T.C.

TARIM VE ORMAN BAKANLIĞI

SU YÖNETİMİ GENEL MÜDÜRLÜĞÜ

GAZİANTEP İLİ KAYNAKTAN MUSLUĞA İÇME VE KULLANMA SUYU GÜVENLİĞİ PLANININ HAZIRLANMASI PROJESİ

KBRN ve SİBER SALDIRILAR ACİL DURUM EYLEM PLANI

SUİŞ PROJE
MÜHENDİSLİK ve MÜSAVİRLİK LTD. ŞTİ.
ENGINEERING & CONSULTING CO. LTD.

ANKARA / HAZİRAN 2023

T. C. TARIM VE ORMAN BAKANLIĞI

SU YÖNETİMİ GENEL MÜDÜRLÜĞÜ

GAZİANTEP İLİ KAYNAKTAN MUSLUĞA İÇME ve KULLANMA SUYU GÜVENLİĞİ PLANININ HAZIRLANMASI PROJESİ

KBRN ve SİBER SALDIRILAR ACİL DURUM EYLEM PLANI

ANKARA / HAZİRAN 2023

SUİŞ PROJE
MÜHENDİSLİK ve MÜSAVİRLİK LTD. ŞTİ.
ENGINEERING & CONSULTING LTD. CO.

T.C. TARIM VE ORMAN BAKANLIĞI
SU YÖNETİMİ GENEL MÜDÜRLÜĞÜ
SU HUKUKU VE POLİTİKASI DAİRE BAŞKANLIĞI

SU YÖNETİMİ GENEL MÜDÜRLÜĞÜ

GENEL MÜDÜR

Afire SEVER

GENEL MÜDÜR YARDIMCISI

Dr. Yakup KARAASLAN

SU HUKUKU VE POLİTİKASI DAİRE BAŞKANLIĞI

Daire Başkanı

Zakir Turan

SU POLİTİKASI ŞUBE MÜDÜRLÜĞÜ

Huriye İNCECİK CEYLAN	Şube Müdürü
Mehmet AKKOYUN	Mühendis
Fatih TÜRKMENDAĞ	Mühendis
Demet Işık KURTOĞLU	Mühendis
Dr. M. Şevki ALTINGÖZ	Mühendis
Dr. M. Yasir AK	Mühendis

T.C. TARIM VE ORMAN BAKANLIĞI
SU YÖNETİMİ GENEL MÜDÜRLÜĞÜ
SU HUKUKU VE POLİTİKASI DAİRE BAŞKANLIĞI

PROJE EKİBİ

Selime Seda ÇETİNKAYA	Çevre Mühendisi
Hasan KIRMIZITAŞ	Jeoloji Mühendisi
Utku Berkalp ÜNALAN	Çevre Mühendisi
Erol DEMİRCİ	Çevre Mühendisi
Hasan ÇEVİK	Kimya Mühendisi
Dr. Okan Çağrı BOZKURT	Y. İnşaat Mühendisi
Oya ORBAY	Biyolog

DANIŞMANLAR

Prof. Dr. Mehmet ÇAKMAKÇI

Prof. Dr. Mahmut FIRAT

Dr. Meltem KAÇIKOÇ

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

KISALTMALAR

AFAD	Afet ve Acil Durum Yönetimi Başkanlığı
BTK	Bilgi Teknolojileri Kurumu
ÇŞİDB	Çevre, Şehircilik ve İklim Değişikliği Bakanlığı
DSİ	Devlet Su İşleri
GASKİ	Gaziantep Su ve Kanalizasyon İdaresi Genel Müdürlüğü
İAT	İçme Suyu Arıtma Tesisi
İTASHY	İnsani Tüketim Amaçlı Sular Hakkında Yönetmelik
KASKİ	Kahramanmaraş Su ve Kanalizasyon İdaresi Genel Müdürlüğü
TAMP	Türkiye Acil Müdahale Planı
TOB	Tarım ve Orman Bakanlığı
USOM	Ulusal Siber Olaylara Müdahale Merkezi
YAS	Yeraltı Suyu
YÜS	Yerüstü Suyu

1 KBRN ACİL DURUM EYLEM PLANI

Tarım ve Orman Bakanlığı 2021 yılında yurt içinde veya dışında meydana gelip ülkemizi etkileyebilecek olan kimyasal, biyolojik, radyolojik ve nükleer tehdit ve tehlikelere karşı insan sağlığı ve çevreye yönelik zararın önlenmesi veya en aza indirilmesi için gerekli tedbirlerin alınması amacıyla, Bakanlık merkez ve taşra teşkilatı ile bağlı ve ilgili kurum ve kuruluşlarının görev ve sorumluluklarını belirlemek, Bakanlık tarafından yapılacak müdahale ve faaliyetlerin etkin bir şekilde yerine getirilmesini sağlamak amacı ile Kimyasal, Biyolojik, Radyolojik Ve Nükleer Tehdit Ve Tehlikelere Dair Görev Yönergesi'ni yayımlamıştır.

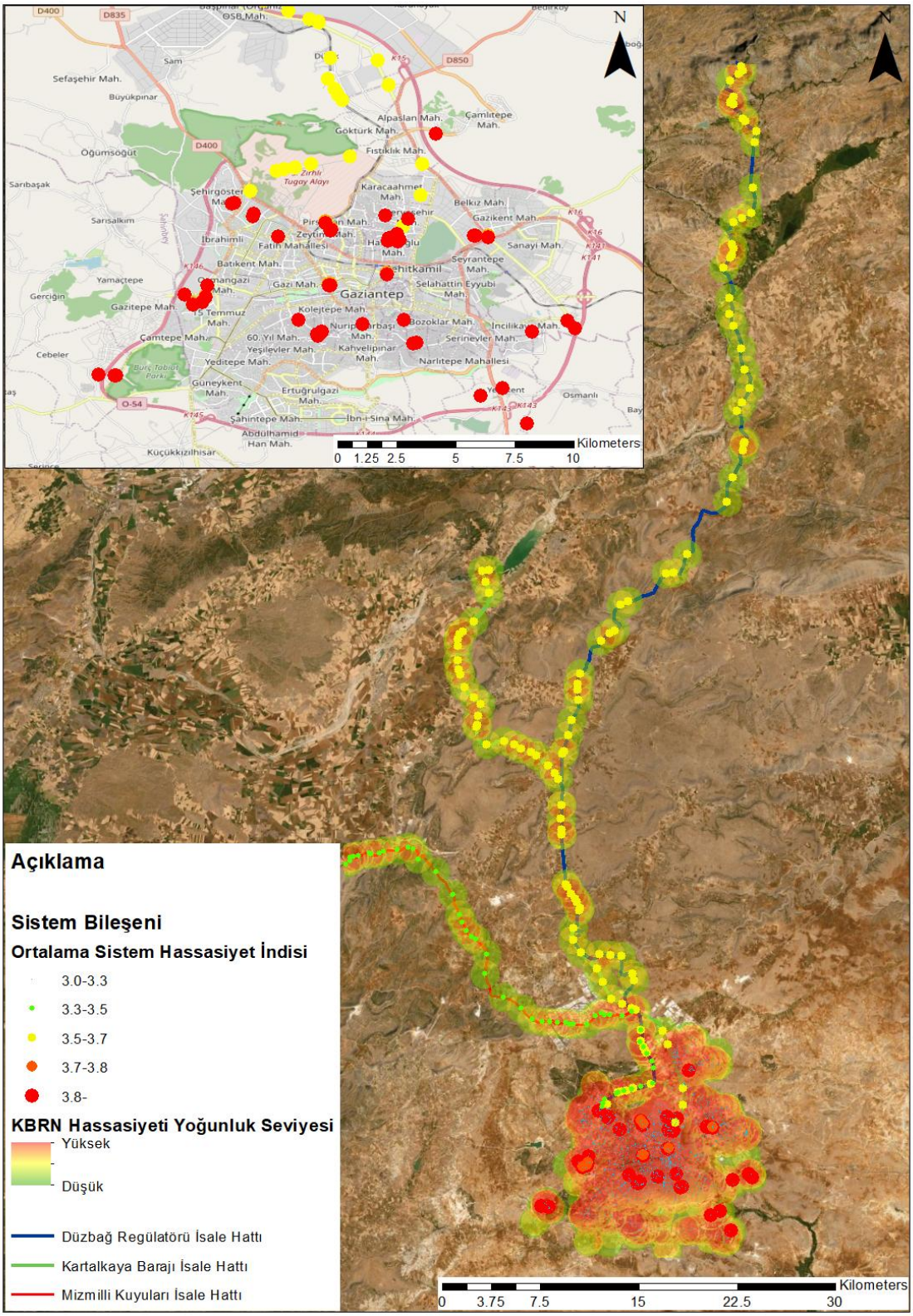
Gaziantep İli İçme ve Kullanma Suyu Güvenliği Planlanması Projesi Kapsamında hazırlanmış olan KBRN/Fiziksel Saldırılara Yönelik Acil Durum Eylem Planı AFAD Başkanlığı-Türkiye Acil Durum Eylem Planı ve TOB- Kimyasal, Biyolojik, Radyolojik ve Nükleer Tehdit ve Tehlikelere Dair Görev Yönergesi ile uyumlu olarak "Kaynaktan Musluğa Su Güvenliğini" sağlamak amacı ile hazırlanmıştır.

