Academic Journal of History and Idea Академическая История и Мысль
Akademik Tarih ve Düşünce Dergisi
ISSN: 2148-2292
Araştırma Makalesi https://doi.org/10.46868/atdd.14 *Original Article*

Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi

Elvin Abdurahmanlı*
ORCID-0000-0002-0629-8317

Öz

‘‘Siber İstihbarat Kapsamında Echelon İstihbarat Sistemi’’ isimli bu makalede ilk olarak istihbarat kavramının ne olduğu ve istihbaratın geçmişten günümüze kadarki tarihine kısaca değinilmiştir. İlaveten de istihbarat kurumlarının milli hedeflerine göre 9 türünden biri olan siber istihbarat türü bu makalede ilk başlıkta incelenmiştir. Bugün herkesin sosyal hayatına gelişen teknolojinin ne derecede etkilediği ve ister bilgisayarımızda, isterse de özel görüşmelerimizde şahsi verilerimizin güvenliği ne derecede güvenli olduğu sorusuna ‘‘siber güvenlik’’ başlığı altında cevap aranmıştır. Echelon istihbarat sistemi başlığı altında Echelon istihbarat sisteminin içeriğinden ve bu sistemin soğuk savaş döneminde yapıldığı belge ve referanslarla ortaya konulmuştur. İlk kuruluş aşamasında Echelon istihbarat sistemine üye olan devletler ve günümüzde bu sisteme erişimi olan devletlerin listesi verilmiştir. Makalenin son kısmında Echelon istihbarat sisteminin yasa dışı olduğuna dair açılan soruşturma sonrası Avrupa Parlamentosunun 2001 raporuyla yasallaştırması süreci ortaya konulmuştur. Makalede esasen Echelon istihbarat sisteminin izinsiz olarak ülkelerde tüm e-postaların incelendiği ve konuşmaların dinlendiği ortaya çıkması ve Avrupa İnsan Hakları Sözleşmesini ihlal edilmesine rağmen Avrupa Parlamentosunun 2001 raporunda bu sistem olumlu referanslar alarak yasal görülmesi sürecine de yer verilmektedir.

Anahtar Kelimeler: Siber İstihbarat, Echelon, Hack, Açık Kaynak, Kapalı Kaynak,

JEL Kodları: F5, K33, N4, K24

Gönderme Tarihi: 30/06/2020 **Kabul Tarihi:29/05/2021**

* *İstihbarat İncelemeri ve Diplomasi Uzmanı, Doktora Öğrencisi, Azerbaycan Cumhuriyeti Diaspora Bakanlığı Karabağ Azerbaijan Milli Platformu Türkiye Cumhuriyeti Genel Koordinatörü, İstanbul- Türkiye, abdurahmanlielvin@gmail.com*

Bu makaleyi şu şekilde kaynak gösterebilirsiniz:
ABDURAHMANLI, E., ‘‘Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi’’, *Akademik Tarih ve Düşünce Dergisi*, C. 8, S. 3, 2021, s.1212-1234.

Within the scope of Cyber Intelligence: Echelon Intelligence System

Elvin Abdurahmanli*
ORCID-0000-0002-0629-8317

Abstract

In this article that named 'Within the scope of cyber intelligence' Echelon intelligence system " , What is the concept of intelligence and the history of intelligence from the past to the present is briefly mentioned. In addition, the type of cyber intelligence, which is one of 9 types according to the national goals of intelligence agencies, is examined in the first title in this article. The question of affection of developing technology in everyone's social life today and the question of the security of our personal data, whether on our computer or in our private conversations, has been sought under the heading 'cyber security'. Echelon under the title intelligence system Echelon intelligence system from the content of the Echelon intelligence system and this system is put forward with documents and references that made the system during the Cold War period . A list of states that were members of the Echelon intelligence system at the first establishment stage and states that have access to this system today is given. In the last part of the article, the process of legalization of the European Parliament's 2001 report after the investigation that the Echelon intelligence system was illegal was laid out. The article also includes the fact that the Echelon intelligence system was found to be unauthorized in countries where all emails were examined and conversations were listened to, and despite the violation of the European Convention on human rights, the European Parliament's 2001 report made this system legal, receiving positive references.

Keywords: Cyber Intelligence, Echelon, hacking, Open source, Closed source

JEL Codes: F5, K33, N4, K24

Received Date: 30/06/2020 **Accepted Date: 29/05/2021**

*Intelligence Investigators and Diplomacy Specialist, PhD student, Republic of Azerbaijan Ministry of Diaspora Karabakh Azerbaijan National Platform General Coordinator of the Republic of Turkey, Istanbul-Turkey, abdurahmanlielvin@gmail.com

You can refer to this article as follows:
ABDURAHMANLI, E.,''Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi'', *Academic Journal of History and Idea*, Vol. 8, Issue 3, 2021, p.1212-1234.

В рамках кибербразведни: разведывательная система Echelon

Элвин Абдурахманлы*
ORCİD-0000-0002-0629-8317

Резюме

В этой статье, названной «Интеллектуальная система Echelon в рамках «Кибербразведки», во-первых, кратко упоминается, что такое понятие интеллекта, и история интеллекта от прошлого до настоящего. Кроме того, тип кибербразведки, который является одним из 9 типов разведывательных учреждений в соответствии с их национальными целями, был рассмотрен в рамках первого заголовка в этой статье. Ответ на вопрос о том, в какой степени развивающиеся технологии влияют на социальную жизнь каждого человека сегодня и насколько безопасна безопасность наших личных данных, будь то на нашем компьютере или в наших личных беседах - был найден в разделе "Кибербезопасность". Разведывательная система Echelon под заголовком Echelon раскрывается по содержанию разведывательной системы, а также с документами и ссылками, сделанными во время холодной войны.На первом этапе создания приведен список государств, которые являются участниками разведывательной системы Echelon и государств, которые и сегодня имеют доступ к этой системе.В последней части статьи рассказывается о процессе легализации разведывательной системы Echelon с отчетом Европейского парламента за 2001 год после расследования, которое было признано незаконным. В статье также описан процесс легализации этой системы путем принятия положительных отзывов в отчете Европейского парламента 2001 года.Несмотря на то, что разведывательная система Echelon выявила, что, без разрешения в странах все электронные письма были проверены, а речи прослушивались, и Европейская конвенция о правах человека была нарушена.

Ключевые слова: кибербразведка, Echelon, Hack-взлом, открытый исходный код, закрытый исходный код.

Коды *JEL*: F5, K33, N4, K24

Получено: 30/06/2020 **Принято: 29/05/2021**

*Следователи разведки и специалист по дипломатии, Аспирант, Азербайджанская Республика Министерство Диаспоры Карабах Азербайджанская Национальная Платформа Генеральный Координатор Турецкой Республики, Стамбул-Турция, abdurahmanlielvin@gmail.com

Ссылка на статью:
ABDURAHMANLI, E.,‘’Siber İstihbarat Kapsamında: Echelon İstihbarat Sistemi’’, *академическая история и мысль*, T.8, NO.3, 2021, C.1212-1234.

