Ulusal ve Uluslararası Bilgi Güvenliği Politikalarının Analizi Üzerine Karşılaştırmalı Bir İnceleme

Arif TULUK
Prof. Dr. Süleyman Sadi SEFEROĞLU

Hacettepe Üniversitesi, Eğitim Fakültesi
Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

Uluslararası Eğitim Teknolojisinde Yeni Eğilimler Konferansı
INTET2016
Salamis Bay Conti Hotel, Gazimağusa, KKTC
03 - 04 Mayıs 2016

İçerik

- Giriş
- Önem
- Amaç
- Yöntem
- Bulgular ve Tartışma
- Sonuçlar ve Öneriler

Giriş (1)

- Ülkelerin kamu düzenine ilişkin birçok faaliyet günümüzde bilgi sistemlerine taşınmaktadır
- Ulusal kalkınmanın temel dinamizmini ortaya koyan bankacılık, finans, eğitim, ulaştırma, haberleşme, vb. pek çok sektör artık internet teknolojileri sayesinde vatandaşa ve iş dünyasına doğrudan hizmet sağlamaktadır.

Giriş (2)

- **Bilgi sistemlerinin risklere ve tehditlere karşı korunmasının** önemi daha da anlaşılmaktadır.
- 1990'lı yılların başından itibaren ABD, Almanya, Japonya gibi bazı ülkeler bu risklerin farkına erken vararak söz konusu risklerle başa çıkmanın yolunu aramışlardır.

Bilgi Güvenliği (1)

- Bilgi güvenliği bilginin korunduğu ve saklandığı bilgi sistemlerinin ve sistemin içerdiği bilginin
  - yetkisiz erişimine,
  - kullanımına,
  - ifşa edilmesine,
  - değiştirilmesine,
  - incelenmesine,
  - hasar verilmesine veya
  - yok edilmesine karşı korunması ve
  - buna ilişkin tedbirlerin bütünü olarak tanımlanabilir.

Bilgi Güvenliği (2)

- Kişisel bilgisayarlardan kurumsal ve ulusal çaptaki tüm bilgi sistemlerine ve kritik altyapılara uzanan geniş bir çerçevede bilgi sistemlerini kapsayan bir güvenlik yönetimi anlayışıdır.

(Unescap, 2008)

Çalışmanın Önemi (1)

- Ülkemizin gelişmiş ülkelere göre yapılan düzenlemeler ve kurumsallaşmalar bağlamında geri kaldığı, gereksinimlerin karşılanmasına yönelik adımların hızlandırılmasında yarar olacağı değerlendirilmektedir.

Çalışmanın Önemi (2)

- Bilgi güvenliği konusu toplumsal yaşamda çok farklı kesimleri ve ilişkileri etkileyebilmektedir.
- Çok hızlı hareket edilmesi ve konuyla ilgili düzenlemelerin hızla yapılması gerekmektedir.
- Bu alandaki uluslararası eğilimlerin ülkemizdeki mevcut durum ile bir arada değerlendirilmesine ihtiyaç duyulmaktadır.

Çalışmanın Amacı (1)

- Bu çalışmada, ulusal ve uluslararası bilgi güvenliği politikaları analiz edilmiştir.
- Bu kapsamda, ulusal bilgi güvenliği uygulamaları, internet teknolojilerinin getirdiği bilgi güvenliği algısındaki değişimleri de içeren bir kavramsal çerçevede incelenmiştir.

Çalışmanın Amacı (2)

- Gelişmiş ülkelerin geliştirdiği ulusal bilgi güvenliği politikaları, stratejileri ve rehber ilkeleri ışığında,
  - Ülkemizin ihtiyaçlarına cevap verecek bir ulusal bilgi güvenliği politikası, stratejisi ve yasasının temel elemanlarının tespit edilmesi,
  - Çözüm önerilerinin sunulması,
  - Hazırlıkları devam eden yasa çalışmasının yeniden ele alınmasına katkıda bulunulması amaçlanmaktadır.

Araştırma Soruları (1)

- Ulusal bilgi güvenliğinin stratejik unsurları nelerdir?

- Ülkemizin ulusal bilgi güvenliği politikası, stratejik yönelimi ve kurumsal yapılanmasının geliştirilmesinde katkıları olabileceği değerlendirilen ülkelerin ulusal bilgi güvenliği politikaları, stratejik yönelimleri ve kurumsal yapılanma durumları nasıldır?

Araştırma Soruları (2)

- Ülkemizde ulusal bilgi güvenliği alanındaki gelişmeler dikkate alındığında ulusal bilgi güvenliği politikalarının geliştirilmesi üzerine getirilebilecek çözüm önerileri neler olabilir?

Yöntem

Yöntem

- Yöntem
  - Araştırmanın Yöntemi
  - Veri Toplama Araçları
  - Verilerin Analizi

Araştırmanın Yöntemi

- Bu araştırma genel tarama modeli türünde bir araştırmadır.

