EK - A1

Üniversitesi	**: İstanbul Teknik Üniversitesi**
Enstitüsü	**: Bilişim Enstitüsü**
Anabilim Dalı	**: Bilişim Uygulamaları**
Programı	**: Bilgi Güvenliği Mühendisliği ve Kriptografi**
Tez Danışmanı	**: Prof. Dr. Ertuğrul KARAÇUHA**
Tez Türü ve Tarihi	**: Doktora – Temmuz 2020**

ÖZET

TÜRKİYE'NİN ULUSAL SİBER GÜVENLİK STRATEJİ VE POLİTİKALARININ OLUŞTURULMASI ÇERÇEVESİNDE CAYDIRICILIK

Mustafa ŞENOL

Teknolojinin, özellikle bilgisayarların icadı sonrasında, her geçen gün daha hızlı gelişen bilgi sistemleri ve iletişim teknolojileriyle, internetin keşfi, gelişmesi ve yaygınlaşmasıyla, haberleşme, finans, enerji ve güvenlik gibi çok önemli faaliyetlerin bilgi sistemleri üzerinden yürütülmesi sonucu sağlanan kolaylıklar ve kazanımlarla bilişim sistemleri dünyada günlük yaşamın vaz geçilmez bir parçası olmuştur.

Bilişim sistemleri günlük yaşamın vaz geçilmezi olurken, siber ortamın önemi her geçen gün daha da artmış ve artmaya da devam etmektedir. Bu kapsamda siber ortamda bilgilere ve bilişim sistemlerine yönelik olarak başlayan kötü niyetli hareketlerin ve saldırıların da her geçen gün çeşitleri ve şiddetleri de artmaktadır. Devletler siber ortamı daha etkin kullanmanın yanında oluşan tehdit ve tehlikelere karşı koymak için strateji ve politikalar geliştirmeye ve bunları uygulamaya başlamışlardır.

Türkiye'de de bilgisayarların kullanımının artması ve internetin de yaygınlaşmasıyla, dünyadaki gelişmelere paralel olarak ortaya çıkan olumsuzlukların giderilmesi için başlatılan çalışmalarla geçmişten bugüne çok önemli mesafeler kat edilmiştir. Bu kapsamda oluşturulan ulusal siber güvenlik strateji ve politikalarıyla ilgili eksiklik ve yetersizliklerin giderilerek etkinliğinin artırılması yanında, siber caydırıcılık konusunun da siber güvenlik strateji ve politikaları ile birlikte bütüncül bir yaklaşımla ele alınmasının uygun olacağı değerlendirilmiştir.

Türkiye'de siber ortamda sahip olunan değerli varlıkların, bilgi ve iletişim sistemleri ile altyapılarının siber güvenliğinin etkinlikle sağlanabilmesi, ulusal siber güvenliğin Türkiye için öneminin ve ulusal güvenliğinin ayrılmaz bir parçası olduğunun ortaya konulması, siber savaş (savunma, taarruz ve caydırıcılık) için etkili bir güç olunabilmesi, ulusal siber gücün geliştirilerek, tek başına ve / veya diğer ulusal güç unsurlarıyla birlikte, caydırıcılık sağlayacak şekilde kullanılması ve siber alanda belirlenecek hedeflere ulaşılabilmesi maksatlarıyla ihtiyaç duyulan ulusal siber güvenlik strateji ve politikaların nasıl hazırlanması ve etkinlikle nasıl uygulanması gerektiği konusunda ilgili kişi, kurum ve kuruluşlara yol gösteren bir kaynak olarak yapılacak çalışmalara ışık tutulması amaçlanmıştır.

Bu amaç doğrultusunda; konuyla ilgili yapılan akademik çalışmalar, dünyada konuyla ilgili önde gelen devletlerin siber güvenlik strateji ve politikaları ile Türkiye'nin konuyla ilgili çalışmaları, uygulamaları ve sonuçları incelenmiş, geçmişten günümüze yaşanan olaylardan çıkarılan derslerle geleceğin ihtiyaç ve hedeflerine yönelik öngörülerde bulunularak, Türkiye'nin aynı zamanda caydırıcılık da sağlayacak siber güvenlik strateji ve politikalarının bilimsel yaklaşım ve yöntemlerle oluşturulması ve uygulanmasına yönelik esas ve prensiplerin belirlenmesine çalışılmıştır.

Bu kapsamda, bilgi, bilgisayar ve iletişim sistemleri ve bu konulardaki gelişmeler tarihi bir bakış açısıyla incelenirken, bilişim sistemleri ve güvenliği ile ilgili teknik kavramlarla, siber uzay, siber saldırı, siber taarruz, siber suç, siber terörizm, siber güvenlik, siber savunma, siber savaş, siber istihbarat, siber güç vb. kavramlar, siber güvenlik strateji ve politikaları ile siber caydırıcılık konularında, yerli ve yabancı hakemli dergiler ve akademik yayınlar başta olmak üzere, konuyla ilgili kurum ve kuruluşların yayınları ve belgeleri, kitaplar, dergiler, kütüphane ve internet ortamları taranmış, gelişmelerin takibi bağlamında çeşitli konferans ve çalıştaylara katılım sağlanmış, konuyla ilgili kurum ve kuruluş yetkilileri ile görüşmelerde bulunulmuştur.