Giriş

Uluslararası sistemde mevcut olan her bir ülke iç güvenliğini muhafaza etmesi gerekmektedir. Bunun için devletler iç ve dış düşmanlardan korumak amacıyla askeri birliklerin yanı sıra istihbarat kurumları mevcuttur. İstihbarat kurumları genel olarak her devlette aynı amaca yönelik olsa da yapı ve şematik olarak farklılık teşkil etmektedir. Ham bilgi istihbarat kurumları tarafından iki yöntem vasıtasıyla elde edilmektedir. Bu yöntemler genelde kapalı kaynaklardan elde edilen bilgiler ve açık kaynaklardan toplanmaktadır. İstihbaratın milli hedeflerine göre dokuz türü mevcuttur. Bunlar:[1]

**Askeri İstihbarat.*

**Biyografik İstihbarat.*

**Ekonomik İstihbarat.*

**Bilimsel ve Teknolojik İstihbarat.*

**Ulaşım ve İletişim İstihbaratı.*

**Coğrafya İstihbaratı.*

**Siyasi İstihbarat.*

**Sosyolojik İstihbarat.*

**Siber istihbarat.*

1-İstihbarat Kavramı Nedir

Kelime itibariyle Türk Dil Kurumu istihbarat kavramı yeni bir bilgi edinmek olarak gösterilmiştir.[2]İstihbarat kelimesi İngilizce'de ''intelligence'' olarak tanımlanmaktadır. Bu kelime bilgi, güncel haberler elde edinme olarak bilinmektedir. İstihbarat kavramı genel itibariyle devletin kurumlarının topladığı verilerin ve bilgilerin saf hale getirilerek ülkeye yönelik olan herhangi bir tehdidi belirlemesi ve bu tehdidi önlenmesidir.[3] İstihbaratçı Michael Herman, istihbarat kavramına farklı bakış açısı getirerek açıklığa kavuşturmuştur. İstihbarat denilen kavram bir veya birkaç kaynaktan aldığın verileri süzgeçten geçirerek gerçek bilgi

[1] Ümit Özdağ, *İstihbarat Teorisi*, Kripto yayınları, Ankara 2016, s.19-150.
2 Kelime ''İstihbarat'' https://sozluk.gov.tr/?kelime= www.tdk.gov.tr, (27.08.2018).
3 Ü. Özdağ., *a.g.e.*, s.19-150.

hale getirilmesi olarak belirtmiştir.[4] Köken olarak Arapçadan alınan ‘‘istihbar’’ sözcüğü Türkçe’mizde haber alma, bilgi edinme olarak anlam ifade etmektedir. Fakat istihbarat kavramı kendi bünyesinde anlamı ve kavramı itibariyle haber almanın ötesinde olan bir kavram niteliğini taşımaktadır. Örneğin, Günlük hayatımızda radyo, televizyon, internet ortamı veya gazetelerden elde ettiğimiz bilgi ve haberlerle istihbarat kurumlarının elde ettiği bilgiler büyük bir farklılık oluşturmaktadır.[5] İstihbarat kurumlarında kurum çalışanları tarafından elde edinilen haber ve kaynaklar istihbarat çarkının analiz aşamalarından geçirilerek saf bilgi ve kaynağa ulaşılmaktadır. İstihbarat faaliyetleri insanların yeni bilgiler edinerek kendilerinin güvene alma isteği sonucu ortaya çıkmıştır. Bu düşünceden yola çıkarak istihbarat kavram olarak insanların birbirleriyle yazılı ve sözlü olarak iletişimin ortaya çıkma aşamasından günümüze dek halen süren bir kavramdır diyebiliriz. Diğer bir örnek ise, şahıs veya şahıslarla ilgili bilgi edinmesinin kendisi de adeta istihbarat toplama yöntemlerinden biridir sadece. Devletlerin en önemli kurumu Milli İstihbarat Teşkilatlarıdır ve devletin geleceğinin devamı açısında yaşam kurumu veya devletin uzun yıllar ayakta kalmasını sağlayan kurum niteliğini taşımaktadır. İlaveten istihbarat kurumu olmayan yahut zayıf istihbarı bilgi edinen bir devlet yaşam sürekliliğinin kaybetme aşamasına gelmekle yükümlüdür ve böyle bir devletin ayakta kalması zordur.[6] Yukarıda gösterildiği gibi genel itibariyle elde edinilen istihbarı bilgi ve belgeler 2 yöntemle elde edilmektedir. Bu yöntemler: açık kaynaklardan elde edinilen bilgiler ve kapalı kaynaklardan elde edinilen bilgiler olarak şekillenmektedir. Açık kaynak yöntemi denilen bu bilgi toplama yöntemi, gazete, televizyon, radyo, akademik makaleler, sosyal medya gibi platformlardan edinilen istihbarı bilgilerden oluşmaktadır. Kapalı kaynaklı istihbarı bilgi toplama yöntemi genelde herhangi devlet kurumu çalışanı tarafında elde edinilen gizli belge veya verilerden oluşmaktadır. İstihbarı bilgi edinemeden taktiksel hareket eden herhangi bir istihbarat servisi gözü kapalı şekilde hedefe doğru ilerleyerek ateş açması gibidir. Elde edinilen bilgiler biz insanlarda olan bu beş duygu özelliğine benzemektedir.[7]

4 Michael Herman, *Intelligence Power in Peace and War*, Cambridge University Press, Cambridge 1999, s. 10-28.

5 Elvin Abdurahmanlı, *‘’İstihbarat Teşkilatlarının Terör Örgütlerine Sızması–İra’’,* Yüksek Lisans Tezi, İstanbul 2019, s. 30-33.

6Yavuz Özalp, ‘’Siber İstihbarat ve Güvenlik Politikaları’’, 2015, Wordpress.com: https://derinstrateji.files.wordpress.com/2015/01/siber-stihbarat-ve-gvenlik-politikalar, (11.01.2018).

7 Yusuf Çağlayan, *Sosyolojik Savaş*, Timaş Yayınları, İstanbul 2016, s. 220-230.

1.1 Siber İstihbarat

Günümüzde teknolojinin hayatımıza girmesiyle ortaya çıkan Siber istihbarat kavramı son 25 yıl içinde bir nevi sosyal dünyamıza dâhil olarak uluslararası bir boyuta ulaşmıştır. Yukarıda belirttiğim gibi Siber istihbarat teknolojik cihazların kullanımı vasıtasıyla yapılan istihbarat türüdür. Siber istihbaratta teknoloji kullanarak herhangi bir şifre sel işlemleri kırmak veya herhangi bir kurumun alt yapısını çökertmeye "hack" kelimesiyle betimlenmektedir. Kelime itibariyle hak bilgisayar teknolojisiyle herhangi bir devletin önemli kurumlarını çökertmeye yönelik yapılan bir operasyon türüdür. Birçok yöntem vasıtasıyla belirlenen hedefe virüs yazılımlı bilgiler yollayarak o kurumun sistem bilgilerini elde edile bilinir veya o kurumu çökertme imkânına sahip yazılımlar mevcuttur. İnternet tarayıcılarında dolaştığımız her an veya sanal âlem dediğimiz sosyal medya hesaplarımıza gelen bildiriler veya mesajlaşma siteleri virüse açık bir alan olduğunu belirtmekte fayda vardır. Bugünün teknolojisi çağında yaşadığımızı kabul etmeliyiz. Bu sebepten dolayı kişisel verilerimizin hepsini neredeyse güvende tutmak kolay değildir. Her gün teknoloji gelişmeye devam ediyor ve güvenliğimiz neredeyse tehlikeli bir duruma gelmektedir. Örneğin: Facebook, Twitter, İnstagram, Gmail, Yandex gibi sosyal haberleşme ağlarını kullandığımız zaman kendi bilgilerimizi bir nevi istihbarat servislerine hediye etmiş oluyoruz. Nasıl mı? Mesela: Facebook, Twitter, İnstagram gibi sosyal ağlarda hangi kitap sevdiğinizi, hangi mekânlara gitmeyi üstünlük verdiğinizi, günlük duygularınızı, hangi tür elbise veya araba sevdiğinizi, kimin sayfasını daha çok sıklıkla takip ettiğinizi bu gibi bilgileri bu sosyal ağlarla paylaştığınız için sizin hakkınızda kısa sürede bir biyografik istihbarat elde edinile bilinir.