İçme-Kullanma suyu sistemlerini hedef alan KBRN saldırıları halk sağlığı üzerinde yoğun etki gösterme riski taşımaktadır. İçme kullanma suyu sistemlerinin KBRN saldırı ve tehditlerine karşı hassasiyet analizi "Nihai Rapor - Bölüm 8 İçme Kullanma Suyu Sisteminin Kimyasal-Biyolojik-Radyolojik-Nükleer (KBRN) Saldırılara Karşı Hassasiyetinin Değerlendirilmesi" başlığı ile sunulmuştur. İçme-kullanma suyu sistemindeki ajan bazlı (K-B-R-N) saldırılara karşı sistemin hassasiyet analizleri detaylı olarak bu bölümde yer almaktadır. İçme-Kullanma suyu sistemlerinin her bir sistem bileşeninin KBRN ajan tiplerine; Arıtıma Dayanıklılık, Potansiyel Etkilenecek Kişi Sayısı, Tehlike, Ajana Erişilebilirlik ve Tespit Edilebilirlik özelliklerine göre değerlendirilmiştir.

Her bir sistem bileşeni için temin edilen veriler ile yapılan mevcut durum değerlendirmeleri ve İçme-Kullanma Suyu sistemi CBS ortamında algoritmik olarak işlenmiştir. Proje kapsamında geliştirilen KRBN saldırıları ve tehditlerine karşı hassasiyetin belirlenmesi metodolojisi sistematiği uygulanarak Gaziantep İçme ve

Kullanma Suyu Sisteminin KBRN tehdit ve saldırılarına karşı hassasiyeti belirlenmiştir. Her bir sistem bileşeni için tüm ajanlara göre değerlendirme yapılmıştır.

Bu çalışma sonucunda elde edilen, Gaziantep İli İçme Kullanma Suyu Sistemi KBRN saldırılarına karşı hassasiyet haritası Şekil 1.1 ile sunulmaktadır.



Şekil 1.1 Gaziantep İli İçme Kullanma Suyu Sistemi KBRN Saldırılarına Karşı Hassasiyetleri Haritası

KBRN saldırılarına karşı ortalama sistem hassasiyeti değerlendirildiğinde, KBRN saldırı ve hassasiyetine karşı en hassas noktalar yapılan 3.84 ortalama hassasiyet indisi puanı ile ***Arıtma Tesisi*** ve ***Temiz Su Depoları*** olmuştur. Bu sistemleri 3.75 ortalama hassasiyet indisi değeri ile ***Şehir İçi Kuyuları*** takip etmektedir. ***Düzbağ Regülatörü*** ve ***Kartalkaya Baraj Gölü Havzası*** 3.5 ortalama hassasiyet indisine sahip olup ***Mizmilli Kuyuları*** 3.4 ile sistemdeki en düşük ortalama hassasiyet skoruna sahip sistem bileşeni olarak değerlendirilmiştir.

KBRN, siber ve fiziksel saldırılar, proses kazaları ya da rutin kirlilik olaylarından farklı ele alınması gereken durumlardır. KBRN ve siber saldırılar TAMP kapsamında afet olarak değerlendirilmekte olup, AFAD koordinasyonunda müdahale edilmesi gerekmektedir. TAMP kapsamında KBRN ve siber saldırılardan sorumlu çalışma grupları Tablo 1.1 ile sunulmaktadır.

Tablo 1.1 KBRN ve Siber Saldırılara İlişkin TAMP Sorumlu Çalışma Grupları

Afet Türü	Çalışma Grupları
Siber Saldırı	• Teknik Destek ve İkmal • Güvenlik ve Trafik • Haberleşme • Enerji • Zarar Tespit • İletişim • Bilgi Yönetimi • Değerlendirme ve İzleme
Kimyasal	• Haberleşme • Nakliye • Ulaşım Alt Yapı • Güvenlik ve Trafik • Arama ve Kurtarma • Sağlık • Tahliye ve Yerleştirme • Planlama • Alt Yapı • Enerji • Barınma • Hasar Tespit • Yangın • Enkaz Kaldırma • Tarım Orman Gıda Su ve Hayvancılık • Zarar Tespit • Beslenme • Psikososyal Destek • İletişim Bilgi Yönetimi • Değerlendirme ve İzleme

Afet Türü	Çalışma Grupları
BİYOLOJİK AFETLER VE SALGIN HASTALIKLAR	• Haberleşme • Nakliye • Ulaşım Alt Yapı • Güvenlik ve Trafik • Arama ve Kurtarma • Sağlık • Tahliye ve Yerleştirme • Planlama • Alt Yapı • Enerji • Barınma • Hasar Tespit • Yangın • Enkaz Kaldırma • Tarım Orman Gıda Su ve Hayvancılık • Zarar Tespit • Beslenme • Psikososyal Destek • İletişim • Bilgi Yönetimi • Değerlendirme ve İzleme
RADYOLOJİK NÜKLEER KAZALAR	• Haberleşme • Güvenlik ve Trafik • Arama ve Kurtarma • Nakliye • Ulaşım Alt Yapı, Sağlık • Tahliye ve Yerleştirme • Planlama • Enerji • Barınma • Beslenme • Yangın • Tarım Orman Gıda Su ve Hayvancılık • Zarar Tespit • Beslenme • Psikososyal Destek • İletişim • Bilgi Yönetimi • Değerlendirme ve İzleme

1.1 Planlama ve Hazırlık (Olay Öncesi)

“Kaynaktan Musluğa İçme Kullanma Suyu Sistemine” KBRN saldırısı gerçekleşmesi durumunda saldırıya yönelik zarar azaltıcı/iyileştirici eylemlerin gerçekleştirilmesi ancak saldırının ve niteliğinin tespit edilebilmesi ile mümkündür.

KBRN saldırıları anlık ve münferit olaylar olma nitelikleri dolayısıyla düzenli takibinin yapılması ve saldırı tipinin tespiti kolay durumlar değillerdir. Dolayısıyla, KBRN saldırılarına dair alınması gereken temel önlemler; içme kullanma suyu sistem bileşenlerine erişilebilirliklerin kısıtlanması ve bu bileşenlerin düzenli olarak izlenmesidir.

Olay öncesinde planlama ve hazırlık aşamasının en önemli adımlarından biri Afet sonrası içme-kullanma suyu güvenliğinin sağlanması için mevcut içme suyu ve kanalizasyon şebekelerinin güncel durumunun GASKİ tarafından tüm hizmet alanlarını kapsayacak şekilde haritalandırılarak sayısal ortama aktarılması ve güncelliğinin sağlanmasıdır. Böylelikle herhangi bir olağanüstü durumda diğer illerden gelen uzman personelin bu sayısallaştırılmış verilere erişimi sağlanmış olacaktır. Afet öncesi, AFAD ve Çevre, Şehircilik ve İklim Değişikliği Bakanlığı bünyesinde verilerin yedeklerinin bulundurulması ve afet sonrası muhtemel görevli tüm personelin (Bakanlık birimleri, Kardeş Belediyeler, 1.-2. Grup destek belediyeler vb.) bu verilere erişimi sağlanmalıdır.

Buna ek olarak içme ve kullanma suyu sisteminin sürdürülebilir şekilde halka su sağlaması için oluşturulan acil durum eylem planlarının etkin bir şekilde uygulanabilmesi amacıyla AFAD koordinasyonunda GASKİ ile tatbikatlar yapması önerilmektedir. Gaziantep ili İçme Suyu sistem bileşenleri için deprem tehlikesine yönelik gerçekleşebilecek riskler ve alınması gereken tedbirler tüm sistem bileşenleri için belirlenmiştir. Bu çalışma kapsamında Dünya Sağlık Örgütü dokümanları, Çevre Koruma Kurumu rehber dokümanı, Su Yönetimi Genel Müdürlüğü rehber dokümanı, Kırsal Toplum Yardım Kurumu acil durum eylem planı, kapsamlı literatür çalışmaları, geçmiş olaylar incelenerek uzman görüşü ile yorumlanarak içme suyu sistemi için riskler ve tedbirler belirlenmiştir. Bu çalışma kapsamında dikkate alınan referanslar aşağıda liste olarak verilmektedir

Organizasyon/Kurum/Kuruluş Adı	Doküman Adı	Kaynakça
ASCE	Can Real-Time Modeling Be Useful for Emergency Planning and Response?	(Walski, 2015)
Bağımsız	Innovative Tools for the Detection and Mitigation of CBRN Related Contamination Events of Drinking Water	(Bernard, ve diğerleri, 2015)
Bağımsız	Preparedness Plan for the Water Supply Infrastructure during Water Terrorism—A Case Study from Irbid, Jordan	(Hindiyeh, ve diğerleri, 2021)
Delft Institute for Water Education	Water Safety Plans	(Setty & Ferrero, 2021)
District Of Summerland	Water Utility Emergency Response Plan	(Summerland, 2022)
EPA	Incident Action Checklist – Power Outages	(EPA, 2021)
EPA	Incident Action Checklist – Cybersecurity	(EPA, 2021)
German Armed Forces Institute for Protection Technologies	Detection of chemical threat agents in drinking water by an early warning real-time biomonitor	(Green, Kremer, & Moldaenke, 2003)
Government of Alberta	Drinking water safety plan training course	(Government of Alberta, 2013)
Government of Alberta	Guidance Notes for Drinking Water Safety Plan Template	(Government of Alberta, 2009)
Government of Alberta	Drinking water safety plans : proactive risk management for water supply systems	(Government of Alberta, 2013)
India Defence Research and Development	Chemical warfare agents	(Ganesan, Raza, & Vijayaraghavan, 2010)
India Journal of Pharmacy and Bioallied Sciences	Ensuring safe water in post-chemical, biological, radiological and nuclear emergencies	(Amar, 2010)
International Committee of the Red Cross	CBRN Response, introductory guidance	(ICRC, 2014)
Loughborough University	An introduction to water safety plans	(Smith & Reed, 2014)
National School of Public Health, Department of Sanitary Engineering and Environmental Health, Athens, Greece	Application of HACCP Principles in Drinking Water Treatment	(Damikouka, Katsiri, & Tzia, 2005)
SYGM	İçme Suyu Güvenliği Planlarına İlişkin Dünyadaki Uygulamalar ve Türkiye	(SYGM, 2015)
U.S. Army Center for Health Promotion and Preventive Medicine	Biological Warfare Agents as Threats to Potable Water	(Burrows & Renner, 1999)
U.S. Department of Energy Office of Nuclear Energy	Protecting Drinking Water Utilities From Cyber Threats	(Clark, Panguluri, Nelson, & Wyman, 2017)
University of Wisconsin	A Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005	(Mohtadi & Murshid, 2006)
US Armed Forces	Operations in Chemical, Biological, Radiological, and Nuclear Environments	(JCS, 2020)