Veri Toplama Araçları

- Bu çalışmada ulusal bilgi güvenliği politikaları alanında gerçekleştirilmiş çalışmalar, raporlar ve diğer eserler incelenmiştir.

Verilerin Analizi (1)

- Yapılan alan yazın taramasında,
  - Ulusal bilgi güvenliğinin stratejik unsurları,
  - Ülkemize katkısı olabileceği değerlendirilen Japonya, ABD, Almanya, İngiltere ve Fransa'daki ulusal bilgi güvenliği politikaları, stratejik yönelimleri ve kurumsal yapılanma durumları,

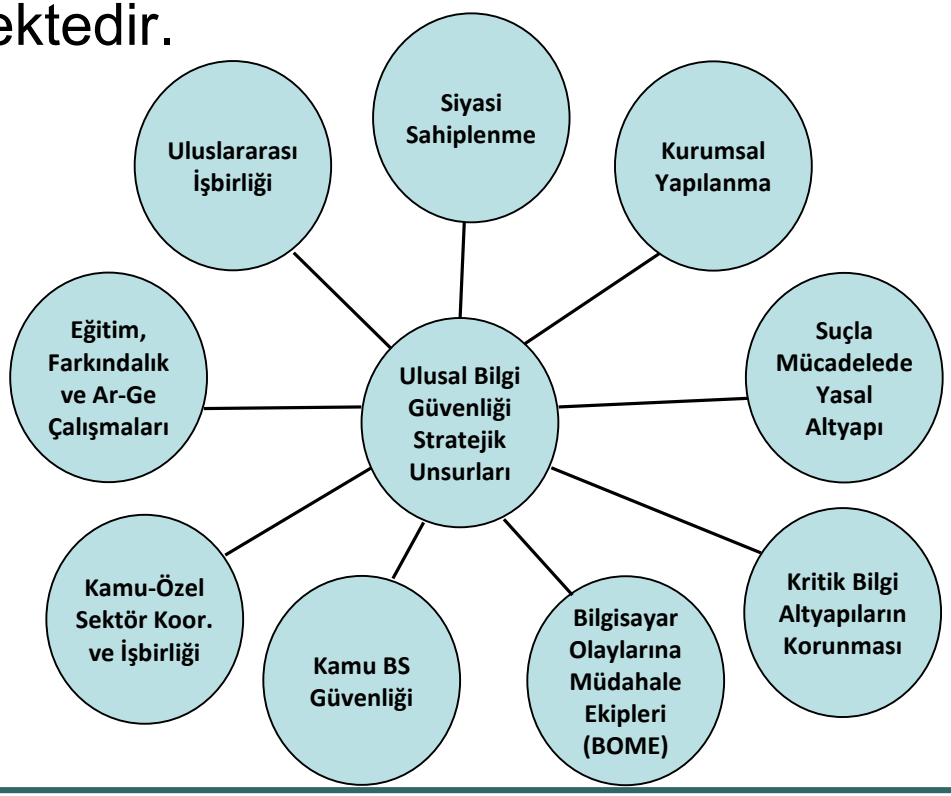
Verilerin Analizi (2)

- Ülkemizdeki ulusal bilgi güvenliği politikaları alanındaki gelişmelere ulaşılarak sistemli bir betimsel analiz çalışması yapılmıştır.

Bulgular ve Tartışma

Ulusal Bilgi Güvenliğinin Stratejik Unsurları Nelerdir?

- Yapılan incelemeler ulusal bilgi güvenliğinin stratejik unsurlarının dokuz ana başlık altında incelenebileceğini göstermektedir. *(ITU, 2011)*



Ülkemizin ulusal bilgi güvenliği politikası, stratejik yönelimi ve kurumsal yapılanmasının geliştirilmesinde katkıları olabileceği değerlendirilen ülkelerin ulusal bilgi güvenliği politikaları, stratejik yönelimleri ve kurumsal yapılanma durumları nasıldır?

Çeşitli Ülkelerin Ulusal Bilgi Güvenliği Politikaları, Stratejik Yönelimleri ve Kurumsal Yapılanma Durumları

- Japonya,
- ABD,
- Almanya,
- İngiltere ve
- Fransa'daki ulusal bilgi güvenliği politikaları, stratejik yönelimleri ve kurumsal yapılanma durumları incelenmiştir.

Japonya (1)

- Bilgi Teknolojileri Temel Kanunu
- Bilgi Güvenliği Politika Konseyi tarafından görevlendirilen iki farklı uzmanlar kurulu
  - "Bilgi Güvenliği Kültürü Uzmanlar Kurulu"
  - "BT Stratejisi Uzmanlar Kurulu"

(Japonya Başbakanlığı, Tarihsiz)

Japonya (2)

- “Ulusal Bilgi Güvenliği Stratejisi” belgesi hazırlanarak yürürlüğe konulmuştur.
- Stratejinin uygulama süresi ile ilgili olarak 3 yıllık bir plan öngörülmüştür.
- Bu kapsamda 2009 yılı için yeni bir ulusal bilgi güvenliği strateji belgesi oluşturulmuştur.

