Akademik Tarih ve Düşünce Dergisi *Academic Journal of History and Idea*

Araştırma Makalesi | Research Article
Geliş tarihi |Received:01.10.2023
Kabul tarihi |Accepted:30.09.2025
Yayın tarihi |Published:25.10.2025

Elvin Abdurahmanlı

https://orcid.org/0000-0002-0629-8317
Dr., General Coordinator of the Republic of Türkiye of the KİAMP – Karabakh is Azerbaijan National Platform, established by the Azerbaijani Ministry of Diaspora / President of the Karabakh is Azerbaijan Coordinating Association. Intelligence and Counter-Terrorism Expert, Azerbaijan, abdurahmanlielvin@gmail.com

Atıf Künyesi | Citation Info

Abdurahmanlı, E. (2025). A Cyber Intelligence Perspective: An Analysis of the Echelon Intelligence System. *Akademik Tarih ve Düşünce Dergisi*, *12* (5), 567-584.

A Cyber Intelligence Perspective: An Analysis of the Echelon Intelligence System

Abstract

This study analyzes the Echelon Intelligence System from a cyber intelligence perspective, exploring its historical background, structure, and implications for global cybersecurity. The research outlines the evolution of intelligence practices, emphasizing the rise of cyber intelligence as a critical component within national security frameworks. It investigates how advancing technology has reshaped social life and raised concerns regarding data privacy and digital surveillance. The Echelon system, established during the Cold War, is examined through official documents revealing its operational scope and member states. The study also discusses the European Parliament's 2001 report, which acknowledged the system's existence despite its controversial legality and potential violations of the European Convention on Human Rights. Overall, the article underscores the growing importance of cyber intelligence in international security and the balance between technological advancement and individual privacy.

Keywords: *Cyber Intelligence, Echelon, Cybersecurity, Surveillance, National Security, Intelligence Systems, Information Warfare*

Siber İstihbarat Perspektifinden: Echelon İstihbarat Sistemine Analitik Bir Bakış

Öz

Bu çalışma, Echelon İstihbarat Sistemini siber istihbarat perspektifinden inceleyerek, sistemin tarihsel arka planını, yapısal özelliklerini ve küresel siber güvenlik üzerindeki etkilerini analiz etmektedir. Araştırmada, istihbarat uygulamalarının tarihsel gelişimi ele alınmış ve siber istihbaratın ulusal güvenlik yapılanmalarında giderek daha kritik bir unsur haline geldiği vurgulanmıştır. Gelişen teknolojinin toplumsal yaşamı nasıl dönüştürdüğü, veri gizliliği ve dijital gözetim bağlamında ortaya çıkan endişeler tartışılmıştır. Soğuk Savaş döneminde kurulan Echelon sistemi, resmi belgeler aracılığıyla yapısı, işleyiş kapsamı ve üye devletler açısından değerlendirilmiştir. Ayrıca, sistemin tartışmalı yasal statüsüne rağmen varlığını kabul eden ve Avrupa İnsan Hakları Sözleşmesi'nin ihlal edilme ihtimaline dikkat çeken 2001 tarihli Avrupa Parlamentosu raporu da analiz edilmiştir. Genel olarak makale, siber istihbaratın uluslararası güvenlikte artan önemini ve teknolojik ilerleme ile bireysel mahremiyet arasındaki dengeyi vurgulamaktadır.

Anahtar Kelimeler: *Siber İstihbarat, Echelon, Siber Güvenlik, Gözetim, Ulusal Güvenlik, İstihbarat Sistemleri, Bilgi Savaşı*

Introduction

Every state operating within the international system holds the responsibility of ensuring its internal security. In this regard, intelligence agencies and military units function to safeguard the nation from both internal and external threats. Although the fundamental objectives of intelligence agencies are similar across different states, their organizational structures and operational mechanisms vary significantly. The raw data collected by intelligence institutions are typically gathered from both open and classified sources. In accordance with national security goals, intelligence activities are generally classified under nine main categories (Özdağ, 2016):

- Military Intelligence
- Biographical Intelligence
- Economic Intelligence
- Sociological Intelligence
- Cyber Intelligence
- The Concept of Intelligence
- Scientific and Technological Intelligence
- Transportation and Communication Intelligence
- Geographical Intelligence
- Political Intelligence

The Concept of Intelligence: Its Objectives and Purpose

The Turkish Language Association (TDK) defines the term *intelligence* as "acquiring new information" (Özdağ, 2016). Although the English equivalent *intelligence* is generally understood as the process of obtaining information or news, the concept extends far beyond this narrow definition. It encompasses a process in which collected data are analyzed, verified, and utilized to identify and prevent potential threats. Intelligence expert Michael Herman (1999) provides a broader perspective, defining intelligence as the systematic filtering and transformation of data gathered from multiple sources into meaningful and reliable information.