Organizasyon/Kurum/Kuruluş Adı	Doküman Adı	Kaynakça
WHO	Water safety plans	(WHO, 2006)
WHO	Water Safety Plan Manual	(WHO, 2006)
WHO	Water safety plans : managing drinking-water quality from catchment to consumer	(WHO, 2005)
WHO	Water safety plan manual: step-by-step risk management for drinking-water suppliers	(WHO, 2006)
WHO	Public health response to biological and chemical weapons : WHO guidance	(WHO, 2004)
WHO	Water safety plan quality assurance tool	(WHO, 2013)
WHO	A practical guide to auditing water safety plans	(WHO, 2015)
NATO	Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security	(NATO, 2018)
NATO	Threats to Food and Water Chain Infrastructure	(NATO, 2010)
Bağımsız	Pick Your POICN: Introducing the Profiles of Incidents involving CBRN and Non-State Actors (POICN) Database	(Binder & Ackerman, 2019)
Bağımsız	21st Century Prometheus, Managing CBRN Safety and Security Affected by Cutting-Edge Technologies	(Martellini & Trapp, 2020)
The Royal Society of Chemistry	Water Contamination Emergencies: Managing the Threats	(RSC, 2013)

Gaziantep İli için KBRN ve siber saldırılara karşı alınacak önlemler her bir sistem bazında sisteme erişilebilirliğin kısıtlanması ve sistem bileşenlerinin düzenli izlenmesi üzerinde değerlendirilmiştir. İçme suyu sistemine erişilebilirliğin kısıtlanması fiziksel erişim durumu ve siber saldırılar olmak üzere iki ana alt başlıkta incelenmiştir.

Gaziantep İçme Suyu Sistemi su kaynakları, içme suyu arıtma tesisi, isale ve şebeke olmak tüm sistem bileşenlerine fiziki erişim durumu için mevcuttaki uygulamalar ve alınması gereken önlemler

Tablo 1.2 ile verilmektedir.

Tablo 1.2 Fiziki Erişim Durumuna İlişkin Alınması Gereken Temel Tedbirler

Sistem Bileşeni	Mevcut Durum	Tedbir Kodu	Tedbirler	Tedbir Sorumlusu	İlgili Kurum ve Kuruluşlar
Düzbağ Regülatörü	Güvenlik ve kameralar ile korunmaktadır.	0003-KYN-02-T157_63	Göksu Deresi kenarındaki yolun yaya geçidine kapatılması için gerekli başvuruların/izinlerin alınması	GASKİ	-
		0003-KYN-02-T157_64	Gerçek zamanlı online ölçüm sistemi kurulması ve ÇO, pH, bulanıklık, redoks potansiyeli ve iletkenlik parametrelerinin sürekli ölçülmesi	GASKİ	-
Kartalkaya Barajı	DSİ standartlarına göre korunmakta olup baraj gölü her türlü tehdide açık, ulaşımı kolay ve herkesin erişebileceği şekildedir.	0003-KYN-01-T157_65	Baraj gölü ve çevresine erişimi daha da zorlaştırmak için ilave güvenlik bariyerlerinin kurulması	DSİ Genel Müdürlüğü	GASKİ
		0003-KYN-01-T157_64	Gerçek zamanlı online ölçüm sistemi kurulması ve ÇO, pH, bulanıklık, redoks potansiyeli ve iletkenlik parametrelerinin sürekli ölçülmesi	GASKİ	DSİ Genel Müdürlüğü
		0003-KYN-01-T157_66	Baraj yakın civarında insan erişimi olabilecek alanlarda kamera sistemleri ile de sürekli izleme yapılması	GASKİ	DSİ Genel Müdürlüğü
Mizmilli Kuyuları	Her bir kuyu etrafında betonarme yapı içerisinde olup SCADA ve pompaların olduğu bina güvenlik ile korunmaktadır.	0003-KYN-03-T157_64	Gerçek zamanlı online ölçüm sistemi kurulması ve ÇO, pH, bulanıklık, redoks potansiyeli ve iletkenlik parametrelerinin sürekli ölçülmesi	GASKİ	-
Şehir İçi Kuyuları	Şehir içi kuyuları şehir merkezinde olup betonarme yapı içerisinde ve sadece GASKİ görevlilerinin erişebileceği şekildedir.	0003-KYN-04-T157_67	Kuyulara sadece yetkili personel tarafından erişilebilmesini sağlamak amacıyla biyometrik erişim kontrol sistemlerinin kurulması	GASKİ	-
		0003-KYN-04-T157_64	Gerçek zamanlı online ölçüm sistemi kurulması ve ÇO, pH, bulanıklık, redoks potansiyeli ve iletkenlik parametrelerinin sürekli ölçülmesi	GASKİ	-
Hacıbaba İAT	Yüksek duvarlar ve güvenlik ile korunmaktadır.	0003-IAT-01-T157_68	İAT ve yakın civarında insan erişimi olabilecek alanlarda kamera sistemleri ile de sürekli izleme yapılması	GASKİ	-
Depolar	Su depoları da yüksek duvarlarla erişime engellenmekte ve güvenlik kameralarıyla izlenmektedir.	0003-SBK-01-T157_64	Gerçek zamanlı online ölçüm sistemi kurulması ve ÇO, pH, bulanıklık, redoks potansiyeli ve iletkenlik parametrelerinin sürekli ölçülmesi	GASKİ	-
		0003-SBK-01-T157_69	Depoların uzaktan yönetiminin sağlanması için aktüatörlü kelebek vana uygulanması	GASKİ	-
İsale Hattı	-	0003-ISL-01-T157_70	Terfi merkezi, su deposu, vana odası ve diğer sanat yapıları için kamera sistemi ile kurulması	GASKİ	-
Tüm Sistem Bileşenleri	-	0003-GNL-01-T157_71	SCADA sistemi ile tüm sistem bileşenleri arasındaki entegrasyonun ve uzaktan erişimin sağlanması için fizibilite çalışmasının yapılması	GASKİ	-

Siber saldırılar, siber güvenlik önlemleri alınmamış veya yetersiz korunmuş uzaktan erişimin mümkün olduğu sistemlere karşı gerçekleştirilebilir ve sistemin verilerine, bilgisayar ağlarına veya diğer dijital kaynaklarına zarar vermek veya izinsiz erişim sağlamak amacıyla yapılmaktadır. İçme suyu temin sistemine yönelik siber saldırılar, içme suyu teminin güvenliğini tehdit ederek su kalitesini ve teminini etkileyebilir. Bu nedenle, içme suyu temin sistemlerini siber saldırılara karşı korumak için güçlü siber güvenlik önlemleri almak ve sürekli olarak izlemek son derece önemlidir.

Gaziantep İli içme-kullanma suyu sisteminin olası siber saldırılara karşı korunması için sistemin öncelikli olarak mevcut durumu değerlendirilmiştir. Buna bağlı olarak siber saldırılara karşı sistemi koruyan mevcut önlemlere ilave edilebilecekler ve bu önlemlerin hayata geçirilmesi için sorumlu kurum ve kuruluşlar Tablo 1.3 ile verilmektedir.