Bu çerçevede; Strateji ve Güvenlik konusunda 20'nin üzerinde kitap, doküman ve çalışma, Siber Güvenlik ve Stratejisi konusunda 30'un üzerinde kitap, doküman ve çalışma, Dünya Ülkeleri Siber Güvenlik Strateji Belgeleri ve Eylem Planları konusunda başta ABD, Çin, Rusya, Fransa, İngiltere, İsrail, Hindistan, Kuzey Kore, Almanya, Kanada, Hollanda, Finlandiya, Japonya, Avustralya ve İran olmak üzere 20'ye yakın ülkenin belgeleri, Türkiye Siber Güvenlik Stratejileri ve Eylem Planları konusunda başlangıçtan bugüne hazırlanarak uygulamaya konulan 17 strateji belgesi ve eylem planı, Caydırıcılık ve Siber Caydırıcılık konusunda 30'un üzerinde kitap, doküman ve çalışma incelenmiş, konuyla ilgili gelişmelerle ilgili seminer, sempozyum, panel, çalıştay ve konferanslar kapsamında 20'nin üzerinde etkinliğe katılım sağlanmıştır.

İncelemeler sonrası analiz ve düzenleme çalışmaları yapılarak, İstanbul Teknik Üniversitesi Lisansüstü Tez Yazım Kılavuzu ve Lisans Üstü Tez Şablonu esasları doğrultusunda hazırlanan tezin içeriği 7 ana bölümden oluşmuştur.

Giriş bölümünde; bilgi ve iletişim sistemleri konusunda gelişmeler ile yaşanan kötü niyetli hareket ve saldırılara karşı ulusal siber güvenliğin sağlanması için strateji ve politikaların geliştirilmesi önemi ve ihtiyacı açıklanmıştır.

Siber güvenlikle ilgili terim ve kavramlar bölümünde; siber güvenlik konusunun bütüncül bir yaklaşımla ele alınarak doğru anlaşılması için öncelikle terim ve kavram birliği sağlanması, ortaya çıkan kavramlarla ilgili gelişmelerin bilinmesinin önemi doğrultusunda, konuyla iç içe olan ve en çok kullanılan terim ve kavramlar tanımlanarak kısaca açıklanmıştır

Siber savaş bölümünde; siber ortamda yaşanan siber saldırılar ve taarruzlar sonucunda siber güvenliğin ulusal güvenlik sorunu ve ulusal güvenliğin ayrılmaz bir parçası olduğu görüşünü destekleyen, geçmişte başlayan, günümüzde devam eden ve gelecekte de artarak devam edecek olan siber saldırı ve savaşlarla ilgili bilgiler verilmiştir.

Siber caydırıcılık bölümünde; geçmişten günümüze siber olay, saldırı ve savaşlardan da örnekler verilerek, savaşlarda kazanmaktan çok caydırıcılığın daha iyisi olabileceği düşüncesi ile siber güvenlik uygulamalarında dünyada çok yeni olan, Türkiye'de ise yeterli önem ve önceliğin verilmediği görülen bu konuda yaklaşımlar ortaya konmuştur.

Ulusal siber güvenlik strateji ve politikaları bölümünde; strateji ve politika kavramları açıklanmış, kurumsal ve ulusal siber güvenlik stratejileri ile bu konuda önde gelen ülkelerin ve Türkiye'nin mevcut siber güvenlik strateji ve politikaları hakkında bilgiler verilmiştir.

Caydırıcılık sağlayacak siber güvenlik strateji ve politikalarının oluşturulması bölümünde; ulusal siber güvenlikte söz sahibi ülkelerin ulusal siber güvenlik strateji belgeleri ile bazı uluslararası kurumların çalışmalarından elde edilen bilgilerden hareketle, Türkiye için mevcut stratejiler ve eylem planları da dikkate alınarak, caydırıcılık da sağlayacak ulusal siber güvenlik stratejisi ve politikalarının hazırlanması ve uygulanması için bir yaklaşım tarzı ortaya konmuştur.

Sonuç ve öneriler bölümünde; tez konusu kapsamında yapılan çalışmanın sonuçları ve yapılan değerlendirme ile görüş ve öneriler sunulmuştur.

Bu tez ile ortaya konulan ve önerilen yaklaşım tarzı; bilimsel taktik ve teknikler çerçevesinde, mevcut durumun değerlendirilmesinden belirlenen hedefe ulaşılmasına kadar teşkilat, kapsam, planlama ve uygulama aşamaları ile süreç içerisinde kontrol ve denetim faaliyetleri ile geliştirme faaliyetlerini içeren 8 aşamalı "Ulusal Siber Güvenlik Stratejisi Oluşturma ve Uygulama Yaşam Döngüsü"dür.

Ayrıca bu yaşam döngüsü içerisinde, bu döngüden, yani 'Ulusal Siber Güvenlik Stratejisinden ve Siber Gücün Yönetiminden', ana sorumlu olarak ve 2016-2019 Ulusal Siber Güvenlik Stratejisinde vurgulanan ve Türkiye'de halâ eksikliği görülen "Siber güvenlik alanında koordinasyonu sağlayacak güçlü bir merkezi kamu otoritesi" ihtiyacını da karşılamak üzere, mevcut yönetim sisteminde Cumhurbaşkanlığına bağlı, "Milli Siber Güvenlik Başkanlığı" yapılanması önerilmektedir.