Although of Arabic origin, the Turkish term *istihbarat*—meaning "information gathering"—represents more than mere acquisition of news. A substantial difference exists between information obtained through ordinary media tools such as television, radio, or newspapers, and the data collected by professional intelligence organizations (Herman, 1999). The data acquired by intelligence agencies undergo an analytical procedure known as the

"intelligence cycle," through which raw information is refined into actionable intelligence. These processes, rooted in humankind's innate need for knowledge and security, have become indispensable components of modern state systems (Herman, 1999).

The Continuity of Intelligence and Its Institutional Importance

Since the inception of written and oral communication, the collection and evaluation of information have formed the foundation of intelligence activity. Information gathered about an individual or group constitutes only one dimension of intelligence; in essence, intelligence collection is a multidimensional and historically continuous process. Within state structures, the central institution responsible for intelligence is typically a nationally organized agency—such as the National Intelligence Organization. These agencies serve as vital mechanisms ensuring state continuity and enabling strategic decision-making for future security. Conversely, a weak or neglected intelligence infrastructure threatens national stability and long-term sovereignty (Özalp, 2015).

Methods of Information Gathering: Open and Classified Sources

Intelligence information is generally obtained through two principal channels: open sources and classified sources. Open-source intelligence (OSINT) encompasses publicly accessible materials such as newspapers, academic publications, radio, television, and social media. Although OSINT provides broad access to data, it requires verification and in-depth analysis to ensure reliability. Classified or covert intelligence, in contrast, is derived from restricted materials—such as confidential government documents, institutional reports, or information obtained from authorized personnel. Neglecting the role of information acquisition in strategic decision-making is tantamount to advancing blindly toward a goal, thereby exposing oneself to grave risks. Hence, accurate and verified information forms the foundation of all intelligence operations (Çağlayan, 2016).

The Emergence and Characteristics of Cyber Intelligence

As technology has become an integral aspect of modern life, cyber intelligence has emerged over the last twenty-five years as a domain of increasing international significance. Cyber intelligence involves collecting and analyzing information through digital technologies. Malicious cyber activities—commonly termed *hacking*—include operations aimed at damaging systems, stealing data, or disrupting institutional functions. Malware such as viruses, trojans, and ransomware can infiltrate systems covertly to exfiltrate data or seize digital control. Web browsers, messaging platforms, and social media networks present frequent security vulnerabilities. Accordingly, protecting personal and institutional data has become an

increasingly complex and essential task in today's digital landscape (Özalp, 2015). Everyday digital environments—such as Facebook, Twitter, Instagram, and search engines—serve as potential sources of intelligence data, as users' personal information may be monitored or exploited for strategic purposes. Uninformed or careless usage of these platforms allows data to be weaponized in intelligence operations. This reality underscores the necessity of robust cybersecurity measures for individuals and institutions alike (Özalp, 2015).

Social Media and Biographical Intelligence

Social media platforms such as Facebook, Twitter, and Instagram facilitate the creation of detailed biographical profiles. Data including users' locations, lifestyle habits, consumer preferences, and online interactions construct a comprehensive digital portrait—commonly referred to as biographical intelligence. Furthermore, modern technological infrastructures support extensive networks for eavesdropping and surveillance. One notable example is the *Echelon* intelligence system, developed collaboratively by the United States, United Kingdom, Canada, Australia, and New Zealand—often referred to as the "Five Eyes" or "Great Ear" alliance (Abdurahmanlı, 2016).

Cybersecurity

Within the international system, states develop comprehensive cybersecurity frameworks to protect classified information and to counter potential cyber threats. Israel, possessing one of the most advanced structures in this field, occupies a leading position globally. The country regularly organizes high-level hacker conferences and seminars aimed at fostering expertise and innovation in cybersecurity (Abdurahmanlı, 2016). A noteworthy example of proactive cybersecurity policy can be observed in Germany. Prior to the federal parliamentary elections held on September 24, 2017, the Federal Intelligence Service (*Bundesnachrichtendienst* – BND) established a specialized unit composed of young hackers to anticipate and prevent possible cyberattacks and disinformation campaigns. Short-term, intensive training programs were implemented to enhance the capabilities of this unit, and the selection of candidates was conducted through a rigorous process. The BND's primary mission is to gather advanced intelligence on operational, tactical, and cyber threats directed against the German federal government, thereby safeguarding Germany's national interests. Furthermore, detecting, assessing, and neutralizing potential espionage activities targeting governmental institutions constitute essential responsibilities within the agency's mandate (DW Akademie, 2017).