(National Information Security Policy Council, Japan, 2009)

Japonya (3)

- Temel stratejik önceliklerin yanı sıra, merkezi ve yerel otoriteler ile kritik altyapılar, iş dünyası ve vatandaşı hedef alan **212** adet eylem hayata geçirilmiştir.

(Yamada, Yamagishi & Katsumi, 2010)

Japonya (4)

Şekil 1: Japonya Ulusal Bilgi Güvenliği Kurumsal Yapılanması.

Kaynak: National Information Security Center, Japan, 2007.

Amerika Birleşik Devletleri (1)

- Federal Bilgi Güvenliği Yönetimi Yasası (Federal Information Security Management Act-FISMA)

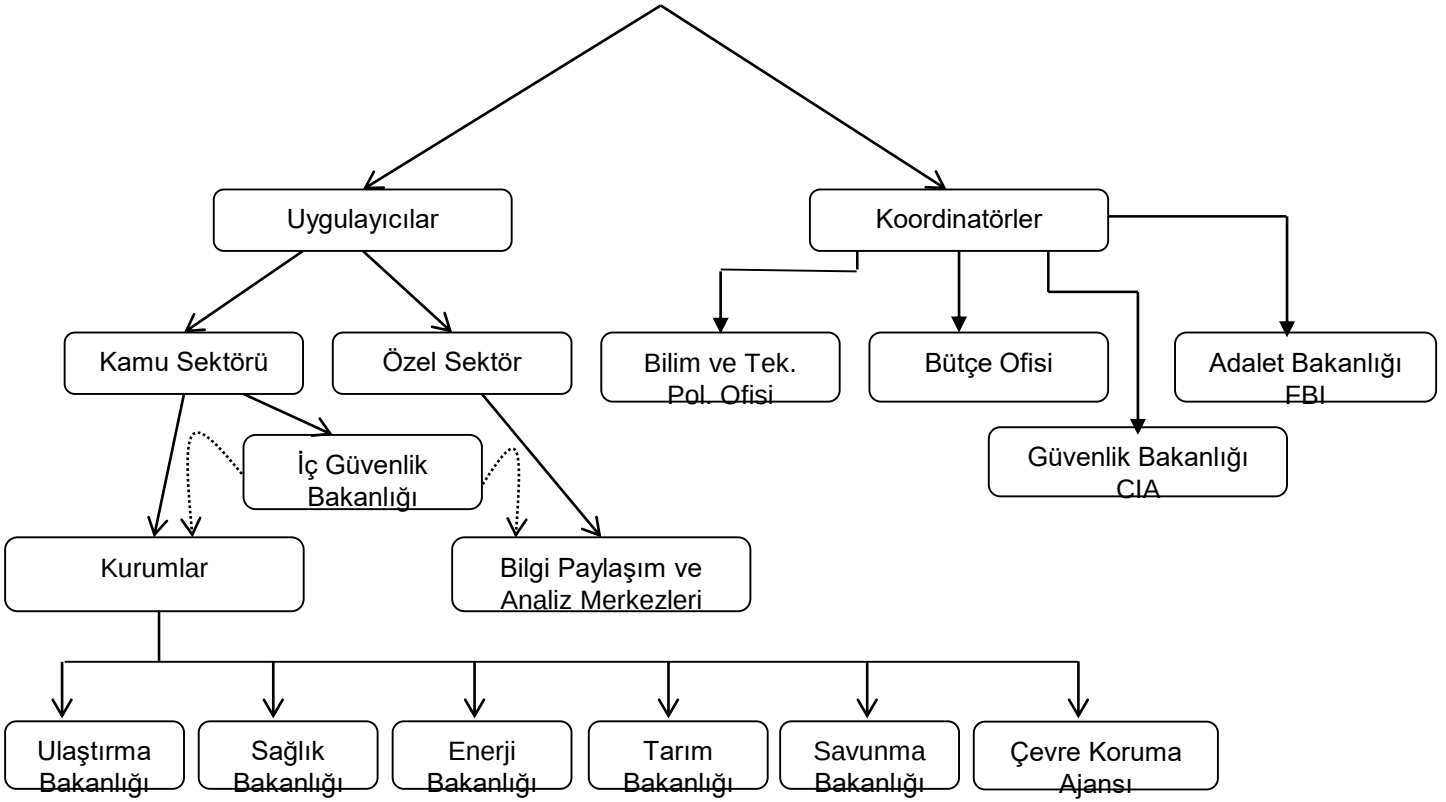
(National Institute of Standards and Technology, 2004)

- İlk ulusal strateji olarak 2003 yılında "Güvenli Siber Uzay İçin Ulusal Strateji" (National Strategy to Secure Cyberspace) yürürlüğe girmiştir.