Tablo 1.3 Siber Saldırılara Yönelik Sistem Bileşenlerinde Alınabilecek Önlemler

Sistem Bileşenleri	Muhtemel Siber Saldırı Senaryoları	Tedbir Kodu	Tedbirler	Tedbir Sorumlusu	İlgili Kurum ve Kuruluşlar
Düzbağ Regülatörü	SCADA sistemine yetkisiz erişim, veri değiştirme veya hizmet aksatma saldırıları	0003-KYN-02-T158_72	Anormal ağ trafiği ve saldırı kalıplarını tespit etmek için IDS/IPS sistemleri kullanılması	GASKİ	-
		0003-KYN-02-T158_73	Yetkisiz girişleri ve tehlikeli trafikleri bloklamak için kuruluşa özgü güvenlik politikaları ile yapılandırılan bir Firewall sistemi kullanılması	GASKİ	-
Kartalkaya Baraj Gölü	Uzaktan kontrol sistemlerine yetkisiz erişim, su seviyesi verilerinin manipülasyonu	0003-KYN-01-T158_74	Kullanıcı adı ve parola dışında bir adım daha eklenerek iki faktörlü kimlik doğrulama kullanılması (örneğin, bir SMS doğrulama kodu)	GASKİ	-
		0003-KYN-01-T158_75	Veri manipülasyonunu önlemek için kritik sistemlerin fiziksel ve ağ düzeyinde izolasyonunun sağlanması.	GASKİ	-
Mizmilli Kuyuları	Pompa performans verilerinin manipülasyonu ve hizmet aksatma saldırıları	0003-KYN-03-T158_76	Zayıf noktaları ve güvenlik açıklarını belirlemek için düzenli ağ ve sistem taramaları yapılması	GASKİ	-
		0003-KYN-03-T158_72	Anormal ağ trafiği ve saldırı kalıplarını tespit etmek için IDS/IPS sistemleri kullanılması	GASKİ	-
Şehir İçi Kuyuları	Kuyu performans verilerinin manipülasyonu ve hizmet aksatma saldırıları	0003-KYN-04-T158_77	İki faktörlü kimlik doğrulama kullanılması	GASKİ	-
		0003-KYN-04-T158_78	Tüm ağ cihazları ve yazılımları için güvenlik güncellemeleri ve yamaları düzenli olarak uygulanması	GASKİ	-
Şehir İçi Su Depoları	Su depoları bilgi sistemlerine yetkisiz erişim ve veri manipülasyonu	0003-SBK-01-T158_79	Anormal ağ trafiği ve saldırı kalıplarını tespit etmek için IDS/IPS sistemleri kullanılması	GASKİ	-
		0003-SBK-01-T158_78	Tüm ağ cihazları ve yazılımları için güvenlik güncellemeleri ve yamaları düzenli olarak uygulanması	GASKİ	-
Su Arıtma Tesisleri	SCADA sistemlerine yetkisiz erişim, işlem kontrollerinin manipülasyonu	0003-IAT-01-T158_80	Fiziksel ve ağ düzeyinde izolasyon ile SCADA sistemlerinin genel ağdan ve potansiyel saldırılardan korunması	GASKİ	-
		0003-IAT-01-T158_81	Belirli IP adresleri veya ağ segmentleri için giriş ve çıkış kuralları tanımlayan ACL'leri kullanılması	GASKİ	-
SCADA Sistemleri	Sistem bilgilerinin manipülasyonu, yetkisiz erişim ve kontrol	0003-GNL-01-T158_82	SCADA ağının genel ağdan ayrı tutulması, özel bir VPN üzerinden güvenli bir bağlantı kullanılması	GASKİ	-
		0003-GNL-01-T158_83	İki faktörlü kimlik doğrulama ve role dayalı erişim kontrolünün kullanılması	GASKİ	-
Arıtma Tesisi		0003-IAT-01-T158_84	Kimyasal madde dozaj verilerinin doğru olup olmadığını sürekli olarak kontrol etmek için otomatik sistemler kullanılması	GASKİ	-
Arıtma Tesisi	Kimyasal dozaj verilerinin manipülasyonu, hatalı dozajın kontrol sistemine gönderilmesi	0003-IAT-01-T158_73	Yetkisiz girişleri ve tehlikeli trafikleri bloklamak için kuruluşa özgü güvenlik politikaları ile yapılandırılan bir Firewall sistemini kullanılması	GASKİ	-

KBRN saldırılarına karşı alınabilecek önlemlerin en başında içme suyu sistem bileşenlerinde yapılması gereken sürekli çevrim içi izlemelerdir. İçme suyu sistemlerinde anlık çevrimiçi olarak izlenmesi gereken başlıca anahtar konvansiyonel parametreler bulanıklık, toplam organik karbon, sıcaklık, klor (arıtma tesisi ve şebekede), basınç (isale ve şebekede), pH ve sıcaklıktır.

Gaziantep İli İçme Suyu Sistemi için çevrimiçi izlenmesi gereken parametrelerin mevcut durumdaki izlendiği bileşenler ve sıklıkları, olası KBRN saldırılarına karşı ilk uyarıyı vermesi için alınabilecek önlemler kapsamında izlenmesi gereken sistem bileşenleri ve izleme yöntemleri Tablo 1.4 ile sunulmaktadır.

Tablo 1.4 İzleme Parametreleri

Parametre	Mevcut Durum İzlemeleri		Alınması Gereken Önlem İzlemeleri		İlgili Olaylar	Tehlikeler	Sistem Bileşenlerinde İzlenmesi Önerilen Parametreler						
	Örneklem Yolu	İzleme Periyodu	Örneklem Yolu	İzleme Periyodu			Baraj	Regülatör	Arıtma Tesisi	Mizmilli Kuyuları	Şehir içi Kuyuları	İsale Hattı	Şebeke
Bulanıklık	Regülatör Arıtma Giriş	Günlük Sürekli	Çevrimiçi	Sürekli	Kimyasal veya Biyolojik saldırı	Yüksek bulanıklık seviyeleri, su kalitesini, suyun görünümünü ve tat/koku profilini etkileyebilir ve filtrasyon gibi arıtma ünitelerinin işletimini zorlaştırabilir ve bakteriyel kontaminasyon riskini artırabilir.	×	×	×	×	×		×
Toplam Organik Karbon (TOC)	-		Çevrimiçi	Her saat	Kimyasal saldırı	Yüksek TOC seviyeleri, su kaynaklarının organik kirlilik yükünü artırır ve dezenfektanlarla reaksiyona girerek zararlı yan ürünler oluşturarak insanlarda sağlık sorunlarına yol açabilir.	×	×	×	×			
Klor	Arıtma Giriş Şehir İçi kuyuları	Sürekli	Çevrimiçi	Sürekli	Kimyasal saldırı	Aşırı klor, suyun tat ve koku profilini olumsuz etkileyebilir ve sağlık sorunlarına neden olabilir; düşük klor, suyun mikrobiyolojik güvenliğini tehlikeye atabilir.			×	×	×		×
Kimyasal Konsantrasyon (örn. asit, baz, koagülant vb.)	-	-	Çevrimiçi	Sürekli	Kimyasal saldırı veya Sabotaj	pH değerinde ani aşırı değişimler görülebilir, filtre sistemi hızlı şekilde tıkanabilir, çıkış suyunda partiküler madde görülebilir vb.			×				
pH	Arıtma Giriş	Sürekli	Çevrimiçi	Sürekli	Kimyasal saldırı (örn: asit veya baz içeren kimyasallar)	1-Kimyasal ajanlar solunum problemleri, cilt yanıkları ve zehirlenme gibi etkilere sahip olabilir. 2-Aşırı asidik veya alkali su, boruları aşındırabilir ve içme suyu kalitesini düşürebilir.	×	×	×	×	×	×	×
Sıcaklık	Arıtma Giriş	Sürekli	Çevrimiçi	Sürekli	Biyolojik saldırı Radyoaktif saldırı	Biyolojik ajanlar, bulaşıcı hastalıklara ve halk sağlığındaki genel düşüşe neden olabilir. Sıcaklık, kimyasal maddelerin konsantrasyonunu, etkinliğini ve suyun viskozitesini etkiler.	×	×	×	×	×	×	×
Basınç	Şebeke İsale	Sürekli	Çevrimiçi	Sürekli	Sabotaj (örn: hat patlamaları)	Basınç düşüşleri, suyun akmamasına veya hizmet kesintilerine neden olabilir, ayrıca bakterilerin boru cidarlarına tutunarak büyümesine neden olabilir.						×	×

1.2 Müdahale (Olay Anı)

1.2.1 KBRN Saldırıları Müdahale Ekibi

Ülkemizde KBRN ve siber saldırı olayları TAMP kapsamında afet kategorisinde yer almakta olup her türlü KBRN ve siber saldırı olayına müdahale çalışmaları AFAD sorumluluğundadır. KBRN ve siber saldırıların herhangi bir içme suyu sistem bileşenine yönelik olması durumunda da müdahale çalışmaları yürütmek, koordinasyonu sağlamak için gerekli çalışmalar AFAD tarafından yapılacaktır.

İçme suyu sistemine yapılan veya içme suyu sistemini etkileyen her türlü KBRN saldırısı için olaya özgü çalışma grubu AFAD tarafından kurulacaktır. AFAD liderliğinde olaya özgü kurulacak çalışma grubu destek çözüm ortakları aşağıda sıralanmıştır.

- Enerji ve Tabii Kaynaklar Bakanlığı
- İç İşleri Bakanlığı
- Ulaştırma ve Altyapı Bakanlığı
- Sanayi, Teknoloji Bakanlığı
- Çevre, Şehircilik ve İklim Değişikliği Bakanlığı
- Tarım ve Orman Bakanlığı
- Ticaret Bakanlığı
- Sağlık Bakanlığı
- Millî Savunma Bakanlığı
- Cumhurbaşkanlığı Savunma Sanayii Başkanlığı
- TÜBİTAK
- STK
- Özel Sektör

Gaziantep İli İçme ve Kullanma Suyu Sistemi dikkate alındığında ise yukarıda verilen destek çözüm ortaklarına ek olarak Gaziantep İli İçme ve Kullanma Suyu Sistemi'ne yapılacak olası KBRN saldırılarına karşı yukarıda verilen destek çözüm ortaklarına ek olarak GASKİ'nin önemli görev ve sorumlulukları olacaktır.

1.2.2 KBRN Saldırı Müdahale Planı

KBRN, saldırılar, ciddi bir tehdit oluşturan olaylardır ve acil müdahale gerektiren riskli durumlardır.

KBRN saldırıları karmaşık ve tehlikeli olaylar olduğundan, bu tür durumlarla başa çıkmak için eğitimli ve uzmanlaşmış ekiplerin görevlendirilmesi önemlidir. Ayrıca, saldırıların önlenmesi için güvenlik önlemleri almak ve toplumun farkındalığını artırmak da önemlidir.

İçme ve kullanma suyu sisteminin KBRN saldırılarında hedef alınması veya etkilenmesi durumunda AFAD koordinasyonunda müdahale planı uygulanır ve süreç yönetilir. İçme ve kullanma suyu sistemi için KBRN saldırısı için müdahale adımları saldırının türüne, boyutuna ve yerine bağlı olarak değişebilir. Ancak genel olarak, aşağıda temel adımlar yer almaktadır:

1. **İhbar Alınma Süreci:**

   İlk adım olayın ihbarın edilmesi ve AFAD'a bildirilmesi.

2. **Olayın Tespit Edilmesi:**

   KBRN saldırısının tespit edilmesidir. Alarm sistemleri, gözlemciler, sensörler ve raporlar gibi veri kaynakları kullanılarak saldırı tespit edilmelidir.

3. **Tehlike Değerlendirmesi:**

   Saldırının niteliği ve boyutu hakkında acil durum yönetim ekibi tarafından hızlı bir değerlendirme yapılmalıdır. Bu değerlendirme, olayın büyüklüğünü, etkilenen alanları ve potansiyel tehlikeleri anlamak için önemlidir.