Figure 1. Germany's Federal Intelligence Service (BND) — Recruitment and Cyber Operations (DW News, 2017)

MI5 and Cyber Intelligence

Andrew Parker, Director General of Cyber Operations at the British intelligence agency MI5, underscores the evolving nature and growing diversity of cyber threats faced by the organization. In his public statements, Parker emphasizes that MI5 currently encounters an unprecedented range of challenges stemming from both state and non-state actors. Reflecting on his approximately thirty-year tenure within the agency, he recalls that recruitment practices in MI5's early years were characterized by strict confidentiality and limited public exposure. Today, however, Parker highlights a significant expansion in both the scale and complexity of intelligence threats.

According to Parker, MI5's principal areas of responsibility include countering international terrorism, preventing terrorist activity in Northern Ireland, and combating the proliferation of weapons of mass destruction. In addition, the agency bears responsibility for implementing protective measures against espionage operations and cyberattacks that may be orchestrated by foreign governments (MI5 Careers, 2019).

Figure 2. Cyber Intelligence and Digital Security — MI5 Careers (MI5 Careers, 2019).

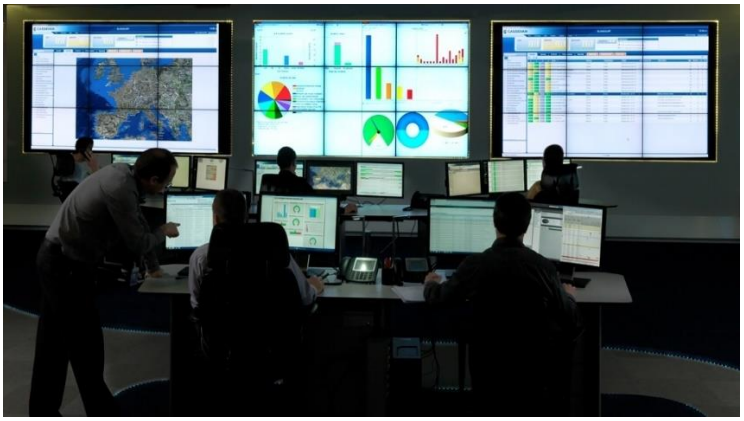
Private Cyber-Intelligence Enterprises

A considerable number of private companies specializing in U.S.-oriented cyber-intelligence operations function both within the United States and across the African continent. These entities deliver a wide range of specialized services to governmental institutions, private corporations, and individual clients. Their principal activities include advanced security operations, penetration testing, identity and access management, and fraud-prevention services. Among these organizations, *CIA Botswana (Pty) Ltd.* stands as a notable example of a private firm conducting cyber-intelligence activities with a strategic focus on U.S.-related operations (CIA Botswana (Pty) Ltd., 2019).

- **Advanced Security Operations:** Sophisticated activities designed to safeguard information systems against cyber threats through proactive monitoring and incident response.
- **Penetration Testing:** Controlled simulations of cyberattacks conducted to identify and mitigate vulnerabilities within digital infrastructures.
- **Identity and Access Management:** The deployment of processes and technologies to authenticate user identities and manage their access to critical resources.
- **Fraud Prevention:** The implementation of systematic measures and strategies to detect, deter, and prevent deceptive or exploitative practices targeting financial and data assets.

Figure 3. Cyber Intelligence Operations Center — CIA Botswana (CIA Botswana, 2019).

.



Cybersecurity Education and Technological Independence

Microsoft products—software originating from the United States—have been banned from official governmental use in several countries, including China, Germany, and France. These states prefer to utilize domestically developed proprietary software within their public institutions to enhance digital sovereignty and reduce dependence on foreign technologies. For instance, the Linux operating system, developed and implemented by the Chinese government for official use, exemplifies this approach. This strategy not only safeguards governmental

institutions from internal and external cyber threats but also enables China to avoid paying annual licensing fees for Microsoft software to the United States. Consequently, the policy fosters technological self-reliance while simultaneously supporting the nation's economic and technological advancement. Given the growing global emphasis on cybersecurity, several countries—most notably Russia and the United States—have established specialized cybersecurity departments within their universities. In particular, Russia's Federal Security Service (FSB) Academy offers undergraduate programs in the field of cyber intelligence. The academy includes three main departments:

- **Computer Security**
- **Information Security of Automated Systems**
- **Information Security Expertise**

Experts in these departments aim to equip students with comprehensive knowledge and practical skills necessary to operate effectively within the field of cyber intelligence and information security (Federal Security Service Academy [FSB Academy], 2019).

Figure 4. Emblem of the Russian Federal Security Service (FSB) / Федера́льная слу́жба безопа́сности (FSB, 2018).