1.2 Siber Güvenlik

Uluslararası sistemde mevcut olan devletler kendi gizli verilerini korumak için siber güvenlik isimli güvenlik sistemleri kurarak riskleri önlemeye ve ortadan kaldırmaya çalışmaktadırlar. Siber Güvenlik konusunda üst düzey Siber Güvenlik yapısıyla İsrail devleti diğer devletlerarasında birinci yeri almaktadır. Genel olarak yüksek düzeyde ''hacker'' konferans ve seminerleri İsrail'de düzenleniyor. Örneğin: 2017 yılının Eylül ayının 24-ünde yapılacak olan parlamento seçimleri ile ilgili Almanya'da oluşa bilecek herhangi bir siber saldırıların ve dezenformasyon kampanyalarının karşısının alınması için Almanya Federal İstihbarat Dairesi (BND) birkaç ay önceden Siber saldırılardan korunmak genç hackerlerden oluşan bir birim kurdu. Bu birime genç hackerlerin işe almak için kısa seçim esnasında gençlere kısa dönemli bir eğitim programı uygulamıştır. Almanya Federal İstihbarat Dairesi olan BND'nin gerçek misyonu, Almanya federal hükümetine yapılacak herhangi operasyonel, taktik veya siber saldırılar hakkında önceden istihbarı bilgi edinmek Almanya Federatif

devletinin çıkarlarını korumayı hedeflemektedir. BND'nin misyonlarından biri, devletin herhangi kurumana yönelik yapılacak olan potansiyel casusluk faaliyetleri hakkında önceden ön bilgi edinme ve elde edilen bilgini değerlendirerek ve yapılacak olan casusluk faaliyetlerini en aza indirmek veya da yok etmektir.

Şekil 1:(https://www.dw.com/en/how-germanys-foreign-intelligence-agency-recruits-young-hackers/a-38056408, 2017).[8]

İngiltere istihbarat kurumu olan Mİ5 ajanlarından olan Andrew Parker bu kurumun Siber saldırılarla ilgili kurumun genel müdürlüğünü yapmaktadır. Andrew Parker Siber tehditler ve Siber istihbarat ile ilgili şu kelimeleri ifade etmiştir:[9]

''Benim adım Andrew Parker ve MI5'in Genel Müdürüyüm. 30 yıldır buradayım ve işe alımın gizli ve özel olarak yapıldığı zamanda katıldım. Hayat şimdi büyük ölçüde ilerledi. MI5'in bugünlerde uğraştığı tehditler, uluslararası terörle mücadele, Kuzey İrlanda terörizminden, karşı-proliferasyonlardan arınmak, kitle imha silahlarının yayılmasını durdurmaktır. İlaveten de kurumumuzun görevi yabancı devletler tarafından casusluk ve siber saldırı tehditleriyle ilgili önlemler almaktır. Bunların tehditlerin hepsini dört gözle beklediğimiz gibi değişen tehditlerdir.''

[8] https://www.dw.com/en/how-germanys-foreign-intelligence-agency-recruits-young-hackers/a-38056408, (09.15. 2019).
[9] Mİ5Careers, Transcripts: ami5.gov.uk/careers/working-at-mi5-video-transcripts (10.09. 2019).

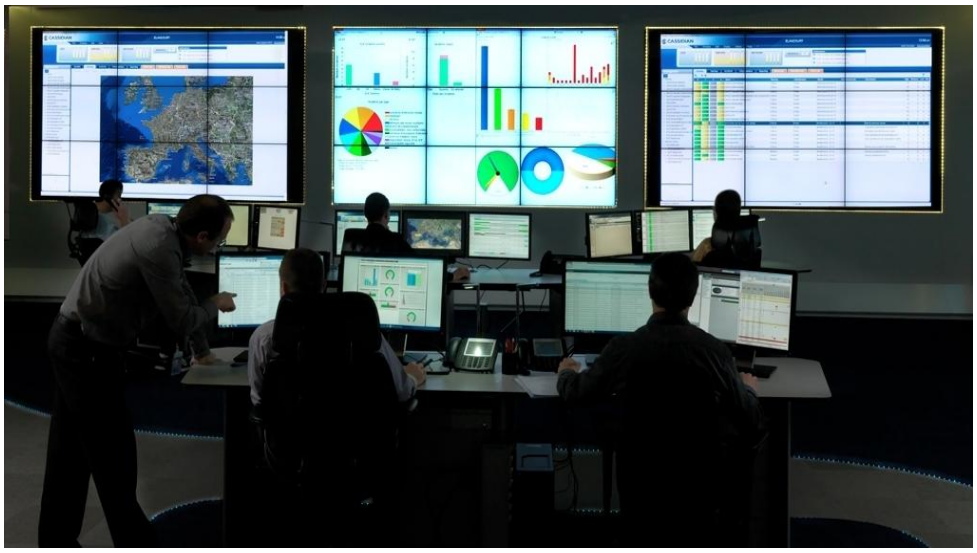
Şekil 2: Cyber intelligence mi5
Kaynak:(ami5.gov.uk/careers/working-at-mi5-video-transcripts, 2019).[10]

Uluslararası bir güç olan Amerika Birleşik Devletleri'ne mahsus Siber istihbarat ilgili birçok özel şirketler ABD sınırları içinde ve Afrika kıtasında mevcuttur. Bu özel kuruluşlar genelde şirketlere veya şahıslara SİBER İstihbarat alanında aşağıdaki bu gibi deneyimleri sunmaktadırlar. Bunlar:

* *Gelişmiş Güvenlik İşlemleri.*
* *Penetrasyon testi.*
* *Kimlik ve Erişim Yönetimi.*
* *Dolandırıcılık Önleme.*

Bu gibi şirketlerden biri de Amerika Birleşik Devletleri'ne mahsus SİBER İstihbarat kapsamında faaliyet gösteren özel şirketlerden biri CIA Botsvana (Pty) LTD kuruluşudur.

