma laboratuvarı olan CERN Nobel ödüllerine de layık görülen çok önemli bilimsel buluşların yapıldığı bir merkezdir. CERN'e üye ülke sayısı 2014 yılı itibariyle 21'dir. CERN laboratuvarlarının temeli hızlandırıcılar ve detektörler üzerine kuruludur [27].

Bhabha Atom Araştırma Merkezi (BARC); BARC bünyesinde Reaktör teknolojilerinin geliştirilmesi, Nükleer yakıt tasarımı ve üretimi, kullanılmış yakıtların yeniden işlenmesi ve radyoaktif atık yönetimi, Radyoizotop uygulamaları, Radyasyon teknolojileri ve bu teknolojilerin sağlık, tarım ve çevreye uygulanması, Hızlandırıcı ve lazer teknolojileri, Elektronik, enstrümantasyon ve reaktör kontrolü ve malzeme bilimi vb. konularda çalışmalar gerçekleştirmektedir. Kurchatov Ulusal Araştırma Enstitüsü: Enerji Dönüştürme, Yenilenebilir Enerji, Enerji Depolama ve Enerji Dağıtımı, Verimli Enerji Kullanımı, Enerji

Sistemleri Analizi, Füzyon Teknolojisi, Nükleer Enerji ve Güvenlik alanlarında faaliyet göstermektedir [26].

Görüldüğü gibi dünyanın pek çok noktasında çeşitli nükleer araştırma merkezlerinde çok önemli, patent başvurusu yapılmış çalışmalar yürütülmektedir. Tedarik zincirinde süregelmiş rekabetçi ortamın doğurduğu savaş ortamında siber tehditlerin göz ardı edilmemesi gerekmektedir.

3.2.4. Acil müdahale organizasyonları ve siber güvenlik

22 Mayıs 2012 tarihli ve 28300 sayılı " Nükleer Tesislerin Ve Nükleer Maddelerin Fiziksel Korunması Yönetmeliği" gereğince; Merkezi Alarm İstasyonu (MAİ): Nükleer tesis yönetimi, kolluk kuvvetleri ve koruma görevlileri ile kesintisiz haberleşmeyi sağlayacak teknik özellikte donatılmış, alarmların sürekli olarak izlendiği ve değerlendirildiği bina veya odayı, ifade etmektedir [18]. Söz konusu yönetmeliğin 17. Maddesine göre; Yetkilendirilen kişi MAİ'yi herhangi bir tehdit durumunda dahi fonksiyonlarını yerine getirebilecek sağlamlıkta tasarımlamakla yükümlüdür. Dolayısıyla bu sistemlerin siber güvenlik açısından garanti altına alınması çok önemlidir.

702 sayılı KHK ve 3.5.2012 tarihli ve 28281 sayılı Resmi Gazete'de yayımlan Kimyasal, Biyolojik, Radyolojik ve Nükleer Tehlikelere Dair Görev Yönetmeliği gereği pek çok bakanlık ve kuruma radyasyon acil durumunda ulusal seviyede görev yapmak üzere sorumluluklar verilmiş ve Ulusal Radyasyon Acil Durum Planı (URAP)'nda bu sorumluluklar belirtilmiştir.

Acil durum hazırlığı kapsamında siber tehditler sebebiyle koordinasyonda yaşanacak herhangi bir aksama, bilgilere erişilememesi, bilgilerin değiştirilmesi, tahrip ve yok edilmesi acil durum müdahalesinin hedeflerine etkin bir şekilde ulaşamaması demektir.

Büyük çaplı müdahale gerektiren radyasyon acil durumlarında, Müdahale Koordinasyon Ekibi bünyesinde yapılacaklar URAP'ta detaylı verilmekle birlikte, URAP' a göre [28] Nükleer Düzenleme Kurumu (NDK) ve Türkiye Atom Enerjisi Kurumu (TAEK), Müdahale Koordinasyon Ekibine kendi kurumlarından katkı sağlayacaktır. Ayrıca kurumlar arasındaki iletişimin kolaylaştırılması için NDK ve TAEK'in birer personeli AFAD AADYM'de

görevlendirilecektir. NDK'da ve TAEK'te Radyasyon Erken Uyarı Sistemi Ağı (RESA) verileri izlenecektir. RESA ve tesisin radyasyon izleme sisteminden alınan bu veriler; Tesisten salınabilecek radyoaktif maddelerin bölgedeki dağılımına ve radyolojik sonuçlara ilişkin öngörü ve Laboratuvarlardan gelen numune analiz sonuçları da dikkate alınarak gerçekleştirilmesi gereken koruyucu eylem ve diğer müdahale faaliyetlerine ilişkin değerlendirme yapılacak ve Acil Durum Müdahale Yöneticisine müdahaleye ilişkin kararların alınmasında teknik destek sağlayacaktır.

Dolayısıyla Örnek olarak RESA'ya veya tesisin radyasyon izleme sistemine yapılacak herhangi bir siber saldırı bu sistemlerden alınan verileri ve bu veriler dikkate alınarak gerçekleştirilecek olan koruyucu eylem ve diğer müdahale faaliyetlerini tümden etkileyecektir.

Ayrıca bahsi geçen kurumların kendilerine acil bir durumla ilgili bildirim yapılmasından hemen sonra belirli bir süre içerisinde müdahale etme sorumluluğu verilmiştir. Var olan siber tehditler bu sürenin gecikmesine sebep olabilir.

Yine aynı şekilde URAP'ta [28] Nükleer Santraller için Örnek Acil Durum Eylem Seviyelerine yer verilmiştir. Nükleer santraller için genel acil durum, saha acil durumu, tesis acil durumu ve uyarı durumu olmak üzere dört farklı acil durum sınıfı tanımlanmıştır. Nükleer santralde genel acil durum, saha acil durumu ve tesis acil durumu ilan edilmesini gerektirecek olaylar için verilen örneklerden biri de Terör eylemleri gibi olaylar sonucunda reaktörün kritik güvenlik sistemlerinin izlenememesi veya kontrol edilememesidir. Dolayısıyla terör motivasyonlu siber saldırılar da bu kapsamda ele alınmalıdır.

URAP' ta yer alan bu bilgiler Acil durum organizasyonlarında da diğer nükleer tedarik zinciri halkalarında olduğu gibi siber güvenliğin sağlanmasının ne kadar önemli olduğunu doğrulamaktadır.

3.2.5. Taşımacılık organizasyonları ve siber güvenlik

Nihai hedef olan nükleer tedarik zincirinde siber güvenlik sisteminin bütünlüğünün korunması açısından taşıma güvenliğini sağlamak da zincirin diğer halkaları kadar önemlidir. Taşıma güvenliğine ilişkin olarak Ülkemizde radyoaktif kaynakların çalınması,

kaybolması, yetkisiz kişilerin eline geçmesi veya sabotaj gibi durumları önlemek üzere radyoaktif kaynakların güvenliğinin sağlanmasına yönelik ilkeleri ve lisanslı kuruluşlarca yerine getirilecek yükümlülüklere ilişkin 12.6.2018 tarihli Radyoaktif Kaynakların Emniyetine İlişkin Usul Ve Esaslar ile belirlenmiştir [29].

Gerek radyoaktif kaynağın yer değişikliği veya taşınmasına ilişkin bilgilerin gizliliği açısından gerek radyoaktif kaynağa ilişkin bilgiler, görevli personelin listesi, güzergâha ilişkin bilgilerin gizliliğine dair alınması gereken önlemler bu usul ve esasın 8.maddesinde detayları ile belirtilmiştir.

Yine aynı hususta Uluslararası Atom Enerjisi Ajansı (UAEA) tarafından 03-06 Eylül 2018 tarihleri arasında Avusturya'nın Viyana şehrinde gerçekleştirilen Nükleer Tesisler İçin Bilgisayar Güvenliği Uygulamalarının Yürütülmesi Üzerine Teknik Toplantı'da (Technical Meeting on Conducting Computer Security Exercises for Nuclear Security) taşıma güvenliğini konu alan bir vaka analizi çalışması gerçekleştirilmiştir. Senaryolarda üç perspektif sağlanmıştır; saldırgan taraf, savunmacı taraf, objektif gözlemci bakış açısıyla tüm senaryolar tek tek ele alınmıştır:

Türkiye'nin de katılım sağladığı taşıma güvenliği senaryosunda, Sezyum kaynağını kirli bombada kullanmak için bir terörist tarafından yönlendirilen A'dan B'ye giden ulusal nakliyat ele alınmıştır. Saldırının düzenlenmesinde aracı olarak Taşımacılık şirketinin araç takip sisteminin kesilmesi ve taşımayı yönlendirmek için içeriden birinin kullanılması şeklinde düşünülmüştür. Saldırının hazırlık aşamasında (preperation), saldırganın amacı nakliyecilerden bilgi edinmek ve kendisine bu konuda yardım edebileceği bir iç tehdit edinmek olacaktır. İç tehditlerin bazı seviyelerde erişim yetkisi de olduğu için saldırıyı kolaylaştırmaktadır

Saldırının engagement aşamasında ise, Saldırganın amacı; nakliye şirketinin ağına bu iç tehdit sayesinde ilk girişi gerçekleştirebilmektir. Bu aşamada yemleme mailleri kullanılmaktadır. Saldırgan IDS/IPS, güvenlik duvarları veya antivirüs programlarını aşmaya yönelik özel teknikler geliştirmektedir.

Presence aşamasında saldırgan gerekli tüm girişleri gerçekleştirirken, GPS verilerini başarılı bir şekilde kaydetmektedir. Bir yandan da sisteme sızıldığı savunmacı tarafça tespit edilip alarm ve karşılık verme durumuna geçmektedir.

Sonuç aşamasında ise saldırgan nihai hedefine ulaşmış ve sezyum kaynağını yakalanmadan yetkisiz bir şekilde elde etmiştir. Bu çalışma göstermektedir ki nükleer tesislerin siber tehditlere karşı savunulması ne kadar önemliyse taşımacılık organizasyonları da bir o kadar önemli olup, kritik sonuçlar doğurabilmektedir.

3.3. Dünyadaki Uygulamalar

3.3.1. Güney Kore

Bir siber tedarik zinciri (CSC), etkili bir değer zinciri oluşturmak için siber tabanlı teknolojilerle geliştirilmiş bir tedarik zinciridir. CSC'lerde ürünler, envanter, üretim ve lojistik konularında çok miktarda hassas bilgi işlenmektedir; bu nedenle, CSC teknolojilerinin kullanımında küçük bir güvenlik ihlali bile felaket olabilmektedir [5].

Bu teknolojiler evrensel olmasına rağmen, kullanımları evrensel değildir. Son yıllarda bilgi sistemleriyle ilgili artan güvenlik kazaları, CSC'lerin güvenliği konusunda endişelere yol açmıştır. Asya şirketlerinde örgüt kültürü, diğer ülkelerdeki şirketlerden farklıdır.

Asya firmaları CSC güvenliğiyle ilgili benzersiz zorluklar ve sorunlara sahiptir. Asya ülkeleri ve diğer ülkelerdeki şirketler hakkında değerli bilgiler edinmek için bu özel güvenlik konularının araştırılması gerekmektedir. Bu çalışmada, Kore merkezli küresel firmaların CSC güvenliğiyle etkileşimleri araştırılmıştır. Kore'de merkezi bulunan dört küresel şirket incelenmiştir [5].

Dört Koreli firmanın yöneticileri (Samsung Electronics, Hyundai Motors, LGElectronics ve POSCO) CSC güvenliği ile ilgili sorunları tespit etmiştir. Kore'ye özgü CSC güvenlik sorunları:

- Kore ve diğer ülkelerdeki şirketler arasında CSC güvenliğinde önemli bir teknolojik farklılık bulunmamaktadır.

- CSC güvenliği için kullanılan teknolojiler genel olarak dünya çapında standarttır. Piyasaya yeni ve faydalı bir güvenlik teknolojisi getirildiğinde, diğer küresel şirketler gibi Kore merkezli şirketler de hızla benimseme eğilimindedir. Çoğu CSC güvenlik sorunu taraması, teknoloji sorunlarından ziyade insan hatasıyla sonuçlanmıştır. Firma içindeki güvenlik ihlallerinin dış güvenlik ihlallerinden daha ciddi olduğu düşünülmektedir.