Amerika Birleşik Devletleri (2)

- Söz konusu strateji belgesi 2009 yılında gözden geçirilerek güncellenmiş haliyle uygulamadadır.
- “Kritik Altyapı ve Ana Varlıkların Fiziksel Korunmasına İlişkin Ulusal Strateji” belgesi hazırlanmıştır.

Amerika Birleşik Devletleri (3)



Şekil 2: ABD Siber Güvenlik Stratejisi Uygulama Organizasyonu.

Kaynak: Ladani ve Berenjkoub, 2006.

Almanya (1)

- Merkezi Şifre Ajansı (Zentralstelle für das Chiffrierwesen, ZfCh)
- “Kurumlar arası BT Güvenliği Komitesi” (ISIT) kurulmuştur.
- Merkezi Şifre Ajansı, 1989 yılında Bilgi Teknolojileri Güvenliği Merkezi Ajansına (Zentralstelle für Sicherheit in der Informationstechnik, ZSI) dönüştürülmüştür.

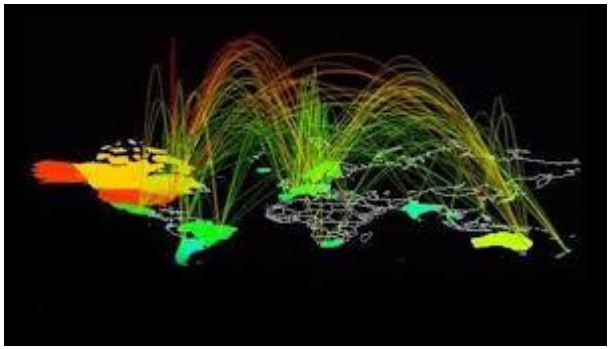
Almanya (2)

- 1989 yılında bilgi güvenliği alanında ilk ulusal politika belgesi yayımlanmıştır.
- Alman Bilgi Güvenliği Ajansı ZSI (Zentralstelle für die Sicherheit in der Informationstechnik) tarafından "BT Güvenliği Kavramsal Çerçevesi" çıkarılmıştır.
- ZSI, 1991 yılında BSI'ye dönüşmüştür.

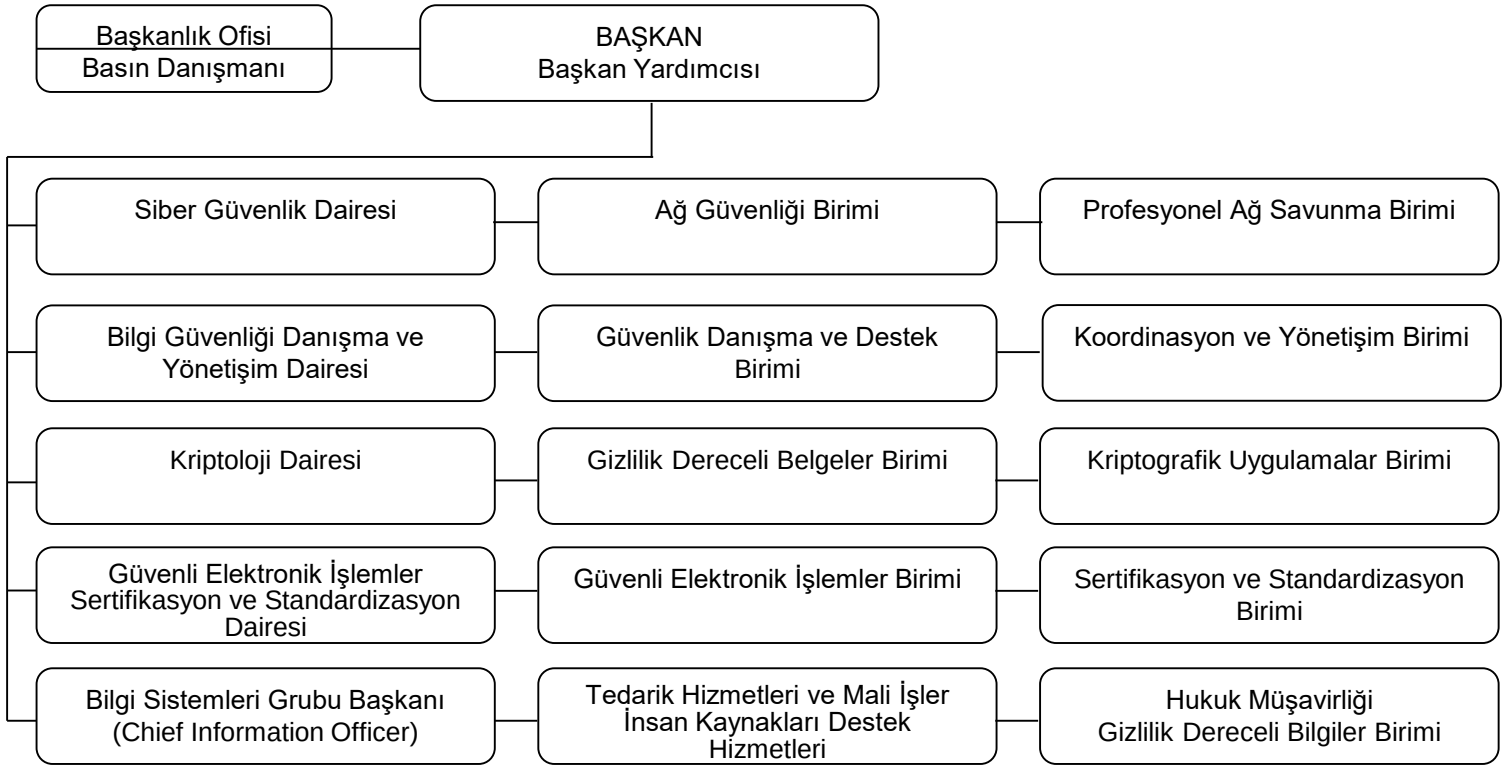
(BSI, 1989)