10 Mİ5Careers, Transcripts: ami5.gov.uk/careers/working-at-mi5-video-transcripts (10.09. 2019).



Şekil 3:(Cyber İntelligence Agency- https://www.ciabotswana.com/contact, 2019).[11]

Amerika Birleşik Devletleri'ne ait yazılımlardan biri de Microsoft yazılımlarıdır. Bu yazılımları Çin, Almanya ve Fransa gibi devletler kendi kurumlarında kullanılmasını yasak etmiştir. Bu yazılımın yerine özel yazılımlar geliştirmiş yazılımları devlet kurumlarında kullanmaktadırlar. Örneğin: Bir işletim sistemi olan Linux, Çin devleti tarafından geliştirilmiş halde kendi resmî kurumlarında kullanılmaktadır. Bu yöntem vasıtasıyla devlet kurumlarının iç ve dış saldırılardan korunmasına yardımcı olmaktadır. Ekonomik açıdan dikkat edilirse, Çin Cumhuriyeti Microsoft yazılımlarının yıllık kullanımı için Amerika Birleşik Devletleri'ne ödeme yapmak zorunda kalmamakla birlikte ilaveten de ülkenin teknolojik ve ekonomik açıdan gelişmesine sebep olmaktadır. Günümüzde Siber güvenlik son derece önemli olduğu için üniversitelerde Siber güvenlik alanında Rusya, ABD gibi ülkelerin üniversitelerin bünyesinde bölümler açılmıştır.

Siber istihbarat Alanında Rusya Federasyonu'nun iç istihbarat kurumu olan Rusya Federal Güvenlik Servisi (FSB) Siber istihbaratı eğitimi kapsamında kendi bünyesinde bulunan Rusya Federasyonu Güvenlik Servisi Akademisinde Lisans eğitimi vermektedir. Mevzubahis olan lisans eğitimi Rusya Federasyonu Güvenlik Servisi Akademisinde iki fakülteden oluşmaktadır. Bunlar:[12]

**Bilgisayar Güvenliği.*

**Otomatik Sistemlerin Bilgi Güvenliği.*

**Bilgi Güvenliği Uzmanı.*

Bu alanda fakülte uzmanları öğrencileri uzmanlık alanına hazırlar.

11 https://www.ciabotswana.com/contact/ (10.09. 2019).
12 http://www.academy.fsb.ru/i_faculty_ib.html (10.09. 2019).

Şekil 4:''Федера́льная слу́жба безопа́сности'' olan Türkçe karşılığı Rusya Federal Güvenlik Servisi FSB'nin günümüzdeki Amblemi
Kaynak: (Федера́льная слу́жба безопа́сности- http://www.fsb.ru/fsb/history.htm, 2018).[13]

Günümüzde halen İran ile ilgili nükleer tartışmalar devam etmektedir. Birkaç yıl önce İran'ın nükleer tesislerinin elektronik ağına siber saldırılar yapılmıştır. Bu saldırılar İsrail'in Hacker grupları tarafından yapıldığı ortaya çıkmıştır. Siber saldırılar sonucu Nükleer tesislerin alt yapılarını büyük derecede zarar görmüştür.[14] İstihbarat kurumları genelde kendi bünyesinde oluşturduğu Hackerler birimi vasıtasıyla cep telefonları belleğinde veya bilgisayardaki verileri deşifre ederek elde ettikleri veya telefon konuşmalarını dinledikleri bilinmektedir. Siber istihbaratta bilgi toplamada birçok program mevcuttur. Bunlardan en önemli olan Echelon isimli dinleme programıdır. Siber istihbarat sistemi olan Echelon programı hakkında daha geniş Echelon istihbarat sistemi başlık altında verilmiştir.

1.3 Echelon İstihbarat Sistemi

1960 yılında Rusya'ya iltica eden iki NSA ajanı olmuştur. Bu şahıslar Bernon Mitchell ve William Martin isimli şahıslardır. Bu şahıslar1960 yılının 6 Eylül tarihinde başkent Moskova'da düzenlenen konferansta konuşmuşlardır. Konuşma esnasında Amerika Birleşik

[13] http://www.fsb.ru/fsb/history.htm (25.10.2018).
14 Çağlar Gün, *''Ulusal Güvenlik Politikalarının Belirlenmesinde İstihbarat ın Rolü ve Önemi''*, Yüksek Lisans Tezi, Ankara 2014, s. 77-85.

Devletleri tarafından NSA ajansına özel bir dinleme sisteminin hazırlanması talimatı verilmiştir. Mevzubahis dinleme sistemi Echelon sistemidir. Bu sistemin ana amacı hedef ülkenin telefon konuşmalarını ve telgrafları, uydu sinyallerini belirlemeye yönelik olmuştur. İlaveten de bu sistem vasıtasıyla İngiltere ABD istihbarat servisleri kendi aralarında bilgi alışverişini sağlamaya başlamıştır. İngiltere, ABD istihbarat servislerinin iş birliğine diğer bir örnek ise, 2. Dünya savaşı zamanı Alman şifreli iletişim makinesi olan Enigma'nın şifresi deşifre edilerek İngiliz'ler tarafında ABD istihbarat servislerine bildirilmiştir. Bu şifreyi deşifre eden ise Alan Turing ve ekibi olmuştur. İlaveten de ABD istihbarat servisi ise Japonların gizli askeri haberleşme şifrelerini deşifre ederek İngilizlere vermişlerdir.[15]

Şekil 5: Intelsat Atlantik ve Hint Okyanusu bölgesi uydularını yakalayan ilk Echelon istasyonu: Bude, Cornwal. Covername: Carboy Kaynak:(http://www.duncancampbell.org/content/nsa-yes-there-echelon-system, 2019).[16]

ABD, 1999 yılına kadar Echelon sisteminin mevcudiyetini kabul etmemiştir; fakat 1999 yılının 23 Mayıs tarihinde Martin Brady bu programın mevcudiyetini belirtti. Martin Brady isimli şahıs dönemin Avustralya, Canberra'daki Savunma Sinyalleri Müdürlüğü (DSD) Başkanlığı görevini yürütmüştür. Fakat bu program gerçekte 50 yıldan fazla bir zamandır mevcut olmuştur. Sistemi ilk kuruluş aşamasından sonra iki devlet kullanmaktaydı. Bu iki devlet: ABD ve İngiltere olmuştur. Kısa bir zaman sonra sistem 3 yeni üyenin katılımıyla beş üyeden oluştu: ABD, İngiltere, Avustralya, Yeni Zelanda ve Kanada. Echelon sistemi 15 yıl

[15] N.Aydın, ''*İstihbarat, Ajan ve Dinleme''*, https://antalyabugun.com/tr/makale/istihbarat-ajan-ve-dinleme-22528.html (16.09.2019).