Kore merkezli şirketlerle diğer küresel şirketler arasında CSC güvenliği açısından önemli farklılıklar bulunmaktadır:

- Güvenlikten sorumlu çalışanlar,
- Şirket çapında politika ve uygulama politikası,
- Sistem arasındaki ilişki kalkınma şirketleri ve müşterileri,

Kore'de son yıllarda yaşanan ciddi güvenlik olaylarından ötürü, Kore merkezli şirketlerde yöneticiler giderek daha fazla CSC güvenliğini hayati olarak algılıamaktadır. Bu güvenlik olayları şunlardır:

- 2009 Temmuz: Finansal kurumlar ve diğer kuruluşlar dahil Cumhurbaşkanlığı Ofisi (theBlueHouse), Dağıtılmış Hizmet Reddi (DDOS) saldırısına uğramıştır. Bunun sonucunda meydana gelen hasar yaklaşık 50 milyon ABD Dolarıdır.
- 2011 Mart: Yaklaşık 40 gazete, yayın ve portal şirketi DDOS saldırısı nedeniyle kapanmıştır.
- 2011 Nisan: Bir bankadaki yaklaşık 300 PC ye zarar verilmiş ve banka sistemleri bilgisayar korsanları tarafından kapatılmıştır [5].

3.3.2. Rusya Federasyonu

Bilgi ve iletişim teknolojilerinin geliştirilmesi, Rusya ekonomisinin modernleşmesinin kilit bir yönüdür. Rusya BİT altyapısı ve internet erişimi konusunda gelişmiş ülkelere giderek yaklaşmaktadır.

BİT'in hızlı gelişimi ve çoğalması ile birlikte açılan fırsatlar sayesinde, kamu ve özel altyapıların kritik bileşenlerin güvenliğine yönelik sistemik tehditler giderek daha ciddi hale

gelmiştir. Buna göre, kabul edilebilir bir tedarik zinciri, siber güvenlik düzeyi ve ilgili riskleri yönetme, ulusal politikanın önceliklerine dönüşmüştür.

Tedarik zincirlerinin siber güvenliği içerisinde Stratejik düzenleme ve Yasal ve teknolojik düzenleme; hükümetin siber tedarik zincirlerinin güvenliğini sağlamada işlev gören kilit fonksiyonları arasındadır.

Son olarak Rusya bu alanda önemli ilerleme kaydetmiştir. Eyalet Duma (Parlamentonun alt odası) ve Güvenlik Rusya Federasyonu Konseyi, bu alan için çok önemli olan bazı stratejik dokümanları bulunmaktadır. Kişisel veriler ile ilgili federal yasa, ulusal ödeme sistemine ilişkin federal yasa, bilgi, bilgi teknolojileri ve verileri koruma ile ilgili federal yasalar siber tedarik zinciri katılımcılarının veri güvenliğine ilişkin sorumluluklarının alan ve derecesini tanımlamaktadır. Kritik bilgi altyapılarının korunmasını amaçlayan faaliyetlerin ana alanlarını ve ilkelerini belirlemektedir [10].

3.3.3. Çin Halk Cumhuriyeti

Siber tedarik zinciri, sistem son kullanıcıları, politikacılar, satın alma uzmanları, sistem entegratörleri, ağ sağlayıcıları ve yazılım/donanım tedarikçileri dahil olmak üzere siber altyapıya dahil olan / kullanan tüm kilit aktörler setini ifade eder. Bu, güvenlik konusundaki en büyük endişelerin bilgi güvenliğinden siber güvenliğe yayıldığı anlamına gelir [6]

Küreselleşmenin ve bilişimin gelişmesiyle birlikte, siber altyapı yavaş yavaş “stratejik bir sınıf” ve daha sonra “ulusal güvenlik” ilkesine sahip olan güvenlik altyapısı olarak ele alınmaktadır [6].

2012 yılından bu yana 50 den fazla ülke stratejik plan yayımlamıştır. Fakat siber tedarik zincirinde güvenlik, tıpkı iklim değişikliği gibi, tek başına bir ülkenin başarabileceği bir şey değildir, dünyadaki tüm paydaşların birlikte çaba sarfetmesi gerekmektedir.

Siber tedarik zincirinde güvenliği sosyo ekonomik gelişme ve ulusal güvenlik konusunda artan zorlukları getirmektedir. Bir taraftan bilgi ve veri erişiminden kaynaklı risk ulusal güvenliği büyük ölçüde tehdit etmektedir. Diğer yandan yazılım zafiyetleri, ağ saldırıları, kötücül yazılımlar ekonomik çöküş ile sonuçlanabilecek enerji, ulaşım, finans vb kilit sanayi

alanlarına zarar verebilir. Ayrıca geleneksel sosyal yönetim kalıpları ve gizliliğin korunması, e- ticaret ve sosyal ağların artışıyla birlikte ciddi tehditlerle karşı karşıyadır [6].

Çin'de Bilgi ve iletişim teknolojileri sanayisi son zamanlarda çok büyük bir gelişme göstermiş ve dünyanın en büyük BİT üreticileri ve ihracatçıları haline gelmiştir. Amerika'nın 140 milyar dolar iken ve OECD ülkelerinin tamamında 728 milyar dolarken, Çin'in 2011 yılında BİT ürünleri ve hizmetleri ihracatı 508 milyar Amerikan dolarına ulaşmıştır.

Çin'de siber kullanıcılar ve altyapı hızla büyümektedir. Aynı şekilde e-ticarette de Çin'de büyük bir ivmelenme görülmektedir. 2013 Haziran sonu itibariyle çevrimiçi alışveriş kullanıcıları Çin'de 271 milyona, çevrimiçi ödeme yapan internet kullanıcıları 244 milyona ulaşmış ve toplam internet kullanıcıların % 45,9 ve % 41,4 'üne denk gelmektedir. Bu sebeple Çin'deki siber tedarik zinciri büyük tehditlerle karşı karşıyadır. Çin bu konuda büyük çaba sarf etmekte ve siber uzay gelişmesi için yönetimsel bir sistem ve sağlıklı bir yasal çerçeve oluşturmaya gayret göstermektedir. Siber güvenlik ve ağ yönetimine odaklı toplam 54 tane kanun ve düzenlemesi bulunmaktadır.

Sosyal ve ekonomik gelişme için siber uzay giderek artan bir öneme sahiptir. Siber güvenlik ile ilgili araştırmalara daha fazla öncelik verilmelidir. Öncelikle, araştırma siber suçlarla mücadelede iki taraflı ve çok taraflı işbirliği ve kullanıcının gizliliğini korumaya teşvik etmek gibi uluslararası hukuku ve uluslararası ilişkiler perspektifinden küresel siber güvenlik yönetim sistemine odaklanılmalıdır. İkincisi, araştırmalar siber güvenlikle ilgili fiziksel ve teknolojik altyapının döşenmesi gibi küresel siber tedarik alanlarında inovasyon kapasite geliştirmeye odaklanmalıdır. Üçüncü olarak, araştırma sürdürülebilir bir siber güvenlik ekosistemi oluşturmak gibi sosyal yönetim perspektifinden teknoloji ve toplum etkileşimi üzerinde durulmalıdır.

4. ANALİTİK MODEL TABANLI BİR UYGULAMA

4.1. Çok Ölçütlü (Kriterli) Karar Verme

Çok kriterli karar verme, karar bilimlerinin bir alt dalıdır. Karar sürecini kriterlere göre modelleme ve analiz etme sürecine dayanır.

Çok kriterli karar verme sürecinde öncelikle problem tanımlanır, amaç ortaya konulur, bu amacı gerçekleştirmeye yönelik kriterler belirlenir. Kriterler belirlendikten sonra bu amacı gerçekleştirmeye yönelik birden fazla alternatif ortaya konması şarttır. Ayrıca kriterlerin birbiri ile çelişmesi gerekmektedir. İlk olarak ortaya konan alternatifler kriterlere göre değerlendirilir sonrasında ise genel bir karar verilir. Sıralama ve seçme problemlerinde kullanılan Promethee, AHP, ANP, VZA Electre vb metodlar çok kriterli karar verme yöntemlerinden bazılarıdır.

Bu yöntemlerden biri olan analitik hiyerarşi prosesi karar verme sürecinde nitel ve nicel kriterleri karşılaştırabilme özelliğindedir. Analitik hiyerarşi prosesi, ilk olarak 1980 yılında, Thomas L. Saaty, tarafından, çok kriterli kompleks problemlerin çözümü için geliştirilmiş bir yöntemdir [30].

Örnek olarak Yogesh Kumar Sharma ve diğerlerinin çalışmasında; gıda sektöründe emniyet ve güvenlik günümüzde büyük bir sorun olduğuna dikkat çekilmiştir. Şirketler, gıda kayıplarını en aza indirmek için güvenlik ve emniyet için büyük miktarda para harcamaktadır. Bu çalışma temel olarak sürdürülebilir Gıda Tedarik Zinciri Yönetimi'nde (SFSCM/ Sustainable Food Supply Chain Management) emniyet ve güvenliğin geliştirilmesine odaklanmaktadır [31].

İlk olarak, SFSCM uygulamasında güvenlik ve emniyetle ilgili dokuz başarı faktörü (SF) literatür taraması ve uzman görüşüne göre belirlenmiştir. Bu nedenle, yaygın olarak kullanılan çok ölçütlü bir karar verme (MCDM) aracı, bulanık analitik hiyerarşi prosesi (AHP), başarı faktörleri arasında göreceli önemi bulmak için bir yöntem olarak kullanılmıştır.

Ambalaj ve devlet politikaları, SFSCM'nin uygulanmasında güvenlik ve emniyette önemli başarı faktörleri olarak bulunur. Önerilen model, uygulayıcıların ve yöneticilerin sürdürülebilir bir gıda tedarik zincirini verimli bir şekilde uygulamada uzun vadeli stratejileri planlamalarına yardımcı olabilecek bir modeldir [31].

Bu tezde de benzer şekilde AHP Yönteminin kullanılarak nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörleri sıralaması yapılacaktır. Bir nükleer tedarik zincirinde siber güvenliğin geliştirilmesinde belirlenen en etkili kriterler:

- C_1 kriteri: Mevzuat geliştirme [14]
- C_2 kriteri: Saldırı öncesinde risk yönetimi [14]
- C_3 kriteri: Eğitim ve farkındalığın arttırılması [14]
- C_4 kriteri: Etkili bir savunma sistemi [14]
- C5 kriteri: Acil müdahale ve siber olaya karşılık verme [32].
- C6 kriteri: Olay sonrası müdahale [33]

4.2. Mevzuat geliştirme

Bu çalışmada Estonya, Avustralya, Çin, Fransa, Finlandiya olmak üzere 5 ülkenin mevzuat ve standartları incelenmiş ve bu çerçevede mevzuat geliştirmenin avantaj ve dezavantajlarına yer verilmiştir.

4.2.1. Estonya siber güvenlik yasaları

Avrupa Birliği, Birleşmiş Milletler ve NATO üyesi olan Estonya, 1995'lerin başında dijitalleşmeye başlamıştır. Estonya'nın Public Information Act, Personal Data Protection Act, Electronic Communications Act olmak üzere 3 adet siber güvenlik yasası ve 1999 yılında kurulan bir adet denetleme yetkisi verdiği kurumu (Estonya Veri Koruma Müfettişliği/ Estonian Data Protection Inspectorate) bulunmaktadır. 2001 yılında yürürlüğe giren Public Information Act yasasının amacı, toplumun ve herbir bireyin demokratik ve sosyal kurallar çerçevesinde genel amaçlı bilgilere erişiminin güvenliğini sağlamaktır. Bu yasa public bilgilere ulaşım ve kullanımı ile ilgili metot ve prosedürleri tanımlar. Ayrıca erişimleri kısıtlar ve yetkisiz erişimleri yasaklar.