Almanya (3)

- 2005 yılında Bilgi Güvenliği ve Kritik Altyapıların Korunmasına İlişkin Ulusal Strateji yürürlüğe girmiştir.
- 2011 yılında Alman Ulusal Siber Güvenlik Stratejisi yürürlüğe girerek özellikle siber ortam kaynaklı risk ve tehditler ile mücadele amacına vurgu yapılmıştır.



Almanya (4)



Şekil 3: Alman Federal Bilgi Güvenliği Örgüt Şeması.

Kaynak: BSI, 2015.

Fransa (1)

- Şifre Teknik Daire Başkanlığı (Direction Technique du Chiffre-DTC)
- Şifre Teknik Merkezi (Central Technique du Chiffre STC-CH)
- İletişim Güvenliği ve Şifre Hizmetleri Merkezi Birimi (Service Central du Chiffre et Sécurité des Télécommunications)
- Bilgi Sistemleri Güvenliği Merkezi Birimi (Service Central de la Sécurité des Systèmes D'information-SCSSI)
- Bilgi Sistemleri Güvenliği Merkezi (Direction Centrale de la Sécurité des Systèmes d'Information -DCSSI)

Fransa (2)

- Fransız Ulusal Bilgi Güvenliği Ajansı (Agence nationale de la sécurité des systèmes d'Information- ANSSI) kurulmuştur.
- “Ulusal Bilgi Sistemleri Savunma ve Güvenliği Stratejisi” ile özellikle siber uzaydan gelen risk ve tehditlere karşı bir stratejik çerçeve oluşturma çabaları.

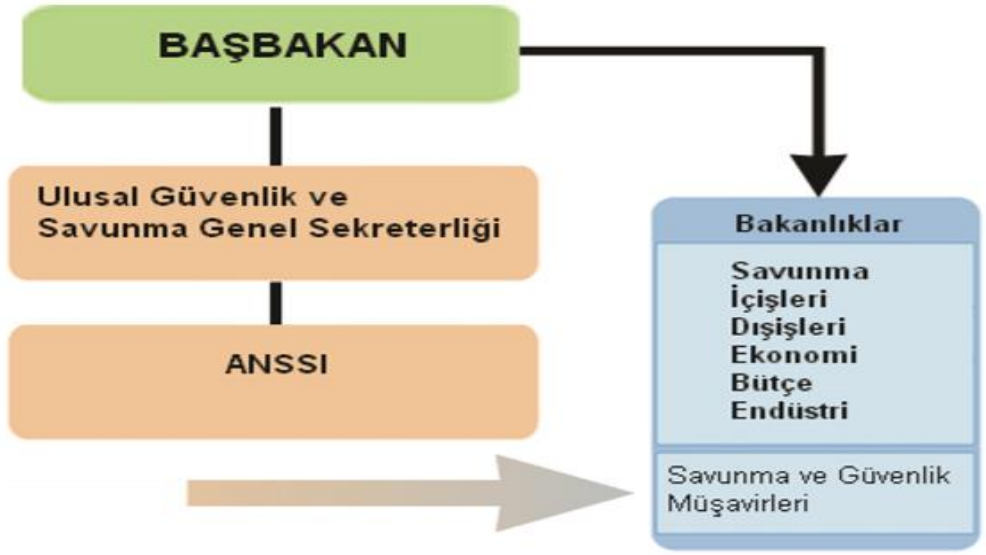
(ANNSI, 2011)

Fransa (3)

- Beyaz Kitap ile toplumun ve ülkenin bilgi sistemlerinin ciddi bir güvenlik riski ile karşı karşıya olduğu belirtilmiş ve Fransa'nın siber ortamda savunma kapasitesinin artırılması gerekliliğine işaret edilmiştir.
- Fransa'nın önümüzdeki 15 yıl içerisinde karşılaşacağı en önemli milli güvenlik riskinin başında *siber saldırıları* görmektedir.

(Ministère de la Défense, 2008)

Fransa (4)



Şekil 4: Fransa'nın Ulusal Bilgi Güvenliği Kurumsal Yapılanması.

Kaynak: SSI, (Tarihsiz).