4. **Güvenli Bölge Oluşturma:**

   Saldırının olduğu bölge, güvenli bir şekilde izole edilmelidir. Böylece etkilenen kişilerin sayısı azaltılabilir ve saldırıya karşı alınacak önlemler kolaylaşır.

5. **Tehlike Uyarısı ve Halkın Bilgilendirilmesi:**

   Kamu sağlığını korumak için etkilenen bölgelerde yaşayan halka tehlike hakkında bilgi verilmelidir. Uygun kanallar kullanılarak halka duyurular yapılmalıdır.

6. **Acil Durum Ekiplerinin Harekete Geçmesi:**

KBRN saldırılarında uzmanlaşmış acil durum ekipleri hızlı bir şekilde olay yerine gitmelidir. Acil durum yönetim ekibi AFAD tarafından kurulup koordine edilen eğitimli personellerden oluşmaktadır. Bu ekipler, tehlikenin türüne bağlı olarak itfaiye, sağlık, polis ve diğer uzmanları içerebilir. Acil durum ekipleri, KBRN saldırılarına karşı koruyucu giysiler ve ekipmanlar kullanarak güvenliklerini sağlamalıdır.

7. **Kurtarma ve Yardım:**

Etkilenen kişilerin tahliye edilmesi, tedavi edilmesi ve acil yardımın sağlanması gerekebilir. Kurtarma ekipleri, bu tür durumlara karşı hazırlıklı olmalıdır.

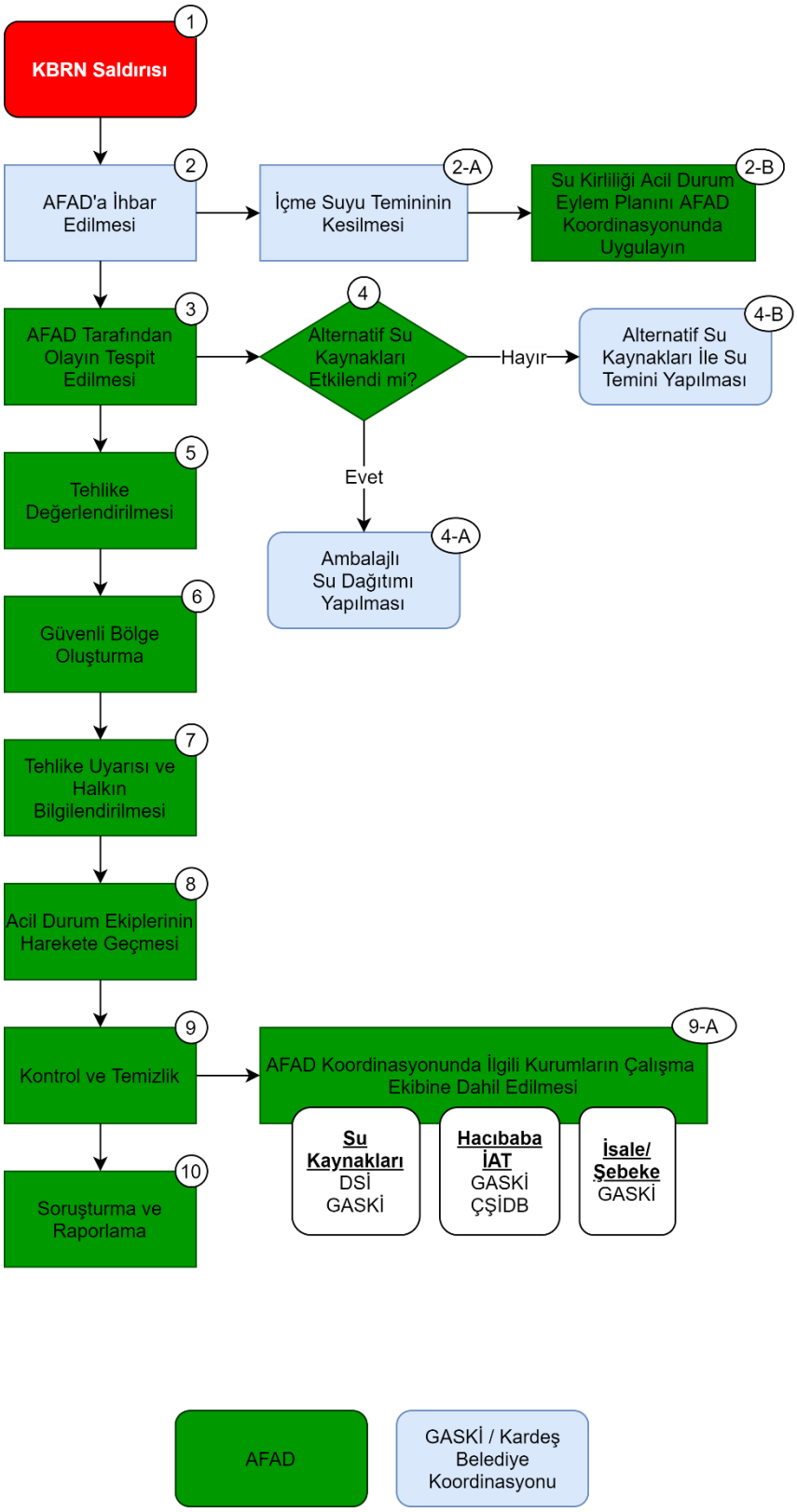
8. **Kontrol ve Temizlik:**

Saldırının ardından etkilenen bölge kontrol altına alınmalı ve temizlik çalışmaları yapılmalıdır. Kontaminasyonu önlemek ve yayılımı engellemek önemlidir. Bu aşamada içme ve kullanma suyu sisteminin ivedilikle işletmeye alınması için DSİ, Su Kanalizasyon İdareleri, Halk Sağlığı Genel Müdürlüğü ve olaya özgü ilgili kurumlar çalışmalara dahil edilir.

9. **Soruşturma ve Raporlama:**

Saldırının sebepleri ve sorumluları tespit etmek için soruşturma yapılmalıdır. Aynı zamanda, olayın nasıl ele alındığı ve müdahale süreci hakkında raporlar oluşturulmalıdır.

Gaziantep İli içme ve kullanma suyu sistem bileşenleri için KBRN saldırı müdahale planları akış şeması Şekil 1.2 ile verilmektedir



Şekil 1.2 KBRN Saldırıları Müdahale Ana Akış Şeması

1.2.2.1 KBRN Saldırı Durumunda Sistem Bileşenlerine Yönelik Operasyonel Eylemler

KBRN saldırıları, AFAD yönetiminde ve sorumluluğunda müdahale edilmesi gereken olaylardır. İçme kullanma suyu sisteminde oluşabilecek bir kirlilik durumuna yönelik operasyonel eylemler iyileştirme ve izolasyon olarak iki ana başlıkta ele alınabilir ancak her kirlilik durumu olaya özgü operasyonel planlamalar gerektirmektedir. Kirlilik durumlarında uygulanabilecek izolasyon ve iyileştirme operasyonları bu başlık altında değerlendirilmektedir.

İzolasyon: Su kirliliği olayları bağlamında izolasyon, kirliliğin yayılmasını önlemek için etkilenen alanı veya su sistemi bileşenini ayırma veya tecrit etme sürecini ifade etmektedir. Vanaların kapatılmasını, fiziksel bariyerlerin uygulanmasını veya kirlenmiş alana veya alandan su akışını durdurmak için diğer yöntemleri içerebilir.

İyileştirme: İyileştirme, kirletici maddelerin alandan uzaklaştırılması, bozulması veya nötralize edilerek orijinal haline geri döndürülmesi sürecidir. Su sistemi açısından bu işlem filtreleme, kimyasal arıtma, biyolojik arıtma ve hatta kirlenmiş bileşenlerin fiziksel olarak çıkarılması ve değiştirilmesi gibi süreçleri içerebilir. İyileştirmenin amacı, içme, sulama veya diğer kullanımlar için suyun tekrar güvenli olmasını sağlamaktır.

1.2.2.1.1 Su Kaynakları

Yerüstü Su Kaynaklarına Yönelik İzolasyon Operasyonları:

- Set ve Bariyerler: Bu fiziksel yapılar, kirleticileri bir yüzey suyu kütlesinin belirli bir alanı içinde tutmak için kullanılabilir. Örneğin, bir göl veya rezervuarda petrol sızıntısı olması durumunda, petrolün su kütlesinin geri kalanına yayılmasını önlemek için bomlar kullanılabilir.
- Absorban Malzemeler: Petrol veya diğer organik maddeler gibi belirli kirletici türlerini içermek ve emmek için kullanılabilir. Örneğin, emici pedler veya bomlar bir rezervuardaki petrol tabakasını tutmak ve absorbe etmek için kullanılabilir.
- Silt Perdeler: Bunlar deniz inşaatı, tarama ve ıslah projelerinde bir su kütlesindeki silt ve tortuyu kontrol etmek için kullanılan yüzer bariyerlerdir.

Örneğin, bir nehirdeki inşaat faaliyetleri sırasında tortu ve ilgili kirleticilerin aşağı akıntıya yayılmasını önlemek için kullanılabilirler.

- Derivasyon Bentleri veya Kanalları: Bu teknik, kirlenmiş su akışının hassas alanlardan uzağa yönlendirilmesini içermektedir. Örneğin, bir nehre kimyasal madde dökülmesi durumunda, kirlenmiş suyu mansaptaki içme suyu girişinden uzağa yönlendirmek için bir derivasyon kanalı inşa edilebilir.
- Su Yollarının Kapatılması: Aşırı durumlarda, kontaminasyonun yayılmasını önlemek için su yolları kapatılabilir. Örneğin, zehirli bir dökülme gibi büyük ölçekli bir kirlenme durumunda, su hattının kirlenmiş bölümünde ulaşım, kontrol altına alma ve temizleme operasyonlarına izin vermek için geçici olarak yasaklanabilir.