2007 yılında yürürlüğe giren Personal Data Protection Act yasasının amacı bireylerin özel hayatına müdahale edebilecek ve kişinin hakları ve özgürlüğünü sağlayabilmek için kişilerin bilgilerini korumaktır. Bu yasa kişisel verilerin kullanılabilmesi ve saklanması için gerekli prosedür ve şartları tanımlar. Kişisel verilerin nasıl işleneceği, saklanacağı ve üçüncü kişilere nasıl paylaşılacağı yasa kapsamında belirlenmiştir.

2006 yılında yürürlüğe giren Electronic Communications Act yasasının amacı elektronik haberleşme ağlarının ve servislerinin gelişmesini teşvik etmek ve elektronik haberleşme hizmeti kullanıcılarının çıkarlarının korunması için gerekli şartların oluşturulmasıdır. Bu yasa e-ticaret, radyo frekans uygulamaları gibi elektronik haberleşme alanlarında kısıtlamalar ve yetkilendirmeler yapmaktadır.

2018 yılında yürürlüğe giren CyberSecurity Act siber güvenlikle doğrudan ilgili en önemli ve en son yasadır. Bu yasa, siber olayların önlenmesi ve çözülmesinin yanında, ağ ve bilgi sistemleri için gerekli olan gereklilikleri, sorumlulukları ve denetimleri kapsar. Bu yasa, tüm kamu ve özel sektör için siber olayları önleme, çözümleme ve iş sürekliliği için gerekli olan tüm organizasyonel, fiziksel ve teknolojik önlemlerin alınmasını zorunlu kılar. Bu kapsamda kurum ve kuruluşların risk yönetim sistemi, saldırı izleme ve tespit sistemi gibi mekanizmaların kurulmasını zorunlu kılar.

Bu yasa ve bu yasaya bağlı oluşturulan mevzuatlara göre tüm kurum ve kuruluşlar Estonya Bilgi Sistemleri Kurumu (RIA) ile koordineli bir şekilde çalışacaktır. Ayrıca RIA Kurumu tüm kamu ve özel sektör için bu yasa kapsamında denetim hakkına sahiptir [9].

4.2.2. Avusturalya siber güvenlik yasaları

Dünya'nın 6. en büyük ülkesi olan Avustralya'da hem operasyonel hem de idari anlamda siber güvenlik ile ilgili hemen her türlü yeteneği ve faaliyeti bünyesinde toplayan birim Avustralya Siber Güvenlik Merkezidir. ACSC (Australian Cyber Security Centre, ACSC):

- Avustralya'nın bilgisayar acil durum müdahale ekibi (CERT) olarak siber güvenlik tehditlerine ve olaylarına cevap verir,(7/24 izleme)
- Tehditlerle ilgili bilgileri paylaşmak ve esnekliği artırmak için özel ve kamu sektörü ile işbirliği yapar.

- Siber güvenlik bilincini artırmak için hükümetlerle, endüstriyle ve toplumla birlikte çalışır
- Tüm Avustralyalılara bilgi, tavsiye ve yardım sağlar.

ACSC, siber tehditlerin analizi, soruşturulması ve raporlanması da dahil olmak üzere ajanslar ve hükümetler arası koordinatör konumundadır. Ayrıca siber suç, siber terörizm ve siber savaş olaylarında ülkedeki ulusal güvenlik yeteneklerinin ve operasyonlarının yönetildiği birimdir [9].

4.2.3. Çin siber güvenlik yasaları

İlk olarak 2016 yılında siber güvenlik içim özel fon ayıran Çin'in Siber Güvenlik Yasası 1 Haziran 2017'de yürürlüğe girmiştir. Çin Siber Güvenlik Yasası, 79 maddeden oluşmaktadır. Kapsamı son derece geniştir ve internet güvenliğini düzenleyen, özel ve hassas bilgilerin korunmasını ve ulusal siber güvenliğinin korunmasını hedefleyen kapsamlı bir içeriğe sahiptir.

Ayrıca Çin Siber Uzay Dairesi (CAC) tarafından 11 Temmuz 2017 tarihinde bir kamuoyu yorumu için taslak CIIP(Critical Information Infrastructure Protection) Tüzüğü yayınlanmıştır [9].

4.2.4. Fransa siber güvenlik yasaları

Fransa'nın siber güvenlik konusundaki ilk yasası veri korunması kanunudur.1978 tarihinde kabul edilen bu kanun temel olarak bilgi teknolojilerinin her vatandaşın hizmetinde olduğu ve kişilerin kimliğini, haklarını, gizliliğini ve kişisel ve kamusal özgürlüğüne zarar vermemesi gerektiği üzerine kurulmuştur. Fransa, İsveç ve Hessen Eyaleti (Almanya) ile birlikte Avrupa'da bu alanda ilk yasal düzenlemeyi yapan ülkelerden birisidir. 1978 Kanunu sonrasında 1995/46 Yasasının da oluşturulmasında öncü olmuştur.

Bu yasa ile Fransa, Üye devletlerarasında kişilerin verilerini işlemeye izin verirken kişilerin bilgilerinin gizliliğini de şart koşmuştur [9].

4.2.5. Finlandiya siber güvenlik yasaları

1995 yılında AB'ye Katılan Finlandiya'da Bakanlıklar ve kamu kurumları, siber güvenlik stratejisini kendi idari şubelerinde uygulamaktan, siber güvenliğe ilişkin görevleri yerine getirmekten ve arz güvenliğini uygulamaktan ve geliştirmekten sorumludur.

Bakanlıklar, kurumlar ve kuruluşlar, Siber Güvenlik Stratejisinin uygulanmasına yönelik kaynakları faaliyet ve mali planlarına dahil etmekle sorumludur. Gelecek Güvenlik Komitesi (The Future Security Committee), Stratejinin uygulanmasını izler ve koordine eder. Hükümet Bilgi Güvenliği Yönetim Kurulu (VAHTI- The Government Information Security Management Board) merkezi hükümetin kilit bilgi güvenliği ve siber güvenlik yönergelerini işler ve koordine eder.

Ayrıca Finlandiya Savunma Bakanlığı tarafından hükümetin internet ağlarının güvenliğini sağlamak üzere gizli servis kurulmuştur. Dışişleri Bakanlığı'nın bilişim ağına yapılan 'ağır casusluk' saldırısının ardından harekete geçen Helsinki yönetimi, istihbarat teşkilatı SAPO'dan ayrı olarak yeni bir birim kurmuştur. Yeni kurulan bu birim, Hollanda istihbarat teşkilatı AIVD'den destek almaktadır [9].

"Finlandiya anayasası gereğince hükümet ve kamu idareleri insan hak ve özgürlüklerine riayet etmelidir. Buradan hareketle aynı temel haklar ağlar üzerinde de geçerli olmalıdır. Örneğin siber güvenliğin arttırılması yoluyla ağ kullanıcılarının gizliliği korunabilir. Dolayısıyla Finlandiya anayasasındaki bu temel bakış açısını siber güvenliğe de yansıtmıştır. Siber güvenlikle ilgili daha detay mevzuat şu şekildedir:

- Chapter 34 of the Criminal Code (Ceza kanununun 34.maddesi)
- The Territorial Surveillance Act (Bölgesel Düzenleme Yasası)
- The Readiness Act (Hazırlık Yasası)
- The State of Defence Act and the Act on the Defence Forces (Savunma ve Savunma Devleti Yasası)
- The Communications Market Act (İletişim Piyasası Yasası)
- The Act on the Protection of Privacy in Electronic Communications (Elektronik İletişimin Mahremiyetinin Korunması Yasası)" [7].

Ceza kanununun 34.maddesine (Chapter 34 of the Criminal Code) göre,bir bilgi veya iletişim sistemine zarar vermek, elektronik haberleşmenin teknik güvenliğini bozmak veya devre dışı bırakmak, veri işleyişini engellemek vb. suçlar en az 2 yıl hapis cezası ile cezalandırılır. Veri işlemeye engel olmak için herhangi bir cihaz bulundurmak ise 6 ay hapis cezası ile cezalandırılır.

Bölgesel Düzenleme Yasası, Bölüm 37 ise şu şekildedir: Bölgesel bir gözetim makamınca, Gizli bilgilerin başka bir bölgesel gözetim yetkilisine açıklanması bir makamın görevini yerine getirmesi için ancak zorunlu ise kabul edilebilir.

İletişim piyasası yasasının (The Communications Market Act) 72.maddesinde " İletişim ağı inşaatı ve bakım çalışmaları ve bilgi güvenliği ile ilgili tedbirlere yer verilmiştir:

Bir telekomünikasyon operatörü, şebeke inşaatı veya bakım çalışması veya bilgi güvenliği için gerekli olduğu durumda ancak kullanıcının izni olmadan bir telefon şebekesi abonesi bağlantısının kullanımını geçici olarak kesebilir veya kısıtlayabilir. Herhangi bir kesinti, kullanıcıya mümkün olduğunca az rahatsızlık verecek şekilde ve mümkün olduğunda önceden bildirilecektir.

Bir abone bağlantısı, bazı nedenlerden dolayı bir takvim ayında 48 saatten daha uzun bir süre kapalı ise, telekomünikasyon operatörü, kullanıcıyı, talep üzerine, bir aylık hizmet oranını iade eder veya makul bir geri ödeme yapar [8].

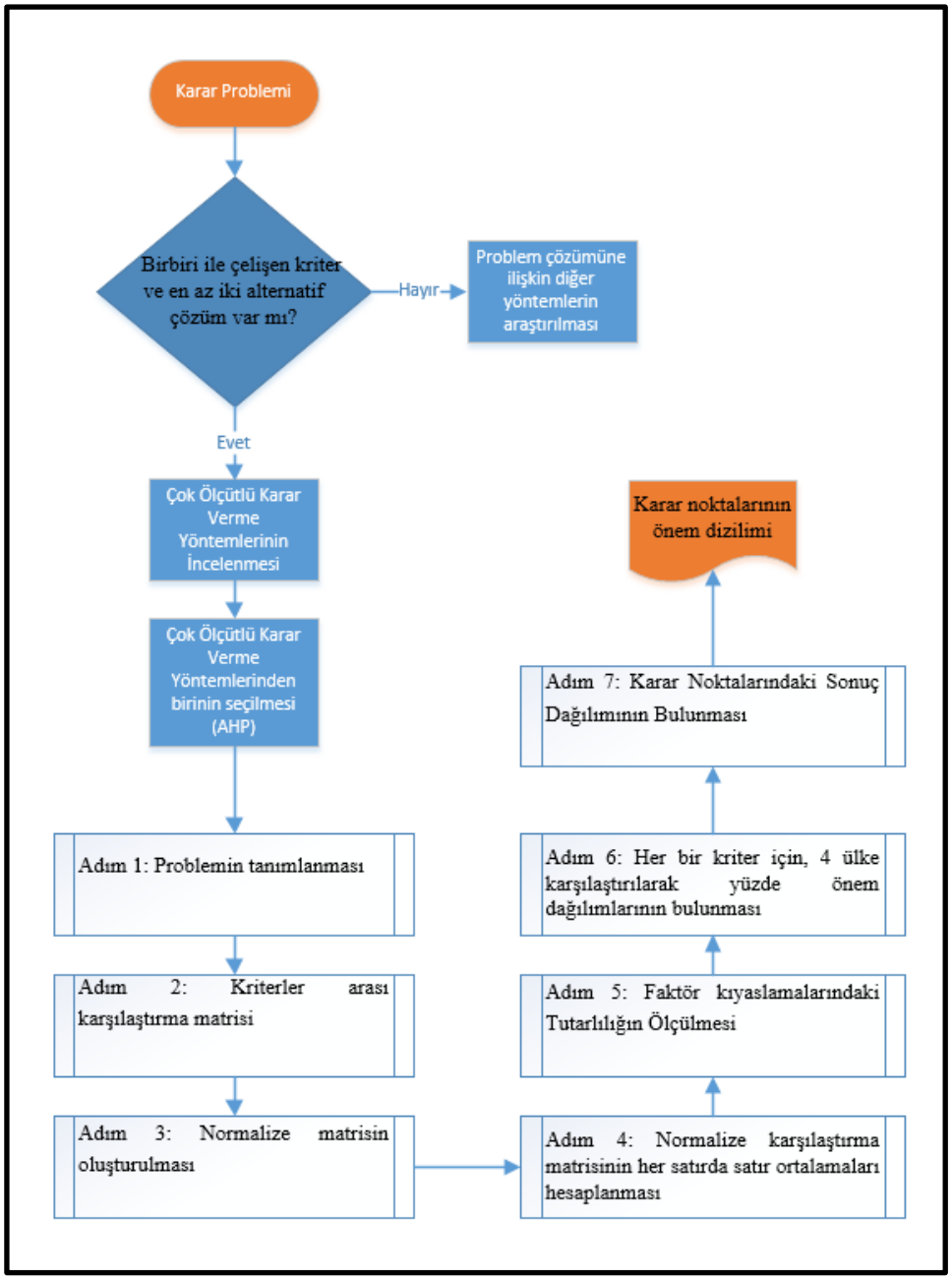
Elektronik İletişimin Mahremiyetinin Korunması Yasasının amacı Elektronik haberleşmede gizliliğin ve mahremiyetin korunmasını sağlamak ve e elektronik iletişim hizmetlerinin dengeli gelişimini sağlamaktır [9].