16 http://www.duncancampbell.org/content/nsa-yes-there-echelon-system (16.09.2019).

içinde NSA tarafından geliştirilmiş ve nano teknolojik sistemlerden oluşturulmuştur. ABD ve İngiltere'nin müttefik olduğu ülkelerde bu sistemin üsleri mevcuttur.[17]

Echelon sisteminin kuruluş zamanındaki öncelikli amacı ülke dâhili, ülke harici telefon dinlemelerini yapmak ve telgraf şifrelerini deşifre etmek idi. Program zaman geçtikçe teknolojik şartlara uygunlaştırılarak geliştirilmiştir. Mevzubahis olan gelişimlerden biri de bu sisteme filtreleme sisteminin ilave edilmesi olmuştur. Filtreleme sistemi genelde kelime ve sözlük bazında yapılmaktaydı. Bu filtreleme sistemi herhangi bir yazlı veya iletinin içeriğinin ne olduğunu deşifre etme ve inceleme gibi kabiliyete sahipti. İlaveten de şahıslar arası konuşulan her türlü görüşme gelecekte o şahsin aleyhinde kullanılması için ilave bir dosya halinde kanıt olarak kaydediliyordu. Gerekli olduğu halde o kayıt bellekten bulunarak kullanılıyordu.[18]

2013 yılı eski NSA ajanı Edward Snowden'in NSA dünyayı dinliyor açıklamasıyla ABD'nin sırlarını ifşa ettikten sonra Amerika Birleşik Devletleri'nin eski Başkanı Barack Obama 2013 yılı aralık ayı açıklamasında bu kelimeleri ifade etmiştir:
Evet dinliyoruz fakat sizlerin düşüncenizin aksine NSA tarafından elde edilen bilgiler insanların şahsi hayatlarını güvenceye almamız için olmuştur her zaman ve özel hayat mahremiyetine dokunulmamıştır.

Edward Snowden, NSA bu başarısını hiç zaman bildirmediği ve gizlemeye çalıştığını söyledi. İlaveten de insanların ister özel iş görüşmelerini dinlemek isterse de e-postalarını denetlemekle NSA çalışanları bu iletileri hiçbir zaman kötü amaçla iş dışında kullanmamışlardır kelimesini kullandı.[19] Barack Obama 2014 yılının 17 Ocak tarihinde NSA Kurumunun reforma gidileceğini duyurdu. Barack Obama 2014 yılının ocak ayında Almanya'nın ZDF adlı televizyon kanalına verdiği röportaj zamanı verilen bir soru ve Başkan Barack Obama'nın verdiği cevap çok ilginç olmuştur. Sorunun içeriği kısaca böyledir:
Sunucu:

"Türkiye Başbakanı Recep Tayyip Erdoğan'ın telefon konuşmaları dinleniyor mu?

Barack Obama:

17https://www.turkishnews.com/tr/content/2017/03/31/teknik-takip-dosyasi-dev-istihbarat -kulagi-gizli-echelon-projesi-echelon-usleri-ve-yeni-d-unya-duzeni/ (31.03.2017).
[18]Yavuz Özalp, Siber İstihbarat ve Güvenlik Politikaları, Wordpress.com: https://derinstrateji.files.wordpress.com/2015/01/siber-stihbarat-ve-gvenlik-politikalar.pdf (11.01.2018).
[19]Stephen Crowley, Obama's Speech on N.S.A. Phone Surveillance, The New York Times: https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html (14. 08.2019).

"Bu konu ve soru üzerine tartışmak istemiyorum çünkü uluslararası arenada olup bitenleri dergi ve makalelerden takip etmek yetseydi o zaman istihbarat servislerini devletler kapatırdı''[20]

Şekil 6: Eski ABD Başkanı Barak Obama, Beyaz Saray'da, Almanya'da yayın yapan ZDF televizyonuna konuştu – 2014. Kaynak:(http://www.milliyet.com.tr/dunya/obama-ya-sordu-erdogan-i-dinliyor-musunuz-1824477, 2014).

Bu cevaptan da anlaşıldığı gibi her bir istihbarat servisi potansiyel olarak rakip bildiği devlet başkanlarının konuşmalarını dinlemektedirler. Çizelge 1'de hangi ülkelerin istihbarat kurumlarını Echelon sisteminden kullandığı verilmiştir. Echelon sistemini kullanan sadece ABD veya İngiltere gibi devletlerle sınırlı olmadığı görülmektedir.

Country	**Communications ı foreign countries**	**State nunications**	**Civilian communications**
Belgium			
Germany			
Denmark			
Finland			
Greece			
Italy			
France			

[20] Milliyet Gazetesi, Obama'ya sordu: Erdoğan'ı dinliyor musunuz?:http://www.milliyet.com.tr/dunya/obama-ya-sordu-erdogan-i-dinliyor-musunuz-1824477 (08.14.2019).

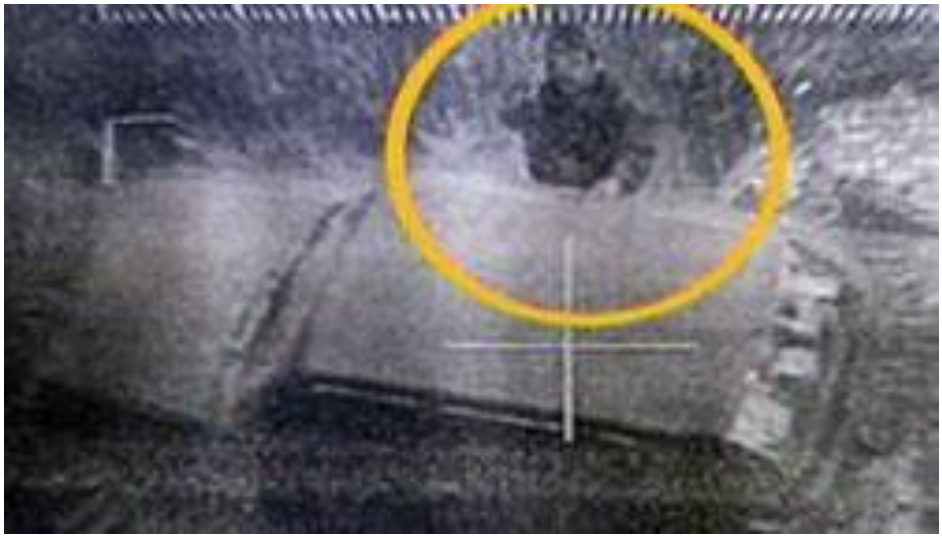
Australia			
Portugal			
USA			
New Zealand			
Canada			
Netherlands			
UK			
Spain			
Austria			
Luxembourg			
Ireland			
Sweden			

Çizelge 1: "Echelon sistemini kullanan devletler[22]

ABD Devletleri'nin Ulusal Güvenlik Teşkilatı olan NSA'nın eski personeli WAYNE Madsen verdiği demeçte Echelon sistemi hakkında önemli bilgiler vermiştir. NSA ajanı Wayne Madsen, Echelon sisteminin iki âdetininse Türkiye Cumhuriyeti sınırları dâhilinde yerleştiğini söylemiştir. Türkiye yerleşen bu sistemler vasıtasıyla Rusya, İran, Irak ve Kafkasya'da yerleşen devletlerin görüşmelerini dinlemek amacıyla kullanıldığını belirtmiştir[21]. Farklı kaynaklarda ise Türkiye Cumhuriyeti sınırları dâhilinde 9 adet Echelon sistemi olduğu belirtilmektedir ve bunlar İstanbul, Sinop, Diyarbakır Edirne, Adana, Ağrı, İzmir, Kars, Antalya'da yerleşmektedir.[22] Kıbrıs Cumhuriyeti'nde1960 yılında kurulan ve İngiltere'ye ait olan 2 adet Dekelya ve Akrotiri isimli askeri üssü mevcuttur. Bu askeri üslerde Echelon sistemi mevcuttur.[23] Eski NSA ajanı Wayne Madsen'nın PKK terör örgütü başçısı olan Abdullah Öcalan'ın yakalanması için Echelon sistemi kullanıldığını belirtti. Dönemin ABD başkanı Bill Clinton, Rusya ile arayı iyi tutmak maksadıyla Echelon sistemini kullandırarak Çeçenistan başkanı Cahar Dudayev'in mevcut konumunu tespit ettirmiş ve Moskova'ya resmi ziyareti zamanı dönemin Rusya başkanı Boris Yeltsin'e koordinatları