Yeraltı Suyu Kaynaklarına Yönelik İzolasyon Operasyonları:

- Hidrolik Kontrol: Kirleticilerin yayılmasını önlemek için kirlenmenin membaında kuyu açılarak veya mevcut kuyudan sular çekilerek kirleticinin yeraltı suyuna yayılması engellenebilir. Bu, örneğin, sızıntı yapan bir yeraltı depolama tankından çıkan petrol hidrokarbonlarının bir kamu su kaynağı kuyusuna ulaşmasını önlemek için uygulanabilir.
- Fiziksel Bariyerler: Yeraltında fiziksel bariyerlerin inşa edilmesi kirleticilerin yayılmasını önleyebilir. Bu, kirleticilerin bir akifer boyunca yanal olarak yayıldığı büyük ölçekli bir endüstriyel deşarj için uygun olabilir.
- Sahada Kapatma: Kirleticilerin yayılmasını önlemek için kirlenmiş alanın üzerine bir malzeme tabakasının yerleştirilmesini içermektedir. Tehlikeli bir maddenin yanlışlıkla yayıldığı ve yeraltı suyuna sızdığı bir senaryoda kullanılabilir.
- Yeraltı Suyu İzleme Kuyuları: Kirlenmiş alanın etrafına yeraltı suyu izleme kuyularının kurulması, kirlenmenin yayılmasını tespit etmek ve izlemek için kullanılabilir. Bu özellikle yavaş, kronik kirlenme durumlarında faydalı olabilir.
- Yeraltı Suyu Havzalarının Korunması: Suyun akifere ulaşmak için toprağa sızdığı alanların korunmasını ve kirlenmenin bu bölgelere yayılmasının önlenmesini içermektedir. Örneğin, tarımsal akış bir akiferde nitrat kirliliğine yol

açıyorsa, yeniden yağış alanlarında gübre uygulamasının kısıtlanması daha fazla kirlenmenin önlenmesine yardımcı olabilir.

Yerüstü Kaynaklarına yönelik İyileştirme Operasyonları:

- Fiziksel Uzaklaştırma: Kirleticinin doğrudan su kütlesinden uzaklaştırılmasını içermektedir. Örneğin, bir rezervuar veya gölde petrol sızıntısı olması durumunda petrolü uzaklaştırmak için sıyırma veya emici bomlar kullanılabilir.
- Biyolojik Arıtma: Kirleticileri parçalamak için biyolojik organizmaların kullanılmasını içerir. Örneğin, alg patlamalarından etkilenen bir gölde, rakip alglerin veya diğer organizmaların eklenmesi patlamanın kontrol edilmesine ve su kalitesinin yeniden sağlanmasına yardımcı olabilir.
- Kimyasal Arıtma: Kirleticileri daha az zararlı hale getirmek için çökeltmek, nötralize etmek veya başka bir şekilde reaksiyona sokmak için kimyasalların eklenmesini içermektedir. Bir nehirdeki ağır metal kirliliği için kullanılabilir; kireç ilavesi, metalleri uzaklaştırmak için çökeltebilir.
- Sediman Tarama: Kirliliğin sedimanlara bağlı olduğu durumlarda, kirlenmiş sedimanları fiziksel olarak uzaklaştırmak için tarama kullanılabilir. Geçmişteki endüstriyel deşarjların tortularda yüksek seviyelerde kirleticilere yol açtığı bir göl veya rezervuarda uygun olabilir.
- Yapay Sulak Alanlar: Bunlar, su kalitesini iyileştirmek için sulak alan bitki örtüsü, topraklar ve bunlarla ilişkili mikrobiyal toplulukları içeren doğal süreçleri kullanan mühendislik sistemleridir. Besin seviyelerinin yüksek olduğu ve ötrofikasyona yol açtığı durumlarda kullanılabilirler.

Yeraltı Suyu Kaynaklarına yönelik İyileştirme Teknikleri:

- Pompala ve Arıt: Bu yöntem, kirlenmiş yeraltı suyunun arıtılmak üzere yeraltından dışarı pompalanmasını içermektedir. Özellikle uçucu organik bileşikler veya petrol hidrokarbonları ile kirlenmiş yeraltı sularının arıtılmasında etkili olabilir. Örneğin, bir yeraltı depolama tankının sızarak çevredeki toprağı ve yeraltı suyunu benzinle kirlettiği bir sahayı temizlemek için kullanılabilir.
- Sahada Biyoremediasyon: Bu süreç, kirletici maddeleri parçalamak için doğal olarak oluşan bakterilerin uyarılmasını içermektedir. Örneğin, tarımsal akıştan

kaynaklanan bir akiferdeki nitrat kirliliği, denitrifikasyon bakterilerinin büyümesini teşvik etmek için melas gibi elektron donörleri eklenerek bu teknikle iyileştirilebilir.

- Kimyasal Oksidasyon: Bu teknik, yeraltı suyuna kimyasal oksidanlar enjekte ederek kirleticileri daha az zararlı formlara dönüştürmek için kullanılır. Madencilik veya endüstriyel faaliyetlerden kaynaklanan arsenik veya kurşun kirliliği gibi ağır metal kirliliği için uygulanabilir.
- İleri Oksidasyon Prosesleri (Advanced Oxydation Processes (AOP's)): Bu prosesler, çok çeşitli organik kirleticileri parçalayabilen yüksek reaktif hidroksil radikalleri üretimektedir. Bu, bileşiklerin genellikle geleneksel arıtma yöntemlerine dirençli olduğu yeraltı sularının farmasötik kirlenmesi için etkili bir yaklaşım olabilir.
- Geçirgen Reaktif Bariyerler ("Permeable Reactive Barriers" - PRBs): PRB'ler reaktif malzeme ile doldurulmuş ve kirlenmiş bir yeraltı suyu birikintisinin yoluna yerleştirilmiş bariyerlerdir. Kirlenmiş su bariyerden akar ve kirleticileri bozmak veya hareketsiz hale getirmek için malzeme ile reaksiyona girer. Örneğin, bu teknik klorlu çözücüler veya radyonüklidlerle kirlenmiş yeraltı suları için kullanılabilir.

1.2.2.1.2 İsale Hattı

İsale Hattı İzolasyona Yönelik Operasyonlar

- Vana İşletimi: Dağıtım sistemine benzer şekilde, sızıntılar veya patlamalar sırasında etkilenen bölümleri izole etmek için vanalar açılabilir veya kapatılabilir.
- Yedek Hatların Kullanımı: Kirlenme durumunda, su akışı yedek bir hat üzerinden yeniden yönlendirilebilir.
- Boru Tapaları: Geçici boru tapaları, onarım veya temizlik için boru hattının bir bölümünü izole etmek için kullanılabilir.
- Boru Kelepçeleri: Boru hattındaki küçük sızıntıları geçici olarak kapatmak ve sızıntı noktasını izole etmek için kullanılabilir.
- Basınç Kontrolü: İletim hattı içindeki basıncın modüle edilmesi bir kirlenme olayının kontrol altına alınmasına yardımcı olabilir.

- Sızdırmazlık: Kontaminasyon girişini önlemek için çeşitli sızdırmazlık türleri (mekanik, conta vb.) kullanılabilir.
- Pompa Muhafazası: Harici kirleticilerin girmesini önlemek için pompaların muhafazası kullanılabilir.

İsale Hattı İyileştirmeye Yönelik Operasyonlar:

- Hat Değişimi: Bir boru hattı kirlenme veya korozyon nedeniyle ciddi şekilde hasar gördüğünde, sızıntılara veya potansiyel kirletici sızıntısına neden olduğunda kullanılır.
- Boru Yeniden Kaplanması: Daha fazla bozulmayı ve potansiyel kirlenmeyi önlemek için küçük boru hasarı veya korozyon durumlarında kullanılabilir.
- Hidrostatik Test: Boru hattı bütünlüğünü sağlamak ve gelecekteki kirlenmeleri önlemek için şüpheli sızıntı durumunda veya boru onarımı veya değişiminden sonra uygulanmaktadır.
- Hiperklorinasyon: Boru hattındaki bir bakteriyel kirlenme olayının ardından kalan bakterileri ortadan kaldırmak için kullanılmaktadır.
- Basınç Yönetimi: Basınç düzensizliklerinin potansiyel olarak boru patlamalarına veya borulara kirletici maddeler girebilecek sifonlama olaylarına yol açabileceği durumlarda kullanılabilir.

1.2.2.1.3 Arıtma Tesisi

Su Arıtma Tesisi İzolasyonu:

- İzolasyon Vanaları: Bir arıza veya kirlenme durumunda arıtma sürecinin belirli kısımlarını izole etmek için kullanılır.
- By-pass Hatları: Su akışını kirlenmiş veya arızalı bir ünitenin etrafına yönlendirmek için kurulmaktadır.
- Muhafaza Alanları: Tesis içinde kimyasal dökülmeleri kontrol altına almak için kullanılır.
- İzolasyon Tankları: Kirlenmiş suyu arıtma tesisi içinde izole etmek için kullanılır.

Su Arıtma Tesisi İyileştirme:

- İleri Oksidasyon Prosesleri: Ham suda kalıcı organik kirleticiler veya belirli mikrobiyolojik kirleticiler tespit edildiğinde kullanılmaktadır.
- Membran Teknolojileri: Ham suda geleneksel arıtma proseslerinin etkili bir şekilde gideremediği belirli kimyasal veya biyolojik kirleticiler tespit edildiğinde kullanılmaktadır.
- Granül Aktif Karbon Adsorpsiyonu: Kirlilik belirli organik bileşikleri veya tat ve kokuya neden olan bileşikleri içerdiğinde kullanılmaktadır.
- Biyolojik Filtrasyon: Biyolojik olarak parçalanabilen kirleticiler (amonyak veya belirli organik bileşikler gibi) suda tespit edildiğinde kullanılmaktadır.