4.3. Örnek Uygulama

Örnek uygulamada A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir) için nükleer tedarik zinciri yönetiminde AHP yöntemi kullanılarak siber güvenliği geliştiren başarı faktörlerinin sıralanması ve en iyi siber güvenlik sistemine ait ülkenin seçilmesi planlanmıştır.

Analitik Hiyerarşi Prosesinde, karar verme süreci, belirli bir amacı gerçekleştirmek üzere hali hazırda var olan alternatifler arasından bir sıralama, seçim veya sınıflandırma sürecidir. Çok ölçütlü karar verme problemlerinde birden fazla birbiri ile çelişen kriter ve en az iki alternatif çözüm olması gerekmektedir.

Bu modelde Analitik Hiyerarşi Prosesi (AHP) kullanılarak A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir.) için nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerinin sıralanması ve bu bilgi ışığında hangi ülkenin nükleer tedarik zinciri yönteminde en iyi siber güvenlik sistemine sahip olduğunu ortaya çıkarmak amaçlanmıştır. Bir karar verme sürecinin AHP ile çözümlenebilmesi için gerçekleştirilmesi gereken aşamalar aşağıdaki şekilde tanımlanmıştır.



Şekil 4.1. AHP formülasyon

Yukarıda şekilsel olarak verilen AHP Çözümünün her bir aşaması formülasyon ile birlikte ilgili açıklamalar yapılmıştır.

Adım 1 (Problemin tanımlanması):_A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir) için nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerini sıralanması ve en iyi siber güvenlik sistemine ait ülkenin seçilmesi.

Adım 2: Kriterler Arası Karşılaştırma Matrisi: İlk olarak etkili bir siber güvenlik sisteminin unsurları belirlenmiştir. Bahse konu unsurlara ilişkin detaylı bilgi ve açıklamalara, ülke uygulamalarına bir önceki bölümde yer verilmiştir.

- C_1 kriteri: Mevzuat geliştirme
- C_2 kriteri: Saldırı öncesinde risk yönetimi
- C_3 kriteri: Eğitim ve farkındalığın arttırılması
- C_4 kriteri: Etkili bir savunma sistemi
- C_5 kriteri: Acil müdahale ve siber olaya karşılık verme
- C_6 kriteri: Olay sonrası müdahale

Belirlenen bu unsurların karşılaştırılması için alanında uzman kişilerce ekte yer verilen anket gerçekleştirilmiş, anket sonuçlarına göre kriterler arası karşılaştırma matrisi oluşturulmuştur. Bu matrisin köşegeni üzerindeki matris elemanları 1 olmalıdır. C_1,C_2,…Cn, kriterleri ; aij ise Ci kriteri ile Cj kriteri arasındaki değerlendirmeyi ifade etmektedir ve n*n boyutundaki (Bu problem için n=6 olmak üzere) A ikili karşılaştırma matrisi aij=1/aji ve aii=1 ilişkisi korunmak üzere aşağıda verilmiştir.

Çizelge 4.1. A matrisi

	C_1	C_2	C_3	C_4	C_5	C_6
C_1	1,000	3,000	5,000	2,000	4,000	6,000
C_2	0,333	1,000	3,000	0,500	2,000	4,000
C_3	0,200	0,333	1,000	0,250	0,500	2,000
C_4	0,500	2,000	4,000	1,000	3,000	5,000
C_5	0,250	0,500	2,000	0,333	1,000	3,000
C_6	0,166	0,250	0,500	0,200	0,333	1,000
Toplam	2,449	7,083	15,500	4,283	10,833	21,000

Bu matriste kriterler arasındaki üstünlük aşağıda verilen önem skalasına göre belirlenmiştir.

Çizelge 4.2. Önem Skalası

Önem Derecesi	Derece Tanımları
1	Her iki kriterin eşit öneme sahip olması durumu
3	1. kriterin 2. kriterden daha önemli olması durumu
5	1. kriterin 2. kriterden çok önemli olması durumu
7	1. kriterin 2. kritere nazaran çok güçlü bir öneme sahip olması durumu
9	1. kriterin 2. kritere nazaran mutlak üstün bir öneme sahip olması durumu
2,4,6,8	Ara değerler

Adım 3(Normalize Matrisin oluşturulması): Adım 2 de verilen A karşılaştırma matrisi, kriterlerin birbirlerine göre önem derecelerini göstermektedir. Bu kriterlerin bütün içerisindeki ağırlıklarını yani yüzde önem dağılımlarını belirlemek için karşılaştırma matrisini oluşturan sütun vektörlerinden yararlanılmıştır ve **n adet** ve **n bileşenli** B sütun vektörü oluşturulmuştur [34]. Aşağıda bu vektör gösterilmiştir:

$$B_i = \begin{bmatrix} b_{11} \\ b_{21} \\ . \\ . \\ . \\ b_{n1} \end{bmatrix} \tag{4.1}$$

B sütun vektörlerinin hesaplanmasında aşağıda belirtilen formülden yararlanılır:

$$b_{ij} = \frac{a_{ij}}{\sum_{i=1}^{n} a_{ij}} \tag{4.2}$$

B_1 Vektörünün diğer elemanları hesaplandığında, vektör aşağıdaki gibi elde edilebilir ve sütun vektörünün bileşenleri toplandığında toplam= 1 olmalıdır. Karşılaştırma matrisinin her elemanı kendi sütun toplamına bölünerek Normalize Matris (C Matrisi) karşılaştırma matrisi elde edilmiştir.

Çizelge 4.3. Normalize matris (C matrisi)

	C_1	C_2	C_3	C_4	C_5	C_6	Satır toplamı
C_1	0,408	0,424	0,323	0,467	0,369	0,286	2,276
C_2	0,136	0,141	0,194	0,117	0,185	0,190	0,963
C_3	0,082	0,047	0,065	0,058	0,046	0,095	0,393
C_4	0,204	0,282	0,258	0,233	0,277	0,238	1,493
C_5	0,102	0,071	0,129	0,078	0,092	0,143	0,615
C_6	0,068	0,035	0,032	0,047	0,031	0,048	0,260

Adım 4: Normalize karşılaştırma matrisinin her satırda satır ortalamaları hesaplanmıştır. Bu ortlama değerleri (W matrisi) kriterlerin göreli önemlerini ifade etmektedir. C matrisinden yararlanarak, faktörlerin birbirlerine göre önem değerlerini gösteren yüzde önem dağılımları elde edilebilir. Bunun için aşağıdaki formülünde gösterildiği gibi C matrisini oluşturan satır bileşenlerinin aritmetik ortalaması alınır ve Öncelik Vektörü olarak adlandırılan W sütun vektörü elde edilir [34].

$$w_i = \frac{\sum_{j=1}^{n} c_{ij}}{n} \tag{4.3}$$

$$W = \begin{bmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{bmatrix} \tag{4.4}$$

Yukarıdaki örnek çözüldüğünde öncelik vektörünün elemanları aşağıdaki gibi hesaplanabilir. Bu durumda aşağıda yer verilen öncelik vektörü (W ağırlık matrisi) oluşturulmuştur.

Çizelge 4.4. W matrisi

	C_1	C_2	C_3	C_4	C_5	C_6	Satır toplamı	Satır aritmetik ortalaması (W ağırlık matrisi)
C_1	0,408	0,424	0,323	0,467	0,369	0,286	2,276	0,379
C_2	0,136	0,141	0,194	0,117	0,185	0,190	0,963	0,160
C_3	0,082	0,047	0,065	0,058	0,046	0,095	0,393	0,065
C_4	0,204	0,282	0,258	0,233	0,277	0,238	1,493	0,249
C_5	0,102	0,071	0,129	0,078	0,092	0,143	0,615	0,102
C_6	0,068	0,035	0,032	0,047	0,031	0,048	0,260	0,043
	1,000	1,000	1,000	1,000	1,000	1,000		

Adım 5: Faktör Kıyaslamalarındaki Tutarlılık Ölçülür.AHP sonuçlarının geçerli olabilmesi için A: ikili karşılaştırma matrisinin tutarlı bir matris olması gerekmektedir. CR (Consistency Rate) ile gösterilen Tutarlılık Katsayısı ile bulunan öncelik vektörünün ve dolayısıyla kriterler arasında yapılan birebir karşılaştırmaların tutarlılığı test edilmiştir [34].

AHP, CR hesaplamasının özünü, faktör sayısı ile Temel Değer adı verilen (λ) bir katsayının karşılaştırılmasına dayandırmaktadır. λ'nın hesaplanması için öncelikle A karşılaştırma matrisi ile W öncelik vektörünün matris çarpımından D sütun vektörü elde edilir [34].

$$D = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ . & & & . \\ . & & & . \\ . & & & . \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} x \begin{bmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{bmatrix} \qquad (4.5)$$

Yukardaki formülde tanımlandığı gibi, Adım 2 de bulunan A matrisi ile Adım 4 te hesaplanan W öncelik vektörünün bulunan D sütun vektörü;

$$D = \begin{bmatrix} 2,356 \\ 0,986 \\ 0,395 \\ 1,546 \\ 0,622 \\ 0,263 \end{bmatrix} \tag{4.6}$$

D sütun vektörü ile W sütun vektörünün karşılıklı elemanlarının bölümünden her bir değerlendirme faktörüne ilişkin temel değer (E) elde edilir. Bu değerlerin aritmetik ortalaması ise karşılaştırmaya ilişkin temel değeri (λ) verir [34].

$$E_i = \frac{d_i}{w_i} \quad (i = 1,2,\ldots,n) \qquad \lambda = \frac{\sum_{i=1}^{n} E_i}{n} \tag{4.7}$$

$$E\ Matrisi\ (D/W) = \begin{bmatrix} 6,209799 \\ 6,14707 \\ 6,031489 \\ 6,211253 \\ 6,067598 \\ 6,062707 \end{bmatrix} \tag{4.8}$$

Tutarlılık Göstergesi (CI) (λ)=6,122 olmak üzere, aşağıdaki formülünden yararlanarak hesaplanmıştır.

$$CI = \frac{\lambda - n}{n - 1} \tag{4.9}$$

$CI = \frac{6{,}122 - 6}{6 - 1}$ ifadesine göre CI=0,024 olarak hesaplanmıştır.

Son aşamada ise CI, Random Gösterge (RI) olarak adlandırılan ve Tabloda gösterilen standart düzeltme değerine bölünerek CR elde edilir [34]. Tablodan kriter sayısına karşılık gelen 6 değeri seçilmiştir. Kullanılacak RI değeri Tablodan bakıldığında 1,24 olarak alınmıştır.