[22] http://www.duncancampbell.org/menu/surveillance/echelon/EU_resolution.pdf (2001).
[21] Ali Kuzu, ''*MIT, MOSSAD, CIA, GLADIO'',* Kariyer Yayıncılık, İstanbul 2015, s.146-147.
[22] *Gazete 2023,* Echelon ve Teknolojik İstihbarat:.http://www.gazete2023.com/echelon-ve-teknolojik-istihbarat-makale,228.html (18.03.2019).
[23]Stelyo Berberakis, *BBC News*, Avrupa Komisyonu, Brexit müzakerelerinde Kıbrıs'taki İngiliz üsleri de masada olsun: https://www.bbc.com/turkce/haberler-dunya-39481699 (16.09.2019).

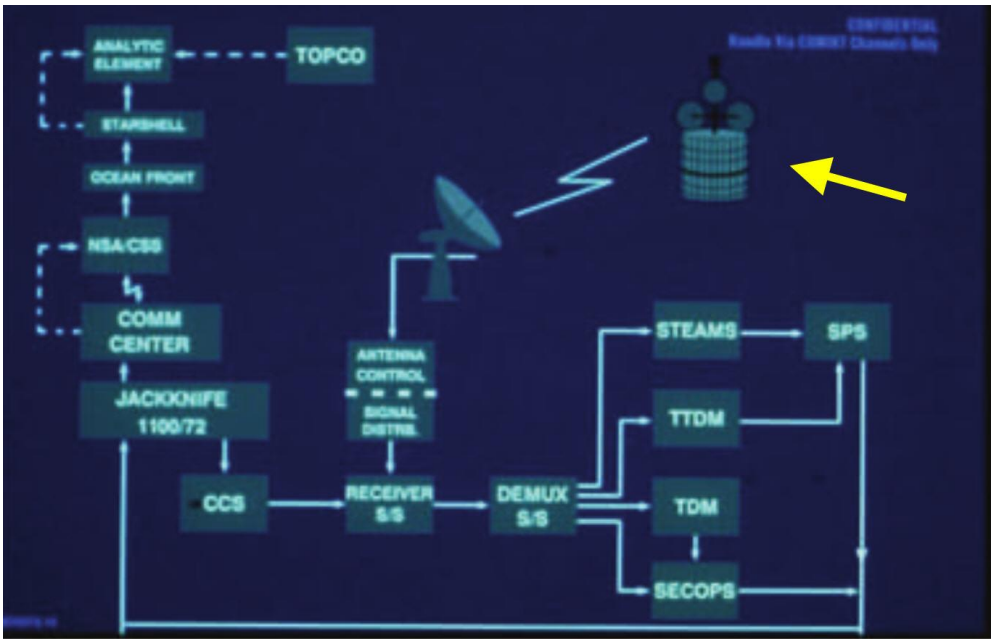
vermiştir. Elde edilen koordinatlar sonrası 1996 yılının 20 Nisan tarihinde Rusya istihbarat servisi olan KGB istihbaratı kurumu tarafından Çeçenistan lideri Cahar Dudayev'i Gekhi-Chu köyü yakınlarında infaz edilmiştir.[24]



Şekil 7: Cahar Dudaye'vin vurulma anı.
Kaynak:(Şehid Çeçen Lider Dudayev'in Son Görüntüsü, 2007).[25]

Diğer bir iddiaya göre ise o dönemin Başbakanı Necmettin Erbakan'ın Dudayev'e hediye verdiği Amerikan üretimi olan uydu telefonun içine yerleştirilmiş dinleme cihazına Echelon sisteminin erişim vasıtasıyla konumu Çeçen Liderin konumunun belirlendiği söylenmektedir.[26] Uydu telefonu Sperry Marine Satellite SP 4100 marka model idi. Hat ise Dubai'den özel olarak alınmıştır. Telefonda bir cipin olmasından Necmettin Erbakan'ın hiçbir bilgisi yoktu. İlaveten de bu infazla ilgili MİT'in bir ilişkisinin olmadığı belirtildi. Ajan Wayne Madsen, NSA'nın "Echelon' sisteminden başka bir sistemin daha geliştirdiğini ve bu sistemin uluslararası boyutta bir bilgi edinile bilir bir sistem kabiliyetine sahip olduğunu, sistemin isminin ''Signet'' olduğunu belirtti. İlaveten de bu sistemin Echelon' sisteminden daha fazla veri üretme kapasitesine sahip olduğunu, program dâhilinde uluslararası 66 dil ve her dilin şive farklılıklarına göre şive kapasitesi olduğunu ifade etti.[27]

[24] Mesut Uyar, Çeçenistan: Siyasi ve Askerî Kısırdöngü, *Güvenlik Stratejileri Dergisi, S.* 28, İstanbul 2018, s.288-295.
[25] http://www.tevhidhaber.com/sehid-cecen-lider-dudayevin-son-goruntusufoto-video-8487h.htm (09.30.2019).
[26]http://www.gazetevatan.com/efsane-lideri-erbakan-in-telefonundan-vurmuslar--372402-dunya/ (09.29.2019).
[27] A. Kuzu, *a.g.e., s.146*-147.



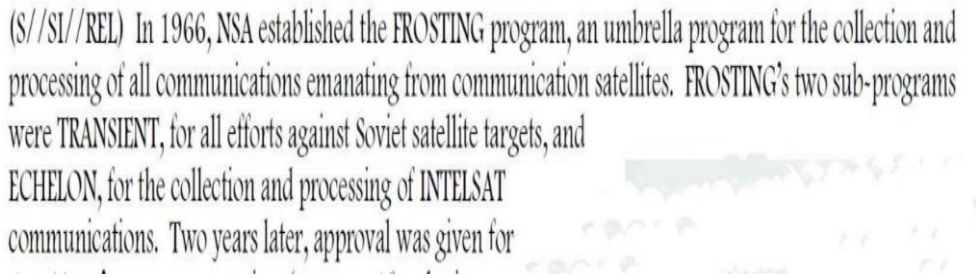
Şekil 8:NSA'nın Yakima Araştırma İstasyonu için Echelon sistem diyagramı.
*Kaynak:**(http://www.duncancampbell.org/content/nsa-yes-there-echelon-system, 2019)***

Şekil 8'de Uydu Intelsat IV vasıtasıyla elde edilen veriler Jackknife'nin Univac 1100/72 bilgisayar işlemcisinden geçerek NSA'ya aktarılmaktadır. Şekil 9'da ikinci Seattle yakınlarındaki Yakima'daki Echelon istasyonunu gösterilmiştir. Bu istasyon 4 Mayıs 1973 yılının 4 Mayıs tarihinde faaliyetine başlasa da Ekim 1974 yılında operasyon-el olarak kullanılmaya başlanmıştır.[28] NSA tarafından Yakima'daki Echelon istasyonu vasıtasıyla Starburst ve Oceanfront adlı iletişim ağları kullanılmak suretiyle tüm bilgiler "Terminal Operasyon Kontrolü" olarak ele alınmış ve tüm veriler bir merkezinden idare edilmeye başlanılmıştır.[29]

[28] http://www.duncancampbell.org/menu/surveillance/echelon/EU_resolution.pdf (2001).
[29] http://cryptome.org/jya/echelon-dc.htm, http://cryptome.org/jya/echelon-dc.htm (16.09.2019).