İngiltere (1)

- Siber Güvenlik Ofisi (The Office of Cyber Security)
- Siber Güvenlik ve Bilgi Güvencesi Ofisi (The Office of Cyber Security and Information Assurance-OCSIA)
- OCSIA faaliyetlerini Birleşik Krallık Kabine Ofisi bünyesinde bir merkezi kamu kurumu olarak sürdürmektedir. *(ITU, 2011)*

İngiltere (2)

- 2010 yılında Stratejik Savunma ve Güvenlik Gözden Geçirmesi ilan edilmiş ve "Belirsizlik Çağında Güçlü Britanya" isimli ulusal güvenlik stratejisi yayımlanmıştır.
- Terörizm, siber savaş, uluslararası askeri kriz ve doğal afetler gibi geleneksel olmayan yeni tehdit unsurları tanımlanmıştır.
- Siber güvenlik riskleri ve siber savaş tehdidi en öncelikli tehdit olarak görülmektedir.

(Cabinet Office, 2010)

İngiltere (3)

- Ulusal Siber Güvenlik Stratejisi yayınlanmıştır.

(Cabinet Office, 2011)

Ülkemizde ulusal bilgi güvenliği alanındaki gelişmeler dikkate alındığında ulusal bilgi güvenliği politikalarının geliştirilmesi üzerine getirilebilecek çözüm önerileri neler olabilir?

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (1)

- İlk çalışma, Bilişim ve Ekonomik Modernizasyon Raporu olarak bilinen rapordur.

(World Bank, 1993)

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (2)

- 1996 yılında kurulan Güvenlik Çalışma Grubu çalışmalarını e-Türkiye Girişimi ile koordineli olarak sürdürmüş ve **13** adet taslak eylem planı hazırlanmıştır.
- Güvenlik Çalışma Grubu'nun çalışması taslak halini almış ancak kanun tasarısına dönüşememiştir.

(Başbakanlık, 2002)

- 1998 yılında Başbakanlık Müsteşarının başkanlığında kamu kurum ve kuruluşlarının katılımı ile Kamu-Net Üst Kurulu ve Kamu-Net Teknik Kurulu oluşturulmuştur.

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (3)

- 1999 yılı Temmuz ayında Ulaştırma Bakanlığı tarafından kabul edilen "Türkiye'de Enformasyon Politikası ve Enformasyon Altyapısı Ana planı (TUENA)" ile ülkemizde bilgi toplumuna dönüşümde ilk defa bütünsel bir bakış açısı yakalanmış ve bu kapsamda yapılması gerekenler çeşitli kurum ve kuruluşların katkılarıyla analiz edilmiştir.

(Ulaştırma Bakanlığı, 1999)

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (4)

- "Ulusal Bilgi Güvenliği Kanun Taslağı" çalışmaları 2005 yılına kadar sürdürülmüş ancak taslağın kapsamı ve bilgi güvenliği kavramının anlamı konusunda tam bir mutabakat oluşturulamadığı için kanun tasarısına dönüşememiştir.

(Ünver, Canbay & Özkan, 2010)

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (5)

- e-Dönüşüm Türkiye Projesi 2003 yılında ilan edilmiştir.
- Projenin başlıca hedefleri;
  - Katılımcı, şeffaf, etkin ve basit iş süreçlerine sahip olmayı ilke edinmiş bir devlet yapısı oluşturacak koşulların hazırlanması,
  - Bilgi ve iletişim teknolojileri politikaları ve mevzuatının öncelikle Avrupa Birliği müktesebatı çerçevesinde gözden geçirilerek yeniden düzenlenmesi,
  - e-Europe+ kapsamında aday ülkeler için öngörülen eylem planının ülkemize uyarlanması.

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (6)

- DPT Müsteşarlığının koordinatörlüğünde 8 çalışma grubuyla yürütülen çalışmalar sonucu, 2003–2004 yıllarını kapsayan bir Kısa Dönem Eylem Planı hazırlanmıştır.
- Ulusal Bilgi Güvenliği Kanunu'nun çıkarılması hedeflenmiştir ancak yasalaşma sürecinin başlatılması mümkün olmamıştır.

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (7)

- Ülkemizde bilgi toplumuna dönüşüm sürecinde üretilen en kapsamlı ulusal politika metni, 2006–2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve Ek'i Eylem Planıdır.
  - "Bilgi Güvenliği İle İlgili Yasal Düzenlemeler" başlıklı 87 numaralı eylem ile
  - "Ulusal Bilgi Sistemleri Güvenlik Programı" adındaki 88 numaralı eylem planlanmıştır.
- Ancak bilgi güvenliği ile ilgili yasal düzenlemeler konusunda gelişme kaydedilmesine rağmen yasal düzenleme tamamlanamamıştır.