Çizelge 4.5. RI değerleri

N	RI	N	RI
1	0	8	1,41
2	0	9	1,45
3	0,58	10	1,49
4	0,90	11	1,51
5	1,12	12	1,48
6	1,24	13	1,56

$$CR = \frac{CI}{RI} \qquad CR = \frac{0{,}024}{1{,}24} \tag{4.10}$$

Hesaplanan CR=0,0197 değerinin 0,10'dan küçük olması bu karşılaştırmaların tutarlı olduğunu göstermektedir. Bu durumda Anket sonucu çıkan karara göre w matrisinde elde edilen ağırlıklara bakıldığında: $c_1 > c_4 > c_2 > c_5 > c_3 > c_6$ sonucu çıkmıştır. Yani;

- Mevzuat geliştirme c_1
- Etkili bir savunma sistemi c_4
- Saldırı öncesinde risk yönetimi c_2
- Acil müdahale ve siber olaya karşılık verme c_5
- Eğitim ve farkındalığın arttırılması c_3
- Olay sonrası müdahale c_6

Şeklinde bir sıralama olduğu görülmektedir.

Adım 6: Her bir kriter için, 4 ülke karşılaştırılarak yüzde önem dağılımları bulunmuştur. Bu aşama yukarıda anlatılan şekilde ancak bu kez, her bir kriter açısından alternatiflerin yüzde önem dağılımları (normalize matris) belirlenir. Diğer bir deyişle birebir karşılaştırmalar ve matris işlemleri kriter sayısı kadar (n=6 kez) tekrarlanır. Ancak bu kez her bir kriter için karar noktalarında kullanılacak G karşılaştırma matrislerinin boyutu mxm (m=4) olacaktır. Her bir karşılaştırma işleminden sonra $mx1$ boyutlu ve değerlendirilen faktörün karar noktalarına göre yüzde dağılımlarını gösteren S sütun vektörleri elde edilir. Bu sütun vektörleri aşağıda tanımlanmıştır [34]:

$$S_i = \begin{bmatrix} s_{11} \\ s_{21} \\ . \\ . \\ . \\ s_{m1} \end{bmatrix} \tag{4.11}$$

Mevzuat Geliştirme Kriteri (C1 Kriteri): A, B, C, D ülkelerine ilişkin olarak nükleer ile ilgili bir kanunun var olup olmadığı, var ise bu kanunun nükleer güvenliğe ilişkin referansları içerip içermediği sorgulanmış ve aşağıdaki tablolar elde edilmiştir.

Çizelge 4.6. Nükleer güvenlik mevzuatının özgünlüğü [3, 14]

Özellikler	Ülkeler
Nükleer kanun yok	D ülkesi
Nükleer güvenlik ile ilgili açık referanslar içermeyen veya hiç referansı olmayan genel bir nükleer kanun	C ülkesi
Nükleer güvenlikle ilgili açık referansları veya detaylı bölümleri olan genel bir nükleer kanun	-
Özellikle nükleer güvenliğe adanmış bir kanun	A ve B ülkesi

Çizelge 4.7. Nükleer mevzuat içerisindeki siber güvenlikle ilgili referanslar [3, 14]

Özellikler	Ülkeler
Siber güvenlik veya bilgi güvenliği veya gizliliğin korunmasından bahsetmeyen nükleer veya nükleer güvenlik kanunları	C ülkesi
Siber güvenlik veya bilgi güvenliği veya gizliliğin korunmasına açıkça gönderme yapan nükleer veya nükleer güvenlik kanunları	B ülkesi
Siber güvenliğe özel bölümlerde yer veren nükleer veya nükleer güvenlik kanunları	A ülkesi

Yukarıda verilen tablolar incelendiğinde; A ülkesi>B ülkesi>C ülkesi> D ülkesi olduğu görülmektedir. Mevzuat geliştirme için ikili karşılaştırma matrisi şu şekildedir:

Çizelge 4.8. Mevzuat geliştirme için ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	
A Ülkesi	1	3	5	7	
B Ülkesi	0,33	1	3	5	
C Ülkesi	0,2	0,33	1	3	
D Ülkesi	0,143	0,2	0,33	1	
Toplam	1,673	4,530	9,330	16	

Karşılaştırma matrisinin her elemanı kendi sütun toplamına bölünerek elde edilen normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S1 sütun vektörü ise aşağıdaki gibidir.

Çizelge 4.9. Mevzuat kriteri için normalize edilmiş matris

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S1 sütun vektörü
A Ülkesi	0,598	0,662	0,536	0,438	2,233	0,558
B Ülkesi	0,197	0,221	0,322	0,313	1,052	0,263
C Ülkesi	0,120	0,073	0,107	0,188	0,487	0,122
D Ülkesi	0,085	0,044	0,035	0,063	0,227	0,057
	1,00	1,00	1,00	1,00		

Saldırı Öncesinde Risk Yönetimi Kriteri (C2 Kriteri): Risk değerlendirmeleri yapılır. Penetrasyon testi, bir sistemde yer alan zafiyetlerin belirlenmesi ve tespit edilen açıklıklardan sistemlere sızma işlemidir. Tasarıma Esas Tehdit (TET) ise Fiziksel koruma sisteminin tasarımına temel teşkil eden, nükleer madde hırsızlığı veya sabotajla sonuçlanabilecek olan potansiyel olarak en güçlü tehdide denir [18].

A,B, C,D ülkelerini değerlendirmek ve karşılaştırmak için risk yönetimine ilişkin aşağıdaki tablolar verilmiştir.

Çizelge 4.10. Saldırı Öncesinde Risk Yönetimi

Özellikler	Ülkeler
1. Güvenlik Denetimleri (security audits) gerçekleştiriliyor.	A,B ülkesi
2. Zaafiyet Değerlendirme (vulnerability assessment)	A, B,C, D ülkesi
3. Sızma testleri(Penetration test)	A, B,C, D ülkesi

Çizelge 4.11. Nükleer tesisler için siber tehdit değerlendirmesi [3, 14]

Özellikler	Ülkeler
Siber tehdit değerlendirmesi yapılmadı.	D ülkesi
Siber tehdit değerlendirmesi gerçekleştirildi.	B ve C ülkesi
Siber tehdit değerlendirmesi yapılır, ulusal istihbarat girdisi alır ve düzenli olarak paydaşlara iletilir.	A ülkesi

Çizelge 4.12. Nükleer tesisler için siber TET [3, 14]

Özellikler	Ülkeler
Siber tehditler TET veya benzeri belgelerde dikkate alınmaz.	D ülkesi
Siber tehditler TET'e bütünleşmiş şekildedir.	B ve C ülkesi
Siber tehditler TET'ten ayrı olarak TET olmayan biçimde sunulmaktadır.	-
Siber TET, TET için ayrı bir tamamlayıcı belgedir.	A ülkesi

Tablolara bakıldığında; A ülkesi>B ülkesi>C ülkesi> D ülkesi (B ile C yakın) olduğu görülmektedir. Buna göre matris işlemleri gerçekleştirildiğinde Saldırı öncesinde risk yönetimi kriteri için için ikili karşılaştırma matrisi şu şekildedir:

Çizelge 4.13. Saldırı öncesinde risk yönetimi kriteri için ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi
A Ülkesi	1	3	4	6
B Ülkesi	0,33	1	2	4
C Ülkesi	0,25	0,5	1	2
D Ülkesi	0,166	0,25	0,5	1
Sütun toplama	1,746	4,750	7,500	13

Karşılaştırma matrisinin her elemanının kendi sütun toplamına bölünerek elde edilen Normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S2 sütun vektörü ise aşağıdaki gibidir:

Çizelge 4.14. Saldırı öncesinde risk yönetimi kriteri için normalize edilmiş matris

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S2 sütun vektörü
A Ülkesi	0,573	0,632	0,533	0,462	2,199	0,550
B Ülkesi	0,189	0,211	0,267	0,308	0,974	0,243
C Ülkesi	0,143	0,105	0,133	0,154	0,536	0,134
D Ülkesi	0,095	0,053	0,067	0,077	0,291	0,073
Sütun toplama	1,00	1	1	1		

Eğitim ve farkındalığın arttırılması kriteri C3: A, B, C, D ülkelerine ilişkin olarak nükleer ile ilgili o alanda çalışan personele Düzenli aralıklarla siber güvenliğe ilişkin eğitimlerin verilip verilmediği, farkındalık çalışmalarının gerçekleştirilip gerçekleştirilmediği, tatbikatlara yeterince önem verilip verilmediği sorgulanmış ve akademik programlara bakılarak aşağıdaki tablolar elde edilmiştir.

Çizelge 4.15. Eğitim ve farkındalığın artırılması

Özellikler	Ülkeler
Bilgisayar Güvenlik Sistemleri alanında Lisans Programı	B ülkesi
Bilgisayar Teknolojisi/Bilgi Güvenliği alanında Yüksek Lisans Programı	A ve B ülkesi
Bilgi Güvenliğine ilişkin Tatbikatlar	A,B, C ülkesi
Düzenli aralıklarla ilk ve güncelleyici güvenlik eğitimleri	A,B,C,D ülkesi

Tablolara bakıldığında; B>A>C>D olduğu görülmektedir. Buna göre matris işlemleri gerçekleştirildiğinde eğitim ve farkındalığın arttırılması kriteri için ikili karşılaştırma matrisi şu şekildedir;

Çizelge 4.16. Eğitim ve farkındalığın arttırılması kriteri için ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi
A Ülkesi	1	0,5	2	3
B Ülkesi	2	1	3	4
C Ülkesi	0,5	0,33	1	2
D Ülkesi	0,33	0,25	0,5	1
Sütun toplama	3,83	2,08	6,5	10

Karşılaştırma matrisinin her elemanının kendi sütun toplamına bölünerek elde edilen Normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S3 sütun vektörü ise aşağıdaki gibidir:

Çizelge 4.17. Eğitim ve farkındalığın arttırılması kriteri için normalize matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S3 sütun vektörü
A Ülkesi	0,261	0,240	0,308	0,3	1,109	0,277
B Ülkesi	0,522	0,481	0,462	0,4	1,865	0,466
C Ülkesi	0,131	0,159	0,154	0,2	0,643	0,161
D Ülkesi	0,086	0,120	0,077	0,1	0,383	0,096
	1	1	1	1		

Etkili Bir Savunma Sistemi C4: Savunma stratejileri göz önünde bulundurulmuştur.

Çizelge 4.18. Savunma sistemi kriteri

Özellikler	Ülkeler
Derinlemesine savunma stratejilerini benimseme	A ve B ülkesi
Hibrit saldırılara karşı fiziksel korunmanın yeterliliği, Fiziksel Korunma programında hibrit saldırılara yer verilmesi	A ülkesi
Güvenlik duvarı, Antivirüs, Sayısal imza, İçerik filtreleme vb. savunma sistemi unsurlarının etkin olarak kullanımı	A,B, C, D ülkesi

Tablolara bakıldığında; A>B>C=D (c ile d eşit, aile b yakın) olduğu görülmektedir. Buna göre matris işlemleri gerçekleştirildiğinde etkili bir savunma sistemi kriteri için ikili karşılaştırma matrisi şu şekildedir:

Çizelge 4.19. Savunma sistemi kriteri için ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi
A Ülkesi	1	2	4	4
B Ülkesi	0,5	1	3	3
C Ülkesi	0,25	0,33	1	1
D Ülkesi	0,25	0,33	1	1
Toplam	2	3,66	9	9

Karşılaştırma matrisinin her elemanının kendi sütun toplamına bölünerek elde edilen Normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S4 sütun vektörü ise aşağıdaki gibidir:

Çizelge 4.20. Savunma sistemi kriteri için normalize matris

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S4 sütun vektörü
A Ülkesi	0,500	0,546	0,444	0,444	1,935	0,484
B Ülkesi	0,250	0,273	0,333	0,333	1,190	0,297
C Ülkesi	0,125	0,090	0,111	0,111	0,437	0,109
D Ülkesi	0,125	0,090	0,111	0,111	0,437	0,109
	1	1	1	1		

Çizelge 4.21. Acil müdahale ve siber olaya karşılık verme c_5

Özellikler	Ülkeler
Acil müdahale ve siber olaya karşılık verme planının varlığı	A ve B ülkesi
Acil müdahale ve siber olaya karşılık verme organizasyonu kurulması	A ve B ülkesi

Tablolara bakıldığında; A=B>C=D olduğu görülmektedir. Buna göre matris işlemleri gerçekleştirildiğinde Acil müdahale ve siber olaya karşılık verme kriteri için ikili karşılaştırma matrisi şu şekildedir:

Çizelge 4.22. Acil müdahale ve siber olaya karşılık verme kriteri ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi
A Ülkesi	1	1	5	5
B Ülkesi	1	1	5	5
C Ülkesi	0,2	0,2	1	1
D Ülkesi	0,2	0,2	1	1
Toplam	2,4	2,4	12	12

Karşılaştırma matrisinin her elemanının kendi sütun toplamına bölünerek elde edilen Normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S5 sütun vektörü ise aşağıdaki gibidir:

Çizelge 4.23. Acil müdahale ve siber olaya karşılık verme kriteri için normalize matris

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S_5 sütun vektörü
A Ülkesi	0,417	0,417	0,417	0,417	1,667	0,417
B Ülkesi	0,417	0,417	0,417	0,417	1,667	0,417
C Ülkesi	0,083	0,083	0,083	0,083	0,333	0,083
D Ülkesi	0,083	0,083	0,083	0,083	0,333	0,083
	1	1	1	1		

Çizelge 4.24. Olay sonrası müdahale

Özellikler	Ülkeler
Etkin bir güvenlik kontrolü ve güvenlik programının varlığı	B ülkesi
Etkin olay bilgisi toplama	A,B, C ülkesi
Yaşanan her siber olay için gelecekte kullanılacak izleme raporunun oluşturulması	A,B, C ülkesi

Tablolara bakıldığında; B>A=C>D olduğu görülmektedir. Buna göre matris işlemleri gerçekleştirildiğinde Olay sonrası müdahale kriteri için ikili karşılaştırma matrisi şu şekildedir:

Çizelge 4.25. Olay sonrası müdahale kriteri için ikili karşılaştırma matrisi

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi
A Ülkesi	1	0,5	1	4
B Ülkesi	2	1	2	5
C Ülkesi	1	0,5	1	4
D Ülkesi	0,25	0,2	0,25	1
Sütun toplama	4,25	2,2	4,25	14

Karşılaştırma matrisinin her elemanının kendi sütun toplamına bölünerek elde edilen Normalize matris ve sonrasında satır ortalamaları alınarak elde edilen S6 sütun vektörü ise aşağıdaki gibidir:

Çizelge 4.26. Olay sonrası müdahale kriteri için normalize matris

	A Ülkesi	B Ülkesi	C Ülkesi	D Ülkesi	Satır toplamı	S6 sütun vektörü
A Ülkesi	0,235	0,227	0,235	0,286	0,984	0,246
B Ülkesi	0,471	0,455	0,471	0,357	1,753	0,438
C Ülkesi	0,235	0,227	0,235	0,286	0,984	0,246
D Ülkesi	0,059	0,091	0,059	0,071	0,280	0,070
	1	1	1	1		

Adım 7: Karar noktalarındaki sonuç dağılımının bulunmasıdır. Bu aşamada öncelikle, yukarıda anlatılan n tane mx1 boyutlu S sütun vektöründen meydana gelen ve mxn boyutlu K karar matrisi oluşturulur. Karar matrisi aşağıda tanımlanmıştır:

$$K = \begin{bmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ . & & & . \\ . & & & . \\ . & & & . \\ s_{m1} & s_{m2} & \dots & s_{mn} \end{bmatrix} \qquad (4.12)$$

Sonuçta karar matrisi W sütun vektörü (öncelik vektörü) ile aşağıdaki gibi çarpıldığında ise m elemanlı L sütun vektörü elde edilir. L sütun vektörü karar noktalarının yüzde dağılımını verir. Diğer bir deyişle vektörün elemanlarının toplamı 1 dir. Bu dağılım aynı zamanda karar noktalarının önem sırasını da gösterir.

$$L = \begin{bmatrix} s_{11} & s_{12} & \dots & s_{1n} \\ s_{21} & s_{22} & \dots & s_{2n} \\ . & & & . \\ . & & & . \\ . & & & . \\ s_{m1} & s_{m2} & \dots & s_{mn} \end{bmatrix} x \begin{bmatrix} w_1 \\ w_2 \\ . \\ . \\ . \\ w_n \end{bmatrix} = \begin{bmatrix} l_{11} \\ l_{21} \\ . \\ . \\ . \\ l_{m1} \end{bmatrix} \quad (4.13)$$

A,B,C, D ülkeleri için her bir kriter bazında yapılan karşılaştırmalar sonucu oluşan S sütun vektörleri matris formatında bir araya getirilmiş ve W vektörü ile çarpılmış ve L sütun vektörü elde edilmiştir:

Çizelge 4.27. L sütun vektörü

S1 sütun vektörü	S2 sütun vektörü		S3 sütun vektörü	S4 sütun vektörü	S5 sütun vektörü	S6 sütun vektörü		W matrisi		L Sütun Vektörü	
0,558	0,550		0,277	0,484	0,417	0,246		0,379		0,492	A
0,263	0,243		0,466	0,297	0,417	0,438		0,160		0,305	B
0,122	0,134		0,161	0,109	0,083	0,246	X	0,065	=	0,125	C
0,057	0,073		0,096	0,109	0,083	0,070		0,249		0,078	D
								0,102		1	
								0,043			

Bu durumda modelin sonucuna göre sıralama: A>B>C>D şeklindedir. Diğer bir deyişle karar noktalarının önem dizilimi A,B,C ve D şeklindedir.

5. SONUÇ

21. yüzyıla doğru yaygınlaşmaya başlayan bilgi teknolojileri kullanım alanlarındaki ilerlemeler; internet, telekomünikasyon ağları ve bilgisayar sistemlerini de içine alan siber uzayı ortaya çıkmıştır. Bu teknolojiler sayesinde dünyanın herhangi bir yerindeki bilgi merkezinden bilgi aktarabilmek mümkün hale gelirken devletler de iletişim ve bilgi alanındaki bu değişimi ve değişimin beraberinde getirdiği tehlikeleri göz önünde bulundurmaktadırlar. Dijitalleşme hayatımızı kolaylaştırırken, diğer yandan da yeni tehditlerin ortaya çıkmasına sebep olmuştur. Özellikle de kritik altyapılar üzerindeki siber tehditlerin ve buna karşı savunmanın önemi bir kat daha artmıştır. Üstelik mevcut tehditler her geçen gün daha karmaşık hale gelmekte ve çözülmesi için mutlaka uzmanlık gerektirmektedir. Bu uzmanlık ise siber güvenlik gereksinimlerini gün yüzüne çıkarmıştır.

Bu tezin amacı, nükleer tedarik zincirindeki bilgisayar ve dijital sistemlerin sabotaj, veri hırsızlığı vb. kötü amaçlı faaliyetlere karşı korunmasını sağlamaktır. Bu amaçla uluslararası çalışmalar incelenmiş, siber güvenliğin sağlanmasında göz önünde bulundurulması gereken hususlara ve sorumluluklara değinilmiştir.

Ayrıca tezin diğer bir amacı, AHP Yöntemi kullanılarak A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir) için nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerinin sıralanması ve en iyi siber güvenlik sistemine ait ülkenin seçilmesidir.

Nükleer tedarik zinciri yönetimi konulu başlık altında tedarik zinciri unsurlarından, tedarik zincirinde bilişim teknolojilerinin ve bilgi yönetimin rolünden, tedarik zinciri yönetiminde dikkat edilmesi gereken hususlardan ve tedarik zinciri yönetiminin öneminden bahsedilmiştir. Nükleer tedarik zinciri yönetimi başlığı altında ayrıca UAEA'nn temel faaliyet alanları ve teşkilat yapısına ilişkin özet bilgilere yer verilmiş ve UAEA 'nın bakış açısı ile tedarik zinciri tipik bir nükleer tedarik zincirinin katmanları ele alınmıştır.

Diğer bir ana başlık nükleer tedarik zincirinde siber güvenlik kısmında siber güvenlik, nükleer güvenlik ve gibi temel tanımlara yer verilmiş, nükleer tedarik zinciri tanımlanmış, siber güvenlik konusunda çeşitli ülkelerden foruma katılan uzmanların, tedarik zincirinde bilgisayar güvenliğini uygulama konusunda deneyimleri, öğrenilen dersler ve tavsiyeler

hakkında yaptıkları sunumlara yer verilmiştir. Ayrıca bu bölümde nükleer tedarik zincirini oluşturan her bir öğe ile siber güvenliğin ilişkisi tek tek incelenmiştir [35].

Nükleer tesislerde siber güvenlik konulu başlık altında siber güvenliğin önemi ve diğer alanlarla ilişkisi, nükleer tesisler için özel durumlar, metodoloji, mevzuata ilişkin göz önünde bulundurulacak hususlar, yönetim sistemleri, örgütsel konular, siber güvenlik uygulaması, yönetimi konuları incelenmiştir. Ayrıca düzenleyici denetim ve iç denetimlerin nasıl gerçekleştirileceği hususları ele alınmıştır. UAEA'nın öneri ve tavsiyeleri başta olmak üzere incelenen uluslararası mevzuat değerlendirilerek elde edilen bulgular sonucu, nükleer tesislerde siber güvenliğin işleyişinin nasıl olması gerektiği anlatılmıştır.

Nükleer malzemelere yönelik hırsızlık ve sabotaj, intikam, karışıklık, kargaşaya sebep olma, toplumda ve uluslararası alanda güvensizlik ortamı oluşturma gibi pek çok amaç güdebilen bu saldırılar kamuoyu imajını ve güvenini zedeleyebilmektedir. Dahası yapılan bu siber saldırılar savaş sebebi sayılarak ülkeyi çok büyük kargaşaya sürükleyebilir.

Tüm bu sebeplerle olası siber saldırılara karşı yetkili makamlar tedbirler almalı iyi bir savunma sistemi geliştirmelidir. Acil müdahale ve siber olaylara karşılık vermenin nasıl olması gerektiği üzerinde durulmalı, kritik altyapıların siber güvenliğinde alınabilecek önlemler dikkate alınmalıdır. Düzenleyici kurum olan NDK tarafından, kurum içi alınması gereken tedbirler belirlenmeli ve yetkilendirilen kişinin yetki ve sorumlulukları ile ilgili bir mevzuat çalışması yürütülmelidir.

Son olarak analitik model tabanlı bir uygulama başlığı altında AHP metodu kullanılarak çok ölçütlü karar verme problemi çözülmüştür. A, B, C, D ülkeleri (Güvenlik nedeniyle ülke isimleri verilmemiştir) için nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerinin sıralanmış ve en iyi siber güvenlik sistemine ait ülke seçilmiştir.

Çok ölçütlü karar verme sürecinde ilk olarak amaç belirlenmiş, sonrasında kriterler oluşturulmuştur. Kriterler belirlendikten sonra alanında uzman kişilerce ekte yer alan anket değerlendirilmiş ve belirlenen mevzuat geliştirme, saldırı öncesinde risk yönetimi, eğitim ve farkındalığın arttırılması, etkili bir savunma sistemi, acil müdahale ve siber olaya karşılık verme ile olay sonrası müdahale kriterleri arasında öncelik değerlendirmesi yapılmıştır. Sonrasında kriterlerin birbirlerine göre ikili karşılaştırma matrisi ve normalize matrisleri

oluşturulmuş en son tutarlılık analizi gerçekleştirilmiş ve karşılaştırmaların tutarlı olduğu ortaya konmuştur.