***Şekil 9:Intelsat Pasifik Okyanusu bölgesi uydusuna müdahale eden ikinci Echelon istasyonu: Yakima, Washington Covername: Jackknıfe.*Kaynak:(http://www.duncancampbell.org/content/nsa-yes-there-echelon-system, 2019).**

Dokümanlara baktığımız zaman ilk kez Echelon sisteminden 1966 yılında Frosting adıyla bilinen büyük bir stratejik programın bir parçası olduğunu ortaya koymaktadır. Transient adlı Frosting'in programı esasen Sovyet Sosyalist Cumhuriyetler Birliği'nin yeni Molniya ‘‘молния veya "Lightning" isimleriyle bilinen haberleşme alanında kullanılan sistem uydularını hedef almaktaydı ve bu sistem gerek askeri gerekse de devlet dâhilindeki haberleşmeleri dinlemek için kullanılıyordu.


(S//SI//REL) In 1966, NSA established the FROSTING program, an umbrella program for the collection and processing of all communications emanating from communication satellites. FROSTING's two sub-programs were TRANSIENT, for all efforts against Soviet satellite targets, and ECHELON, for the collection and processing of INTELSAT communications. Two years later, approval was given for

Şekil 10:(http://www.duncancampbell.org/content/nsa-yes-there-echelon-system, 2019).


yes, there is an ECHELON system,

***Şekil 11: (http://www.duncancampbell.org/content/nsa-yes-there-echelon-system, 2019)*.**

EUROPEAN PARLIAMENT

1999 *2004*

Session document

FINAL
A5-0264/2001
PAR1

11 July 2001

REPORT

on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))

Part 1: Motion for a resolution
Explanatory statement

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

RR\445698EN.doc PE 305.391

Şekil 12: (Temporary Committee on the ECHELON Interception System, 2001).

rights, for which reason the idea was rejected by a majority of Members of the European Parliament.

1.5. Working method and schedule

With a view to carrying out its mandate in full, the committee decided to proceed in the following way. A programme of work proposed by the rapporteur and adopted by the committee listed the following relevant topics: 1. Certain knowledge about ECHELON, 2. Debate by national parliaments and governments, 3. Intelligence services and their operations, 4. Communications systems and the scope for intercepting them, 5. Encryption, 6. Industrial espionage, 7. Aims of espionage and protective measures, 8. Legal context and protection of privacy and 9. Implications for the EU's external relations. The topics were considered consecutively at the individual meetings, the order of consideration being based on practical grounds and thus not implying anything about the value assigned to the individual topics. By way of preparation for the meetings, the rapporteur systematically scrutinised and evaluated the material available. At the meetings, in accordance with the requirements of the topic concerned, representatives of national administrations (particularly secret services) and parliaments in their capacity as bodies responsible for monitoring secret services were invited to attend, as were legal experts and experts in the fields of communications and interception technology, business security and encryption technology with both academic and practical backgrounds. Journalists who had investigated this field were also heard. The meetings were generally held in public, although some sessions were also held behind closed doors where this was felt to be advisable in the interests of obtaining information. In addition, the chairman of the committee and the rapporteur visited London and Paris together to meet people who for a wide variety of different reasons were unable to attend meetings of the committee but whose involvement in the committee's work nonetheless seemed advisable. For the same reasons, the committee's bureau, the coordinators and the rapporteur travelled to the USA. The rapporteur also held many one-to-one talks, in some cases in confidence.

1.6. Characteristics ascribed to the ECHELON system

The system known as 'ECHELON' is an interception system which differs from other intelligence systems in that it possesses two features which make it quite unusual:

The first such feature attributed to it is the capacity to carry out quasi-total surveillance. Satellite receiver stations and spy satellites in particular are alleged to give it the ability to intercept any telephone, fax, Internet or e-mail message sent by any individual and thus to inspect its contents.

The second unusual feature of ECHELON is said to be that the system operates worldwide on the basis of cooperation proportionate to their capabilities among several states (the UK, the USA, Canada, Australia and New Zealand), giving it an added value in comparison to national systems: the states participating in ECHELON (UKUSA states[9]) can place their interception systems at each other's disposal, share the cost and make joint use of the resulting information. This type of international cooperation is essential in particular for the worldwide interception of satellite communications, since only in this way is it possible to ensure in international communications that both sides of a dialogue can be intercepted. It is clear that, in view of its

[9] See Chapter 5, 5.4.

RR\445698EN.doc 23/194 PE 305.391

Şekil 13:(Temporary Committee on the ECHELON Interception System, 2001).[30]

Elde edilen belgelere esasen Echelon sisteminin soğuk savaş döneminde kurulduğu ortaya çıkmıştır. Kanada devletinin ‘‘The Canada's Communications Security Establishment

[30] http://www.duncancampbell.org/menu/surveillance/echelon/EU_resolution.pdf (08.14.2019).

(CSE) intelligence agency'' adlı istihbarat kurumunun eski ajanlarından biri Mike Frost Echelon sistemi hakkında Şubat 2000 yılında bir belgeyi rapor halinde sunmuştur. Echelon sisteminin veri toplamasının ileri derecede olduğunu ve yüksek potansiyele sahip sistem olduğunu söyledi. Amerika Birleşik Devletleri tarafından Avrupa İnsan Hakları Sözleşmesini ihlal edildiği gerekçesiyle 2000 yılında, Avrupa Parlamentosu bu sistemi araştırmak için özel üyelerden oluşan bir inceleme kurulu kurdu.[31] 2000-2001 yılları arasında Avrupa Parlamentosunda Echelon sistemiyle ilgili soruşturma açılmıştır. Avrupa Parlamentosu'nun 11 Haziran 2001 raporunda Echelon sistemi hakkında referanslar verilmiştir. Bu raporda sistemin ABD kontrolü altında olduğu belirtilmiş ve NSA istihbarat servisi tarafından idare edildiği belirtilmiştir. Ayrıca raporda üye ülkelerin isimleri de yer almıştır.[32] NSA kurumu tarafından yapılan açıklamada bu sistemin mevcudiyetini gerçek olduğu söylenildi. Rapor olumlu çıksa da 2005 yılında dönemin ABD başkanı Bush tarafından izinsiz olarak ülkedeki tüm epostaların incelendiği ve konuşmaların dinlendiği ortaya çıkmıştır. Bu programı kullanma yetkisi olan diğer ülkelerinde bu programı kullanarak konuşmaların dinlendiği ve epostaların içeriğini elde ettiğine işaret etmekteydi.[33]

[31] Lucas Matney, *Uncovering ECHELON, The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life*: https://techcrunch.com/2015/08/03/uncovering-echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/ (09.16.2019).