1.2.2.1.4 Şebeke/Musluk

Dağıtım Sistemi İzolasyonu:

- Hava Boşluğu Kurulumu: Dağıtım sisteminde geri akışı önlemek için servis bağlantılarının sonunda kullanılmaktadır.
- Geri Akış Önleyici Kurulumu: Suyun geri akış olaylarına eğilimli olduğu bağlantılara monte edilmektedir.
- Hidrant Kullanımı: Yangın hidrantları su akışını yönlendirmek için açılarak dağıtım sisteminin belirli bir bölümünün izole edilmesine yardımcı olabilir.
- Servis Bağlantısı Sızdırmazlığı: Belirli bir noktada kirlenme olması durumunda, kirlenmeyi izole etmek için servis bağlantıları geçici olarak kapatılabilir.
- Ayrık Hazneli Tank Kullanımı: Büyük tanklarda, kirlenme durumunda suyu izole etmek için bölmeler kullanılabilir.
- Tank Kaplaması: Suyu tank yapısı içindeki potansiyel kirleticilerden izole etmek için iç astar kullanılabilir.

Dağıtım Sistemi İyileştirmesi:

- Tek Yönlü Yıkama: İçilebilir olmayan bir suyun veya tortunun dağıtım sistemine girdiği bir geri akış olayını veya boru korozyonunu takiben kullanılabilir.

- Buz Püskürtme: Rutin denetimler sırasında veya bir mikrobiyal kontaminasyon olayının ardından borularda önemli bir biyofilm birikiminin tespit edildiği senaryolarda kullanılabilir.
- Hava ile Temizleme: Borularda tortu birikiminin tespit edildiği, su akışını veya kalitesini potansiyel olarak engelleyen durumlarda uygulanabilir.
- Dezenfektan Değiştirme: Rutin izleme, mevcut dezenfektana dirençli belirli mikrobiyal kirleticilerde bir artış tespit edilirse yapılabilir.
- Olay Sonrası Numune Alma: Dağıtım şebekesinin belirli bir bölümündeki su kalitesini etkileyen kimyasal bir dökülme gibi herhangi bir kirlenme olayının ardından uygulanabilir.

1.2.3 Siber Saldırı Müdahale Planı

- **Tehdit Tespiti ve Doğrulama:** Kullanılacak araçlar ve yöntemler; ağ trafik analizi araçları (örn. Wireshark), işletim sistemi günlük analiz araçları (örn. Splunk), ve ağ sızma tespit sistemleridir (örn. Snort). Bu araçlar sürekli olarak ağ trafiğini ve sistem davranışlarını izler, normalden sapma olması durumunda uyarı verirler. IT (Information Technology) ve siber güvenlik ekibi bu tespiti gerçekleştirir. Gerçekleştirilen tespitler ile olası bir siber saldırıyı erkenden fark edip hızlı bir şekilde önlem almak mümkün olabilir.
- **Tehdidi Sınıflandırma:** Doğrulanan tehdit, etkisinin ve ciddiyetinin belirlenmesi için sınıflandırılır. Sınıflandırma, NIST Cybersecurity Framework veya MITRE ATT&CK gibi standartlara göre yapılır. Sınıflandırma aşaması saldırının türünün ve seviyesinin anlaşılmasını sağlamaktadır. Bu da alınacak önlemleri ve önceliklendirme ihtiyacını belirlemektedir.
- **Kurumsal İletişim:** GASKİ dahil olmak üzere ilgili tüm tarafların hızlı bir şekilde bilgilendirilmesi gerekmektedir. Bilgi Teknolojileri ve İletişim Kurumu BTK ve USOM gibi yetkili kurumlar bilgilendirilirken, saldırıya maruz kalan sistemlerin yedeği alınır ve sistemler karantinaya alınır.
- **Saldırıyı İzole Etme ve Sınırlandırma:** Saldırının etkilediği sistemler ağdan izole edilir. Bu işlem, saldırının diğer sistemlere yayılmasını önlemek ve saldırının etkisini sınırlamak amacıyla yapılır. Örneğin, bir sunucu üzerindeki

anormal işlem yoğunluğu tespit edildiğinde, bu sunucu ağdan izole edilir veya trafiği sınırlandırılır.

- **Saldırının Etkisini Azaltma:** Siber saldırının yol açtığı hasarın etkisini azaltmak için acil düzeltmeler ve güncellemeler yapılır. Örneğin, bir ransomware saldırısı durumunda, etkilenen dosyaların yedeği geri yüklenir ve saldırının yayılmasını önlemek için gerekli yama ve güncellemeler hızlıca uygulanır.
- **Sistemi Kurtarma:** Saldırı sonrasında sistemlerin normal işleyişine geri dönmesini sağlamak için gereken adımlar atılır. Bu süreçte, sistemler yeniden başlatılır ve gerekiyorsa, işletim sistemi yeniden kurulur.
- **Olay İncelemesi ve Raporlama:** Olayın nedenlerini, etkilerini ve saldırının nasıl önlenebileceğini belirlemek için olayın ayrıntılı bir incelemesi yapılır. Bu inceleme sürecinde, saldırının kaynağı, hangi güvenlik açığından yararlanıldığı ve saldırının nasıl önlenebileceği gibi konular incelenir. Bu bilgiler, ileride benzer saldırıları önlemek için alınacak önlemlerin belirlenmesinde kullanılır.

1.3 Normal Operasyona Dönüş (Olay Sonrası)

1.3.1 KBRN Saldırısı Sonrası Normal Operasyona Dönüş

- **Olayın Değerlendirilmesi:**
  - KBRN saldırısı sonrası, saldırının etkileri ve kontaminasyonun yayılımı değerlendirilmelidir.
  - Güvenlik yetkilileri ve ilgili otoriteler, saldırının türüne bağlı olarak uygun önlemleri belirlemek için durumu analiz etmelidir.
- **Kontaminasyonun Temizlenmesi:**
  - Kontaminasyonun etkilerini ortadan kaldırmak için uygun dekontaminasyon işlemleri gerçekleştirilmelidir.
  - Kontamine olan alanlar, su kaynakları, arıtma tesisleri ve dağıtım sistemleri temizlenmeli ve dezenfekte edilmelidir.
- **Su Kaynaklarının İyileştirilmesi:**
  - Su kaynaklarının kalitesi kontrol edilmeli ve gerekli önlemler alınarak suyun tekrar kullanıma uygun hale getirilmesi sağlanmalıdır.

- Kimyasal, biyolojik veya radyolojik kontaminasyonun varlığına bağlı olarak uygun arıtma yöntemleri kullanılmalıdır.

- **Dağıtım Sisteminin Kontrolü:**
  - Dağıtım sistemi, kontaminasyonun yayılmasını önlemek için düzenli olarak kontrol edilmeli ve gerekli önlemler alınmalıdır.
  - Basınç kontrolü, vanalar ve pompalar, filtrasyon ve dezenfeksiyon sistemleri gibi bileşenler incelenerek gerekli iyileştirmeler yapılmalıdır.
- **Güvenlik Önlemlerinin Güçlendirilmesi:**
  - Saldırı sonrası, güvenlik önlemleri güçlendirilmeli ve sistemin gelecekteki saldırılara karşı daha dirençli hale getirilmesi sağlanmalıdır.
  - Fiziksel güvenlik önlemleri, siber güvenlik protokolleri, erişim kontrolleri ve izleme sistemleri gözden geçirilmeli ve geliştirilmelidir.
- **İlgili Otoritelerle İletişim:**
  - Olay sonrası, ilgili otoritelerle düzenli iletişim sağlanmalı ve gerekli bilgilendirme yapılmalıdır.
  - İlgili kamu kurumları, belediyeler, acil durum ekipleri ve sağlık kuruluşları ile iş birliği içinde hareket edilmelidir.
- **Eğitim ve Farkındalık:**
  - Sistem operatörleri, personel ve halk, KBRN saldırılarına karşı farkındalık düzeyini artırmak üzere eğitilmeli ve bilgilendirilmelidir.
  - Acil durum eğitimleri ve senaryoları hazırlanmalı ve düzenli olarak uygulanmalıdır.
- **İyileştirme ve İyileştirme Planlaması:**
  - Olayın ardından, sistemdeki zayıf noktaların belirlenmesi ve gerekli iyileştirmelerin yapılması için bir iyileştirme planı oluşturulmalıdır.
  - İyileştirme süreci, güvenlik önlemlerinin güçlendirilmesi, kontaminasyonun önlenmesi ve etkilerinin azaltılması için sürekli olarak gözden geçirilmelidir.

1.3.2 Siber Saldırı Sonrası Normal Operasyona Dönüş

- **Olayın Değerlendirilmesi:**

- Siber saldırısı sonrası, olayın etkileri ve sisteme verilen zarar değerlendirilmelidir.
- IT uzmanları ve siber güvenlik ekipleri, saldırının türüne ve etkilerine bağlı olarak uygun önlemleri belirlemek için durumu analiz etmelidir.