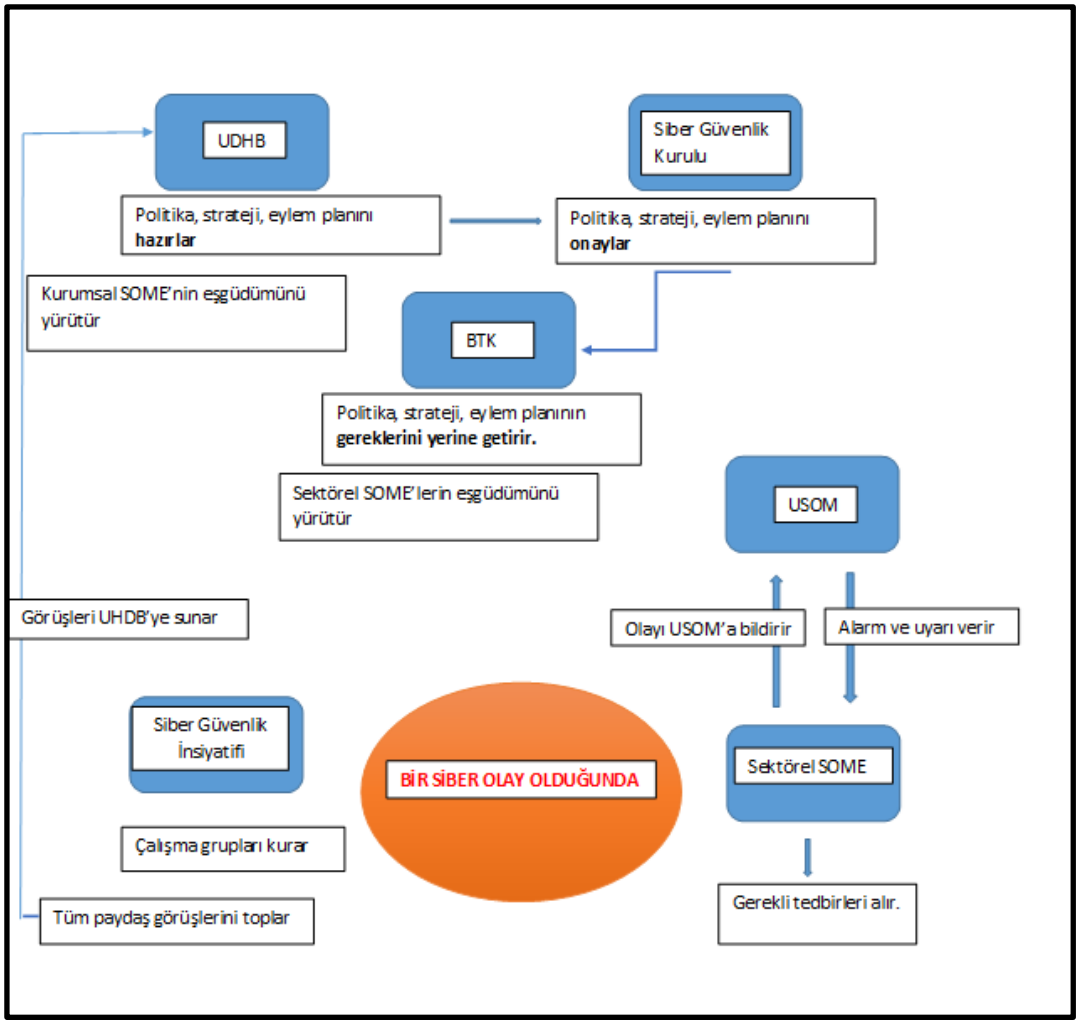
Sonrasında alternatifler belirlenmiş, A,B, C, D ülkelerinin seçilen altı kritere göre nitelikleri tablolar ile verilmiştir. Bu tablolardaki verilere göre karşılaştırmalar yapılmış ve alternatiflerin kriterlere göre değerlendirilmesi gerçekleştirilmiştir. Modelin sonunda çıkan sonuca göre siber güvenliğin en etkin olduğu ülke A ülkesidir. Bu durumda modelin sonucuna göre sıralama: A>B>C>D şeklindedir. Diğer bir deyişle karar noktalarının önem dizilimi A,B,C ve D şeklindedir.

Analitik Hiyerarşi Prosesi ile yapılan bu uygulama önümüzdeki süreçte yapılacak çalışmalarda kriterler arası bağımlılıklar göz önünde bulundurularak ANP metodu ile de gerçekleştirilebilir.

Bu tezde uygulanan modelde seçilen altı kriter arasından önem derecesi en fazla olan kriter mevzuat kriteridir bu sebeple tezde verilen öneri ve iyileştirmeler mevzuat odaklıdır. Türkiye'de bu siber güvenlik sisteminde rol oynayan pek çok devlet kurumu yer almaktadır. Bunların başlıcaları Ulaştırma Denizcilik ve Haberleşme Bakanlığı, Siber Güvenlik Kurulu, Bilgi Teknolojileri ve İletişim Kurumu, Ulusal Siber Olaylara Müdahale Ekibi, Kurumsal ve Sektörel SOME'ler ile diğer bakanlıklardır.

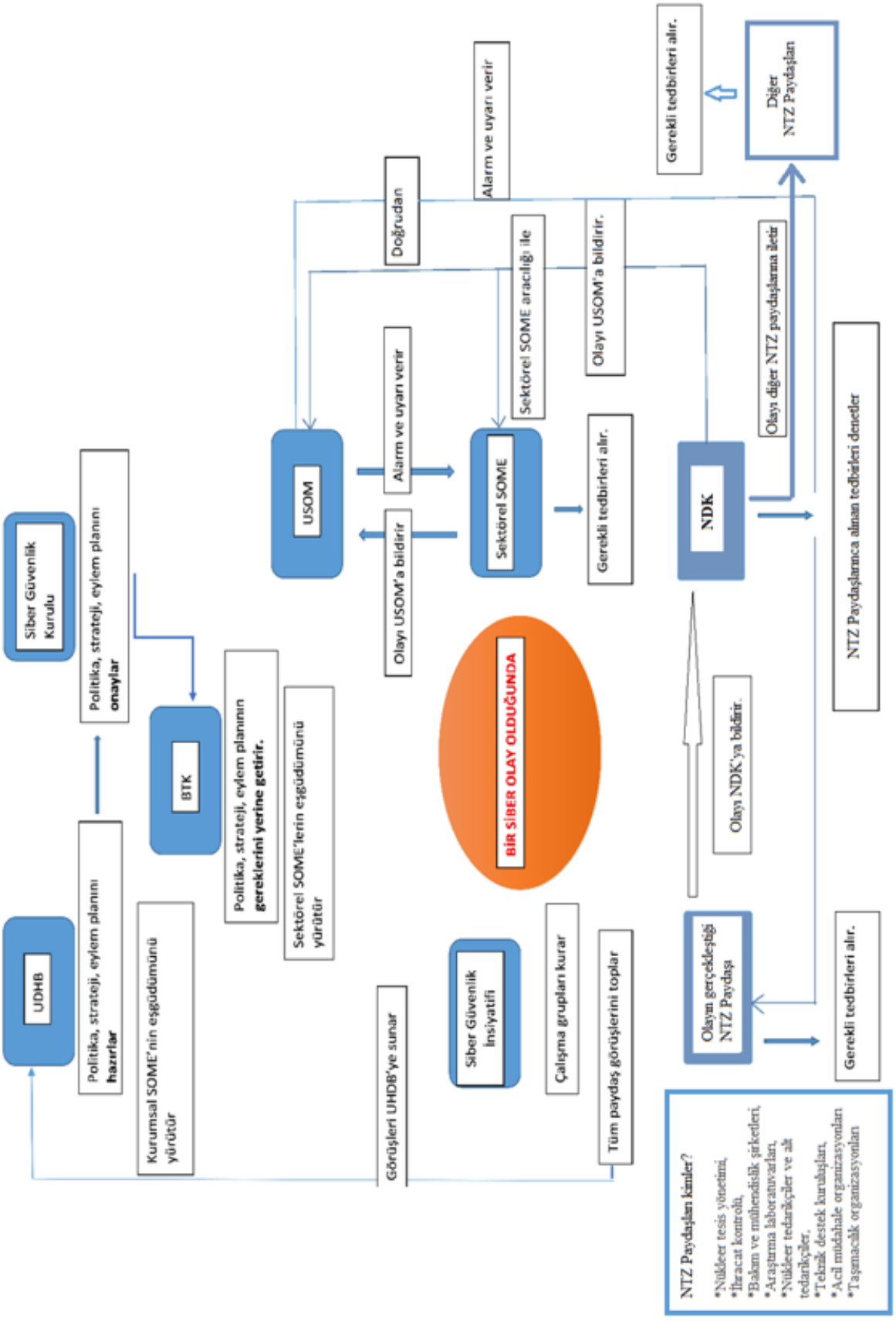
Genel hatlarıyla bakıldığında siber emniyetin sağlanmasında gerekli politika, strateji ve eylem planı UDHB tarafından hazırlanır, Siber Güvenlik Kurulu tarafından onaylanır. Ayrıca bu stratejilerin gereklilikleri BTK tarafından yerine getirilmektedir. Siber olayların müdahalesinde ulusal ve uluslararası koordinasyonun sağlanmasından ise USOM sorumludur. Bu kurum ve kuruluşlar dışında ulusal siber emniyet sisteminin bir öğesi de Siber Güvenlik İnisiyatifi'dir. Bu kurul, tüm paydaş görüşlerini değişik konularda toplar ve değerlendirmek üzere UDHB'ye sunar, çalışma grupları kurarak siber emniyetin sağlanmasına katkıda bulunur. Bu emniyet zincirinde görev alan diğer bir oluşum ise Kurumsal SOME'lerdir ve Sektörel SOME'lerden aldıkları bilgilerle ilgili faaliyetlere katılım göstermektedirler [14].

Siber güvenlik uygulamalarıyla ilgili Türkiye'deki mevcut durumun yalın haliyle şekilde verilmiştir:



Şekil 5.1. Siber güvenliğe ilişkin kurumların rolleri

Bu tezde, Merve Çetin tarafından hazırlanan "Nükleer Tesislerde Siber Emniyet, Siber Saldırı Senaryoları, Sonuçları Ve Savunma Sistemleri" isimli uzmanlık tezinden alınan yukarıdaki model yeniden geliştirilerek Nükleer Düzenleme Kurumu ve Nükleer Tedarik Zincirindeki paydaşların rolleri de dahil edilmiş ve aşağıdaki şekilde de gösterilen Kurumların rolleri yeniden tasarlanmıştır.



Şekil 5.2. Siber güvenliğe ilişkin kurumların ve NTZ paydaşlarının tasarlanan rolleri

Nükleer tedarik zincirine (NTZ) yönelik bir saldırı durumunda nasıl bir yol izleneceği ile ilgili tatbikat gerçekleştirilmeli ve NDK ve diğer NTZ paydaşlarının da katılımı sağlanmalıdır. Kritik altyapılara olası bir saldırı durumunda izlenecek rota ve adımlar ilgili kurumlarla toplantılar düzenlenerek ve görüşler değerlendirilerek belirlenmeli, çizilecek rotada NDK' nın ve diğer TZY paydaşlarının rolü ve sorumlulukları da belirlenmelidir. Siber güvenlikte önemli bir başlık olan risk değerlendirmesi USOM tarafından gerçekleştirilmektedir. Nükleer tedarik zincirine yönelik risk değerlendirmesi çalışmaları da yapılmalı, NDK ve diğer NTZ paydaşları da bu çalışmalarda yer almalıdır.

Nükleer tedarik zincirinin, ulusal düzenleyici kurum olan NDK tarafından belirlenen gereksinimlerle uyumlu olup olmadığı düzenli ve resmi denetimlerle kontrol edilmelidir. Koruyucu siber emniyet tedbirleri belirlenmeli ve uygulandığı denetlenmelidir. Bütünleşik bir tesisin yönetim sistemi ve siber emniyet oluşturulmalıdır. Sistem düzenli olarak gözden geçirmeli ve geliştirilmelidir

NTZ paydaşlarının ve düzenleyici kurumun yetki ve sorumluluklarının açıkça belirtildiği özel bir mevzuat hazırlanmalıdır. NTZ'deki her bir halka birbiriyle uyumlu ve NDK tarafından uygulandığı denetlenmiş bir bilgi güvenliği politikasına sahip olmalıdır. Bununla birlikte NTZ paydaşlarının her biri için siber emniyet çalışanları ve takımların rollerinin detaylıca belirtildiği bir siber emniyet programı hazırlamalıdır.

Düzenleyici kurum ve diğer paydaşlar ayrıca periyodik olarak tehdit değerlendirmesi yapmalıdır. Paydaşlar tehdit değerlendirmesi bulgu ve sonuçlarını birbirleriyle güvenli bir ortamda paylaşmalıdır. Yapılacak denetimlerde paydaşların yönetime düzenli olarak bilgi verip, devamlı bir tehdit değerlendirmesi yapıp yapmadığı sorgulanmalıdır.