Ülkemizde Ulusal Bilgi Güvenliği Alanındaki Gelişmeler (8)

- 2012 yılında Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bünyesinde bir Siber Güvenlik Kurulu kurulmuştur.
- Ulusal Bilişim Güvenliği Kanun Taslağı çalışmaları devam etmektedir.
- Ulusal bilgi güvenliği ile ilgili yasal düzenleme tedbirlerinin ilk olarak yer verildiği kalkınma planı, Sekizinci Beş Yıllık Kalkınma Planı (2001-2005)'dır.

(DPT, 2000)

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (1)

- Ulusal bilgi güvenliği kavramı, bu çalışmada incelenen ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumlarına paralel olarak sadece kamu bilgi sistemlerinin değil, aynı zamanda özel sektöre ait kritik bilgi altyapıları da dâhil olmak üzere daha geniş bir çerçevede ele alınmalıdır.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (2)

- Bilgi güvenliği kültürünün toplumun tüm kesimlerinde yaygınlaştırılması ve içselleştirilebilmesi için ilköğretimden başlayarak bilgi teknolojileri derslerinde ele alınması gereken bir konu olması gerektiği değerlendirilmelidir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (3)

- Siber suçla mücadelede özellikle yeni suç türlerinin ortaya çıkmasının bir sonucu olarak,
  - Suç tasnifi ve tiplerinin yasal çerçeveye alınmasından
  - Bu suçlarla ilgili delil tespiti ve değerlendirmesine uzanan geniş bir yelpazede ceza ve usul kanunlarında bir takım yetersizlikler göze çarpmaktadır.
- Gerekli düzenlemelerin yapılması gerekmektedir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (4)

- Ulusal kalkınma ve yaşam tarzını sürdürülebilir kılmada bilgi sistemlerinin hayati önem taşıdığı hesaba katılmalı,
- Değişen teknolojiler ve incelenen ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumları da dikkate alınarak
  - esnek,
  - güncellenebilir,
  - değişen şartlara uyarlanabilir bir stratejik yaklaşım geliştirilmelidir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (5)

- Bilgi güvenliğini hem kamu kurumları hem de özel sektör bir kültür olarak görmeli ve bu alanda gerekli farkındalık artırıcı faaliyetler desteklenmelidir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (6)

- Bu çalışma kapsamında ele alınan ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumları dikkatle incelendiğinde ülkemizde de kamu ve özel kesimdeki tüm paydaşları kapsayan bir ulusal bilgi güvenliği stratejisi oluşturulabilir ve hayata geçirilebilir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (7)

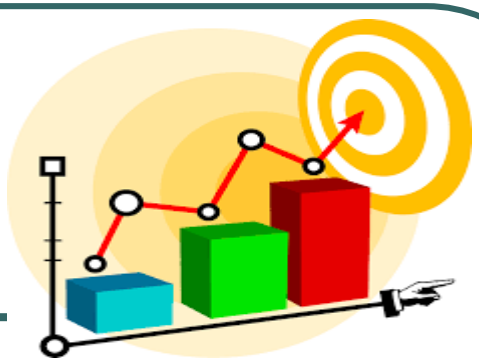
- Bu çalışma kapsamında incelenen ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumları göz önünde bulundurularak,
  - Ülkemizin jeopolitik ve jeostratejik koşullarına uygun, güçlü bir yasal altyapı ve yapılanma modeli ile kurgulanması gerekmektedir.
  - Başbakanlıkla ilişkili bir özerk yapının kurulmasının uygun olacağı değerlendirilmektedir.

Ulusal Bilgi Güvenliği Politikalarının Geliştirilmesi Üzerine Getirilebilecek Çözüm Önerileri (8)

- Ulusal Siber Güvenlik Stratejisi, kalkınma hedefleri doğrultusunda tekrar gözden geçirilmelidir.
- Ulusal bilgi güvenliği politikasındaki stratejik öncelikler tespit edilmelidir.

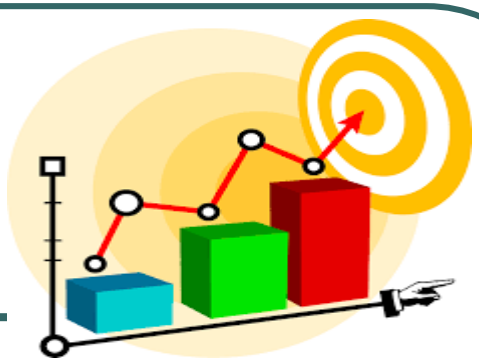
Sonuçlar ve Öneriler

Sonuçlar (1)



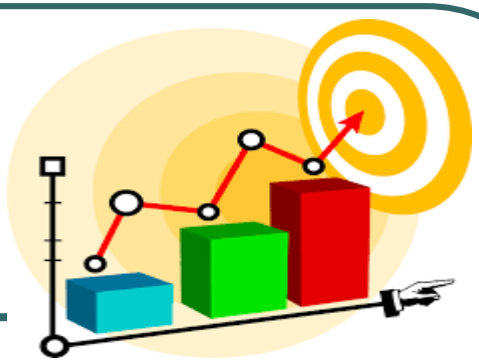
- Ülkemizde ulusal bilgi güvenliği alanında ciddi bir takım eksiklikler göze çarpmaktadır.
- Öncelikle bilgi güvenliğinin kültürü ülkemizde arzu edilen düzeyde gelişmemiştir.
- Ulusal bilgi güvenliğinin sağlanabilmesi için kurumsal yapılanma ve ilgili mevzuat oldukça sık gündeme gelmesine rağmen kalkınma ile ilişkisinin kurulduğu bir ulusal strateji metni henüz bulunmamaktadır.