- **Sistem Güvenliğinin İyileştirilmesi:**
  - Saldırı sonrası, sistem güvenliğini iyileştirmek için gerekli önlemler alınmalıdır.
  - Güvenlik duvarları, saldırı algılama sistemleri, virüs koruma yazılımları ve diğer güvenlik araçları güncellenmeli veya güçlendirilmelidir.
- **Sistem ve Ağ İyileştirme:**
  - Saldırıya maruz kalan sistem ve ağ bileşenlerinin iyileştirme süreci başlatılmalıdır.
  - Zarar gören sunucular, ağ cihazları veya diğer sistem bileşenleri onarılmalı veya değiştirilmelidir.
- **Veri Kurtarma ve Geri Yükleme:**
  - Saldırı sonucunda kaybedilen veya zarar gören verilerin kurtarılması ve geri yüklenmesi için uygun adımlar atılmalıdır.
  - Yedekleme sistemleri ve veri kurtarma planları kullanılarak verilerin geri yüklenmesi sağlanmalıdır.
- **Siber Güvenlik İyileştirme:**
  - Saldırı sonrası, sistemin gelecekteki saldırılara karşı daha güvenli hale getirilmesi için siber güvenlik önlemleri iyileştirilmelidir.
  - Kullanıcı eğitimi, parola politikaları, erişim kontrolleri ve güvenlik politikalarının gözden geçirilmesi önemlidir.
- **Olayın İncelenmesi:**
  - Saldırı sonrası gerçekleştirilen detaylı bir olay incelemesi yapılmalıdır.
  - Saldırının nasıl gerçekleştiği, zayıf noktaların belirlenmesi ve gelecekteki saldırıları önlemek için alınabilecek önlemler incelenmelidir.
- **İlgili Otoritelerle İletişim:**
  - Olay sonrası, ilgili paydaşlarla düzenli iletişim sağlanmalı ve gerekli bilgilendirme yapılmalıdır.

- Siber olaylarla mücadele birimleri, siber suç birimleri ve diğer ilgili kurumlar ile iş birliği içinde hareket edilmelidir.

- **Eğitim ve Farkındalık:**
  - Sistem operatörleri, personel ve kullanıcılar, siber saldırılara karşı farkındalık düzeyini artırmak üzere eğitilmeli ve bilgilendirilmelidir.
  - Sosyal mühendislik saldırıları, kimlik avı gibi yaygın saldırı yöntemleri hakkında eğitimler düzenlenmelidir.

KAYNAKÇA

AFAD. (2020). *Gaziantep İl Risk Azaltma Raporu.* Ankara: AFAD.

Amar, P. K. (2010). Ensuring safe water in post-chemical, biological, radiological and nuclear emergencies. *Journal of Pharmacy and Bioallied Sciences*.

Bata, M. H., Cariveau, R., & Ting, D. S. (2022). Urban water supply systems resilience under earthquake scenario. *Scientific Reports*.

Bernard, T., Moßgraber, J., Madar, A. E., Rosenberg, A., Deuerlein, J., Lucas, H., . . . Ulitzur, N. (2015). *SAFEWATER – innovative tools for the detection and mitigation of CBRN related contamination event of drinking water.* Elsevier Ltd.

Binder, M., & Ackerman, G. (2019). *Pick Your POICN: Introducing the Profiles of Incidents Involving CBRN and Non-State Actors (POICN) Database.*

Burrows, W. D., & Renner, S. E. (1999). Biological Warfare Agents as Threats to Potable Water. *Environmental Health Perspectives*, 975-983.

Chemical, biological, radiological and nuclear response: introductory guidance: for training purposes only. (2014). ICRC.

Clark, R. M., Panguluri, S., Nelson, T. D., & Wyman, R. P. (2017). Protecting drinking water utilities from cyberthreats. *Journal of the American Water Works Association*.

Damikouka, I., Katsiri, A., & Tzia, C. (2005). Application of HACCP Principles in Drinking Water Treatment. *Elsevier*.

ENSTİTÜSU. (2017). *Acil Durum ve Tahliye Planı.* Ankara Üniversitesi Su Yönetimi Enstitüsü.

EPA. (2015). *How CanWater Utilities Obtain Critical Assets to Support Decontamination Activities?* EPA.

EPA. (2018). *Earthquake Resilience Guide for Water and Wastewater Utilities.* EPA.

EPA. (2021). *Incident Action Checklist – Cybersecurity.* EPA.

EPA. (2021). *Incident Action Checklist – Earthquake.* EPA.

EPA. (2021). *Incident Action Checklist – Extreme Cold and Winter Storms.* EPA.

EPA. (2021). *Incident Action Checklist – Extreme Heat.* EPA.

EPA. (2021). *Incident Action Checklist – Flooding.* EPA.

EPA. (2021). *Incident Action Checklist – Harmful Algal Blooms.* EPA.

EPA. (2021). *Incident Action Checklist – Pandemic Incidents.* EPA.

EPA. (2021). *Incident Action Checklist – Power Outages.* EPA.

EPA. (2023, 2). *EPA*. Incident Action Checklists for Water Utilities: https://www.epa.gov/waterutilityresponse/incident-action-checklists-water-utilities adresinden alındı

EU. (2013). *Review of sensors to monitor water quality.* EU.

Ganesan, K., Raza, S. K., & Vijayaraghavan, R. (2010). Chemical warfare agents. *Journal of Pharmacy and Bioallied Sciences*.

Government of Alberta. (2009). *Guidance Notes for Drinking Water Safety Plan Template.* Government of Alberta.

Government of Alberta. (2013). *Drinking water safety plan training course.* Government of Alberta.

Government of Alberta. (2013). *Drinking water safety plans : proactive risk management for water supply systems.* Government of Alberta.

Green, U., Kremer, J., & Moldaenke, C. (2003). *Detection of chemical threat agents in drinking water by an early warning real-time biomonitor.* Wiley Periodicals, Inc.

GWP Nepal. (2017). *Impact of Earthquake on Water Resources in Selected Earthquake Hit Areas.* Kathmandu: GWP Nepal.

Hindiyeh, M., Albatayneh, A., Tarawneh, R., Suleiman, S., Juaidi, A., Abdallah, R., . . . M., J. (2021). Preparedness Plan for the Water Supply Infrastructure during Water Terrorism—A Case Study from Irbid, Jordan. *Water*.

ICRC. (2014). *Chemical, Biological, Radiological and Nuclear Response.* Geneva: ICRC.

JCS. (2020). *Operations in Chemical, Biological, Radiological, and Nuclear Environments.* US Joint Chiefs of Staff.

Martellini, M., & Trapp, R. (2020). *21st Century Prometheus Managing CBRN Safety and Security Affected by Cutting-Edge Technologies.* Springer.

Meinhardt, P. (2005). Water and bioterrorism: preparing for the potential threat to U.S. water supplies and public health. *Annual Review of Public Health*.

Mohtadi, H., & Murshid, A. P. (2006). *A Global Chronology of Incidents of Chemical, Biological, Radioactive and Nuclear Attacks: 1950-2005.*

NATO. (2006). *Management of Intentional and Accidental Water Pollution.* Springer.

NATO. (2010). *Threats to Food and Water Chain Infrastructure.* Springer.

NATO. (2018). *Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security.* Springer.

NATO. (2020). *Functional Nanostructures and Sensors for CBRN Defence and Environmental Safety and Security.* Springer.

RCAP. (2005). *Emergency Response Planning Guide for Public Drinking Water Systems.* RCAP.

RSC. (2013). *Water Contamination Emergencies Managing The Threats.* Cambridge: RSC.

Serio, F., Martella, L., Imbriani, G., Idolo, A., & Bagordo, F. (2021). *The Water Safety Plan Approach: Application to Small Drinking-Water Systems—Case Studies in Salento (South Italy).* International Journal of Environmental Research and Public Health.

Setty, K., & Ferrero, G. (2021). Water Safety Plans. *Oxford Research Encyclopedia of Global Public Health*.

Shermer, S. D. (2006). The Drinking Water Security and Safety Amendments of 2002: Is America's Drinking Water Infrastructure Safer Four Years Later? *UCLA Journal of Environmental Law and Policy*.

Smith, M., & Reed, B. (2014). *An introduction to water safety plans.* Leicestershire: WEDC, Loughborough University.

Summerland, D. o. (2022). *Water Utility Emergency Response Plan.* California: District of Summerland.

SYGM. (2015). *İçme Suyu Güvenliği Planlarına İlişkin Dünyadaki Uygulamalar ve Türkiye.* Ankara: SYGM.

Teixeira, R., Carmi, O., Raich, J., Gattinesi, P., & Hohenblum, P. (2019). *Guidance for production of a Water Security Plan in drinking water supply.* EU.

Walski, T. (2015). *Can Real-Time Modeling Be Useful for Emergency Planning and Response?* ASCE Library: https://ascelibrary.org/doi/10.1061/9780784479162.063 adresinden alındı

WHO. (2003). *Application of Hazard Analysis and Critical Control Point (HACCP) methodology to pharmaceuticals.* WHO.

WHO. (2004). *Public health response to biological and chemical weapons : WHO guidance.* WHO.

WHO. (2005). *Water safety plans : managing drinking-water quality from catchment to consumer.* WHO.

WHO. (2006). *Water Safety Plan Manual.* WHO.

WHO. (2006). *Water Safety Plan Manual.* WHO.

WHO. (2006). *Water Safety Plans.* WHO.

WHO. (2011). *Case Study on Water Safety Plan Implementation and Lessons Learned.* WHO.

WHO. (2013). *Water safety plan quality assurance tool.* WHO.

WHO. (2015). *A practical guide to auditing water safety plans.* WHO.

WHO. (2018). *Strengthening operations and maintenance through water safety planning.* WHO.

#SudaSıfırİsraf

#SuVatandır

#SuMedeniyettir

#SuVerimliliği

@suyonetimi

@suyonetimi

/Suyonetimi

Su Yönetimi Genel Müdürlüğü

Su Verimliliği Seferberliği

Suda Sıfır Kayıp

Adres : T.C. Tarım ve Orman Bakanlığı, Beştepe Mahallesi

Alparslan Türkeş Caddesi No: 71 Yenimahalle / ANKARA

Telefon : 0312 207 50 00

www.tarimorman.gov.tr/SYGM www.suverimliligi.gov.tr

SUİŞ PROJE MÜHENDİSLİK ve MÜSAVİRLİK LTD. STİ. ENGINEERING & CONSULTING CO. LTD.

ANKARA / HAZİRAN 2023