Normal işletmenin sürekliliğini korumalı, sistemin geçici süreyle durdurulmasına veya tamamen kapatılmasına sebep olabilecek herhangi bir siber saldırı için öncelikle mevzuatı desteklemeli, iyi bir risk değerlendirmesi çalışması yapılmalı, tüm NTZ paydaşları ve çalışanlarına farkındalık eğitimleri verilmeli, etkili bir savunma mekanizması geliştirmelidir. Tüm bu sebeplerle olası siber saldırılara karşı yetkili makamlar tedbirler almalı iyi bir savunma sistemi geliştirmelidir. Acil müdahale ve siber olaylara karşılık vermenin nasıl olması gerektiği üzerinde durulmalı, kritik altyapıların siber emniyetinde alınabilecek önlemler dikkate alınmalıdır.

KAYNAKLAR

1. İnternet: Computer Security at Nuclear Facilities Nuclear Security Series No.17. *IAEA.* URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1527_web.pdf, Son Erişim Tarihi: 01.11.2019.

2. İnternet: Bıçakçı, S. Nükleer Tesislerin Siber Güvenliğine Giriş. *Türkiye'de Siber Güvenlik ve Nükleer Enerji.* URL: http://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b4.pdf, Son Erişim Tarihi: 04.10.2019.

3. İnternet: Cyber Security at Nuclear Facilities: National Approaches,The Nuclear Threat Initiative. *ISS&NTI.* URL: http://www.nti.org/media/pdfs/Cyber_Security_in_Nuclear_FINAL_UZNMggd.pdf?_=1466705014, Son Erişim Tarihi: 03.09.2019.

4. İnternet: Procurement Engineering and supply chain guidelines in support of operation and maintenance of nuclear facilities. *IAEA.* URL: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1725_web.pdf, Son Erişim Tarihi: 04.10.2019.

5. Kim, K.C. (2014). Issues of cyber supply chain security in Korea. *Technovation*, 7, 387-388.

6. Rongping, M. ve Yonggang, F. (2014). Security in the cyber supply chain: A Chinese perspective. *Technovation,* 7, 339-394.

7. İnternet: Finlands Cyber Security Strategy. *Ministry of Defence*. URL: https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, Son Erişim Tarihi: 08.07.2019.

8. İnternet: Communications Market Act. *Ministry of Transport and Communications*. URL: https://www.finlex.fi/en/laki/kaannokset/2003/en20030393.pdf, Son Erişim Tarihi: 08.07.2019.

9. Bengsghir, T. (2018). *Bilgi Güvenliği Yönetimi Dersi Ders Notları.* Gazi Üniversitesi

10. Sokolov, A., Mesropyan, V. and Chulok, A. (2014). Supply chain cybersecurity A Russian outlook. *Technovation,* 34, 389-391.

11. İnternet: Methods of Compromise. International Training Course on Information and Computer Security for Facilities That Handle Nuclear and Other Radioactive Material. *NUSEC.* URL: https://nusec.iaea.org/portal/User-Groups/Computer-Information-Security/NSNS-CSP-Overview, Son Erişim Tarihi: 12.07.2019.

12. İnternet: Conducting Computer Security Assessments at Nuclear Facilities. *IAEA.* URL: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf, Son Erişim Tarihi: 13.09.2019.

13. İnternet: Computer Security for Nuclear Security (NST 045/ Draft Implementing Guide). *IAEA.* URL: https://www-ns.iaea.org/downloads/security/security-series-drafts/implem-guides/nst045.pdf, Son Erişim Tarihi: 12.07.2019.

14. İnternet: Çetin, M. ve Alim, F. Nükleer Tesislerde Siber Emniyet, Siber Saldırı Senaryoları, Sonuçları ve Savunma Sistemleri. *TAEK.* URL: http://kurumsalarsiv.taek.gov.tr:8080/xmlui/handle/1/1024, Son Erişim Tarihi: 14.09.2019.

15. Sevinç, N. (2008). *Tedarik zinciri yönetim bilgi teknolojilerinin kullanılması ve önemi,* Yüksek Lisans Tezi, Trakya Üniversitesi Sosyal Bilimler Enstitüsü, Edirne, 1-14.

16. Yılmaz, E. (2017). *Kritik Altyapılar ve Güvenliği Dersi Ders notları*. Gazi Üniversitesi

17. İnternet: Safety Glossary. *IAEA.* URL: https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf, Son Erişim Tarihi: 28.12.2019.

18. İnternet: Nükleer Tesislerin ve Nükleer Maddelerin Fiziksel Korunması Yönetmeliği. *Resmi Gazete.* URL: https://www.resmigazete.gov.tr/eskiler/2012/05/20120522-7, Son Erişim Tarihi: 14.09.2019.

19. Akman, G., Alkan, A. (2006). Tedarik Zinciri Yönetiminde Bulanık Ahp Yöntemi Kullanılarak Tedarikçilerin Performansının Ölçülmesi: Otomotiv Yan Sanayiinde Bir Uygulama. *İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi,* 9, 24-25.

20. İnternet: Computer Security of Instrumentation and Control Systems at Nuclear Facilities. *IAEA.* URL: https://www.iaea.org/publications/11184/computer-security-of-instrumentation-and-control-systems-at-nuclear-facilities, Son Erişim Tarihi: 25.12.2019.

21. İnternet: NUSEC Chair Report. *IAEA.* URL: https://nusec.iaea.org/portal/User-Groups/Computer-Information-Security/NSNS-CSP-Overview, Son Erişim Tarihi: 13.07.2019.

22. İnternet: AREVA CM Computer security in the supply chain. *IAEA.* URL: https://nusec.iaea.org/portal/User-Groups/Computer-Information-Security/NSNS-CSP-Overview, Son Erişim Tarihi: 14.07.2019

23. Lee, J. (2018). Evaluating the Effectiveness of the Nuclear Suppliers Group: A Functionalist Perspective on the Regime. *The Korean Journal of International Studies,* 2, 193-195.

24. İnternet: The IAEA SafeGuards State Declerations Portal. *IAEA.* URL: https://www.iaea.org/sites/default/files/sg-sdp.pdf, Son Erişim Tarihi: 25.07.2019.

25. İnternet: The IAEA SafeGuards State Declerations Portal. *IAEA.* URL: https://www.iaea.org/resources/databases/safeguards-state-declarations-portal, Son Erişim Tarihi: 20.07.2019.

26. Türkiye Atom Enerjisi Kurumu. (2017). *Dünyadaki AR-GE Merkezlerinin Faaliyetlerinin İncelenmesi Çalışma Grubu Raporu.* Ankara

27. İnternet: Avrupa Nükleer Araştırma Merkezi (CERN). *TAEK*. URL: https://www.taek.gov.tr/tr/sesame/1037-avrupa-nukleer-arastirma-merkezi%20-cern.html, Son Erişim Tarihi: 23.08.2019.

28. Türkiye Atom Enerjisi Kurumu. (2017). *Ulusal Radyasyon Acil Durum Planı (URAP)*. Ankara

29. İnternet: Radyoaktif Kaynakların Emniyetine İlişkin Usul ve Esaslar. *TAEK*. URL: https://www.taek.gov.tr/tr/belgeler-formlar/rsgd-formlari/usul-esaslar/Radyoaktif-Kaynaklar%C4%B1n-Emniyetine-%C4%B0li%C5%9Fkin-Usul-ve-Esaslar/lang,tr-tr/, Son Erişim Tarihi: 18.09.2019.

30. Dağdeviren, M. ve Eren, T. (2001). Tedarikçi Firma Seçiminde Analitik Hiyerarşi Prosesi ve 0-1 Hedef Programlama Yöntemlerinin Kullanılması. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, 16(2), 41-52.

31. Sharma, Y. K., Yadav, A. K., Mangla, S. K. ve Patil, P. (2018). Ranking the Success Factors to Improve Safety and Security in Sustainable Food Supply Chain Management Using Fuzzy AHP. *Materialstoday*, 5, 12187-12196.

32. İnternet: Conducting Computer Security Assessments at Nuclear Facilities. *IAEA*. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL006web.pdf, Son Erişim Tarihi: 15.10.2019.

33. İnternet: Computer Security Incident Response Planning at Nuclear Facilities. *IAEA*. URL: https://www-pub.iaea.org/MTCD/Publications/PDF/TDL005web.pdf, Son Erişim Tarihi: 15.10.2019.

34. İnternet: Yaralıoğlu, K. Analitik Hiyerarşi Proses. URL: http://www.deu.edu.tr/userweb/k.yaralioglu/dosyalar/Analitik_Hiyerarsi_Proses.doc, Son Erişim Tarihi: 07.10.2019.

35. İnternet: Gökçen, H., Çetin, M. Nükleer Tedarik Zincirinde Siber Emniyet Farkındalığı. *V. International Congress on Natural and Health Sciences (ICNHS-2019*). URL: https://756d243f-9742-4892-987f-8834db07019e.filesusr.com/ugd/e42d97_14fc09f9162d40349f80f02fbe22103f.pdf, Son Erişim Tarihi: 20.01.2020.

EKLER

EK-1. Nükleer tedarik zincirinde siber güvenliğe ilişkin anket

Bu anket; Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalında yüksek lisans öğrencisi Merve ÇETİN tarafından hazırlanan yüksek lisans tezinde kuracağı analitik modelde girdi olarak kullanılacak ölçütlerin belirlenmesinde kullanılacak olup başka hiçbir yerde kullanılmayacaktır.

1. Mevzuat geliştirme (Nükleer alanda siber güvenlik sistemini geliştirmeye yönelik mevzuatın hazırlanması)
2. Saldırı öncesinde risk yönetimi
3. Eğitim ve farkındalığın arttırılması
4. Etkili bir savunma sistemi (Güvenlik duvarı, Antivirüs, Sayısal imza, İçerik filtreleme vb. savunma sistemi unsurları)
5. Acil müdahale ve siber olaya karşılık verme (Hasarın yayılmasını Önleme /Yok etme /İyileştirme) (Günümüzdeki siber saldırıların dinamik olması ve sürekli değişen tehditler sebebiyle söz konusu nükleer tesiste bütün önlemlerin alındığı, iyi tasarlanmış ve iyi yönetildiği düşünülen bir siber güvenlik planına sahip olunmasına rağmen yine de saldırıların olması ihtimali her zaman vardır. Böyle bir durumda olaya anında müdahale uygun şekilde saldırıya cevap verme ve tabi sonrasında sistemin iyileştirilmesi iyi bir güvenlik planı ve savunma sistemi kadar önemlidir)
6. Olay sonrası müdahale (Güvenlik kontrolü ve güvenlik programının etkinliğini belirleyin, Her olay için gelecekte kullanımı oldukça faydalı olabilecek bir izleme raporu oluşturun, Gelecek olayları önlemek adına olay bilgisi toplayın)

Yukarıda verilen Nükleer tedarik zinciri yönetiminde siber güvenliği geliştiren başarı faktörlerini önem sırasına göre sıralayınız (En önemli:1, En önemsiz: 6 olmak üzere).

1)…… 2)…… 3)…… 4)…… 5)……6)……

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı : ÇETİN, Merve

Uyruğu : T.C.

Doğum tarihi ve yeri : 26.11.1988, Ankara

Medeni hali : Evli

Telefon : 0 (554) 282 40 20

e-mail : mervekuba@gmail.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilgi Güvenliği Mühendisliği	Devam ediyor
Lisans	Gazi Üniversitesi / Endüstri Mühendisliği	2012
Lise	Alparslan Süper Lisesi	2006

İş Deneyimi

Yıl	Yer	Görev
2014-Halen	Türkiye Atom Enerjisi Kurumu	Uzman

Yabancı Dil

İngilizce

Yayınlar

1. Gökçen, H., Çetin, M. (2019). *Nükleer Tedarik Zincirinde Siber Emniyet Farkındalığı*. V. International Congress on Natural and Health Sciences (ICNHS-2019) Kongresinde sunulmuş bildiri, INSAC, Adana.

Hobiler

Kitap Okumak, Ney üflemek

GAZİ GELECEKTİR...