Sonuçlar (2)



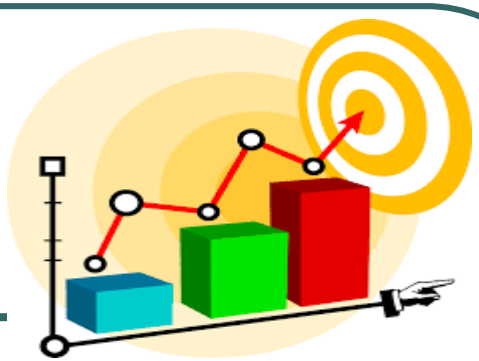
- “Ulusal Siber Güvenlik Stratejisi çalışmaları” kapsam açısından daha dar kalmakta ve ulusal kalkınma hedefleri ile ilişki net bir biçimde kurulamamaktadır.

Sonuçlar (3)



- Ulusal Bilişim Güvenliği Kanun Tasarısı Taslağı,
- Siber Suç Sözleşmesinin Uygun Bulunmasına İlişkin Kanun gibi ulusal bilgi güvenliğini sağlam bir yasal altyapıya kavuşturacak mevzuat çalışmaları henüz tamamlanamamıştır.

Sonuçlar (4)



- Kritik altyapıların korunması ile ilgili, incelenen ülkelerde olduğu gibi, ulusal ölçekte bir strateji ve eylem planı bulunmamaktadır.
- Bu noktada ülkemizde hem özel sektör tarafından işletilen kritik bilgi altyapılarını hem de kamu bilgi sistemlerini koordine edebilecek yetkiye sahip bir kurum bulunmamaktadır.

Öneriler (1)

- Ulusal bilgi güvenliği kavramı, bu çalışmada incelenen ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumlarına paralel olarak,
  - sadece kamu bilgi sistemlerinin değil,
  - aynı zamanda özel sektöre ait kritik bilgi altyapıları da dâhil olmak üzere daha geniş bir çerçevede ele alınabilir.

Öneriler (2)

- Bilgi güvenliği kültürünün toplumun tüm kesimlerinde yaygınlaştırılması ve içselleştirilebilmesi için ilköğretimden başlayarak bilgi teknolojileri derslerinde ele alınması gereken bir konu olması gerektiği değerlendirilmelidir.

Öneriler (3)

- Ulusal kalkınma ve yaşam tarzını sürdürülebilir kılmada bilgi sistemlerinin hayati önem taşıdığı hesaba katılarak, değişen teknolojiler ve incelenen ülkelerin ulusal bilgi güvenliği politikaları, stratejileri ve kurumsal yapılanma durumları da dikkate alınarak
  - esnek,
  - güncellenebilir,
  - değişen şartlara uyarlanabilir

  bir stratejik yaklaşım geliştirilebilir.

Öneriler (4)

- Bilgi güvenliğini hem kamu kurumları hem de özel sektör bir kültür olarak görmeli ve bu alanda gerekli farkındalık artırıcı faaliyetler desteklenmelidir.

Öneriler (5)

- Stratejik yönetim ile kurumsal bilgi güvenliği süreçleri arasında ilişki kurulabilir ve bilgi güvenliği yönetişimi süreçleri kamu kurumlarında zorunlu hale getirilebilir.

Öneriler (6)

- Kamu ve özel kesimdeki tüm paydaşları kapsayan bir ulusal bilgi güvenliği stratejisi oluşturulabilir ve hayata geçirilebilir.

Öneriler (7)

- Siber Güvenlik Kurulunun yapısı ve işlevi değiştirilebilir, sadece kamu kurumlarının temsilcilerine verilen kararlara katılım yetki ve sorumluluğu, kamu sektöründe ve özel sektörde faaliyet gösteren kritik altyapı işletmecilerine de tanınabilir.

Öneriler (8)

- Hazırlık çalışmaları devam etmekte olan Ulusal Siber Güvenlik Stratejisi, kalkınma hedefleri doğrultusunda tekrar gözden geçirilebilir.
- Ulusal bilgi güvenliği politikasındaki stratejik öncelikler tespit edilebilir.

Öneriler (9)

- Ulusal Bilişim Güvenliği Kanun Tasarısı Taslağı,
- Siber Suç Sözleşmesinin Uygun Bulunmasına İlişkin Kanun gibi ulusal bilgi güvenliğini sağlam bir yasal altyapıya kavuşturacak mevzuat çalışmaları tamamlanabilir.

Teşekkürler…