[32] http://www.duncancampbell.org/menu/surveillance/echelon/EU_resolution.pdf (08.14.2019).

[33] L. Matney, *a.g.e., s.*1-5.

Sonuç

Siber istihbarat Kapsamında Echelon istihbarat sistemi isimli makalede Siber istihbaratın öneminin yüksek olduğu ve Echelon istihbarat sistemi bir nevi siber istihbaratta bir başlangıç olmuştur. Siber İstihbarat türü başlık altında incelenmiş ve geçmişten günümüze kadar Siber İstihbarat türü hakkında bilgi verilmiştir. Siber istihbarat ilk kullanıldığı yıllarda halen günümüzde teknolojik şartlara uygunlaşarak gelişmiştir. Gelişen bu teknolojiyle birlikte Siber istihbaratın önemi artmış ve sosyal hayatımıza etki ederek güvenliğimizi tehdit altına koyduğu sonucuna varılmıştır. Siber Güvenlik başlığı altında küresel sistemde mevcut devletlerin gerekse istihbarat kurumları gerekse de özel güvenlik kurumları Siber güvenlik alanında ilerleme kaydetmiş ve şahsi verilerimizi korumaya yönelik sistemler üretmeye yöneldikleri görülmüştür. Almanya Rusya, İngiltere gibi ülkelerde siber güvenlik alanında üniversitelerde ve devlet kurumlarında eğitimlerin verildiği görülmektedir. Echelon istihbarat sistemi başlığı kapsamında ise Echelon istihbarat sisteminin soğuk savaş döneminde ortaya çıktığı ve uzun yıllar bu sistemin gizli tutulduğu görülmektedir. İlaveten de bu dinleme sisteminin ulusal güçler tarafından bir nevi tehdit nitelikli kullanıldığı, ülkelerin ve insanların Avrupa İnsan Hakları Sözleşmesinde belirtildiği maddeleri yok sayarak insan hakları ihlal edildiği ve yok sayıldığı sonucuna varılmıştır.

Kaynaklar

ABDURAHMANLI, E., *"İstihbarat Teşkilatlarının Terör Örgütlerine Sızması: İra"*, Yüksek Lisans Tezi, İstanbul 2019.

AVCI, G., İstihbarat Teknikleri, Timaş yayınları, İstanbul 2004.

AYDIN, N., İstihbarat , Ajan ve Dinleme: https://antalyabugun.com/tr/makale/istihbarat-ajan-ve-dinleme-22528.html (16.09.2019).

ÇAĞLAYAN, Y., *Sosyolojik Savaş*, Timaş Yayınları, İstanbul 2016.

ÇİMEN, A., *İstihbarat Dünyasının Perde Arkası*, Timaş Yayınları, İstanbul 2002.

CAMPBELL, D., Somebody's listening. Cryptome:http://cryptome.org/jya/Echelon-dc.htm (16.09.2019).

CAMPBELL, D., http://www.duncancampbell.org/content/nsa-yes-there-Echelon-system. NSA: "yes, there is an Echelon system" : http://www.duncancampbell.org/content/nsa-yes-there-Echelon-system (16.09.2019).

GÜN, Ç., *"Ulusal Güvenlik Politikalarının Belirlenmesinde İstihbarat ın Rolü ve Önemi"*, Yüksek Lisans Tezi, Ankara 2014.

HERMAN, M., Intelligence Power in Peace and War. Cambridge: Cambridge University Press. www.cambridge.org/core/boos/intelligence-power-in-peace-war/39B13810C2D49FD2894827D9BA373CCB (27.08.2018).

KUZU, A., MIT, MOSSAD, CIA, Gladıo, Kariyer Yayıncılık, İstanbul 2015.

MATNEY, L., Uncovering Echelon: The Top-Secret NSA/GCHQ Program That Has Been Watching You Your Entire Life. https://techcrunch.com/2015/08/03/uncovering-Echelon-the-top-secret-nsa-program-that-has-been-watching-you-your-entire-life/ (16.09.2019).

UYAR, M., "Çeçenistan: Siyasi ve Askerî Kısırdöngü", Güvenlik Stratejileri Dergisi, S. 28, İstanbul 2018, s.288-295.

ÖZTÜRK, M., Gazete 2023. Echelon ve teknolojik istihbarat: http://www.gazete2023.com/Echelon-ve-teknolojik-istihbarat-makale,228.html(16.09.2019).

ÖZALP,Y., Siber İstihbarat ve Güvenlik Politikaları, Wordpress.com:https://derinstrateji.files.wordpress.com/2015/01/siber-stihbarat-ve-gvenlik-politikalar.pdf (11.01.2018).

ÖZDAĞ, Ü., İstihbarat Teorisi, Kripto yayınları, Ankara 2016.

NERGİS, S., "Time Türk, tarihinde Dudayev'e o telefonu kim götürdü", https://www.timeturk.com/tr/2014/10/15/dudayev-e-o-telefonu-kim-goturdu.html (30.09.2019).

BERBERAKİS, S., "BBC News, Avrupa Komisyonu: Brexit müzakerelerinde Kıbrıs'taki İngiliz üsleri de masada olsun", https://www.bbc.com/turkce/haberler-dunya-39481699 (30.09.2019).

https://www.ciabotswana.com/contact/: https://www.ciabotswana.com/contact/ (10.09.2019).

http://www.duncancampbell.org/menu/surveillance/Echelon/EU_resolution.pdf (10.09.2019).

http://www.duncancampbell.org/menu/surveillance/Echelon/EU_resolution.pdf (14.08.2019).

http://www.fsb.ru/fsb/history.htm (25.10.2018).

https://www.turkishnews.com/tr/content/2016/02/16/istihbarat -dosyasi-istihbari-tesekkuller-ve-terimler/ (13.09.2019).

https://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html (14.08.2019).

Mİ5Careers: ami5.gov.uk/careers/working-at-mi5-video-transcripts (10.09.2019).

http://www.milliyet.com.tr/dunya/obama-ya-sordu-erdogan-i-dinliyor-musunuz-1824477 (18.09.2019).

http://www.academy.fsb.ru/i_faculty_ib.html (08.03.2020).

www.tdk.gov.tr. www.tdk.gov.tr: www.tdk.gov.tr (27.08.2018).

http://www.tevhidhaber.com/sehid-cecen-lider-dudayevin-son-goruntusufoto-video-8487h.htm (10.09.2019).

https://www.turkishnews.com/tr/content/2017/03/31/teknik-takip-dosyasi-dev-istihbarat -kulagi-gizli-Echelon-projesi-Echelon-usleri-ve-yeni-d-unya-duzeni/ (10.09.2019).

http://www.gazetevatan.com/efsane-lideri-erbakan-in-telefonundan-vurmuslar--372402-dunya/ (29.09.2019).

https://www.dw.com/en/how-germanys-foreign-intelligence-agency-recruits-young-hackers/a-38056408 (15.09.2019).