Cyber Operations Targeting Iran

Negotiations concerning Iran's nuclear program continue to this day. Several years ago, extensive cyberattacks were carried out against Iran's nuclear facilities, reportedly by hacker groups affiliated with Israel. These cyber operations caused substantial damage to the infrastructure of Iran's nuclear sites and temporarily disrupted the country's nuclear development processes (Gün, 2014). Intelligence agencies typically obtain information by infiltrating the information systems of target states. Common methods include analyzing data stored in mobile devices, manipulating computer systems, and intercepting telecommunication networks. Within these agencies, specialized hacker units are often established to execute such operations. Numerous software programs and systems are employed for the purpose of cyber-intelligence collection; one of the most prominent examples is the Echelon surveillance system, which plays a major role in global cyber-intelligence operations (Gün, 2014).

The Echelon Intelligence System

In 1960, two agents from the United States National Security Agency (NSA), Bernon Mitchell and William Martin, defected to the Soviet Union. On September 6 of the same year, they publicly disclosed during a press conference in Moscow that the United States had tasked the NSA with developing a sophisticated electronic surveillance network, later known as Echelon. The system's primary objective was to detect and monitor telephone conversations, telegrams, and satellite communications belonging to target countries. Additionally, Echelon enabled systematic information exchange between the intelligence agencies of the United States and the United Kingdom (Aydın, 2016). A historical precedent for this cooperation can be found during World War II, when the British mathematician Alan Turing and his team successfully deciphered the German Enigma cipher machine. The intelligence derived from this breakthrough was shared with U.S. intelligence agencies, marking a milestone in transatlantic intelligence collaboration. Similarly, American intelligence services intercepted and decrypted Japan's secret military communication codes and subsequently transmitted this information to British intelligence (Aydın, 2016).

Figure 5. Intelsat — The First Echelon Station Capturing Atlantic and Indian Ocean Region Satellites (Bude, Cornwall; Covername: Carboy)(Duncan Campbell, 2019).

The Global Expansion of the Echelon System

The United States did not officially acknowledge the existence of the Echelon surveillance system until 1999. However, on May 23 of that year, Martin Brady, then Director of the Defense Signals Directorate (DSD) in Canberra, Australia, publicly confirmed the existence of the program. In reality, Echelon had already been operational for more than fifty years. Initially, the system was used exclusively by the United States and the United Kingdom but later expanded to include Australia, New Zealand, and Canada—forming a five-member alliance commonly known as the *Five Eyes* network. Developed over approximately fifteen years by the National Security Agency (NSA), the Echelon system was built using nanotechnological infrastructure and established its bases in countries allied with the United States and the United Kingdom (Turkish Forum Dünya Türkleri Birliği, 2017). At the time of its inception, the primary purpose of Echelon was to intercept domestic and international telephone communications and to decrypt telegraph codes. Over time, the system evolved alongside technological advancements, integrating a sophisticated keyword-based filtering mechanism. This system, utilizing algorithmic dictionaries, enables the automated analysis and interpretation of text and voice communications. Moreover, the system records and archives individual conversations, allowing such data to be retrieved and used for intelligence purposes when deemed necessary (Özalp, 2015). The 2013 revelations by former NSA contractor Edward Snowden brought the global scope of the NSA's surveillance activities into public view. In response, U.S. President Barack Obama acknowledged in December 2013 that the NSA conducted extensive global surveillance operations but asserted that such activities were aimed

at safeguarding citizens' security and did not infringe upon personal privacy. Snowden, however, claimed that the NSA intentionally concealed the scale of its operations and failed to disclose its successes to the public. He also emphasized that, according to his experience, NSA personnel did not exploit private data—such as emails or personal communications—for purposes beyond their official responsibilities (Crowley, 2014). On January 17, 2014, President Obama announced that the NSA would undergo a series of structural and procedural reforms. During an interview with Germany's ZDF television network in the same month, when questioned about whether Turkish Prime Minister Recep Tayyip Erdoğan's telephone conversations had been intercepted, Obama declined to comment directly, stating:

"I do not want to discuss this issue because if it were sufficient to follow international developments merely through magazines and articles, then states would simply shut down their intelligence agencies." (Milliyet Gazetesi, 2014)

Figure 6. Former U.S. President Barack Obama During an Interview with ZDF Television at the White House (2014) (Milliyet Newspaper, 2014).

As the aforementioned interview illustrates, intelligence agencies actively monitor the communications of heads of state and high-level officials in cases where political or security-related disputes may arise. This practice underscores the extensive scope and operational reach of international intelligence networks.

Table 1 presents the national intelligence agencies known to employ or collaborate within the framework of the Echelon system. As demonstrated in the table, the utilization of Echelon extends beyond the United States and the United Kingdom. The network also encompasses other allied states, reflecting a broader multilateral intelligence partnership that transcends bilateral cooperation. This structure highlights the strategic significance of information sharing and cyber coordination among member nations engaged in global surveillance activities.

Table 1. States Using the "Echelon" System (Duncan Campbell, 2001).

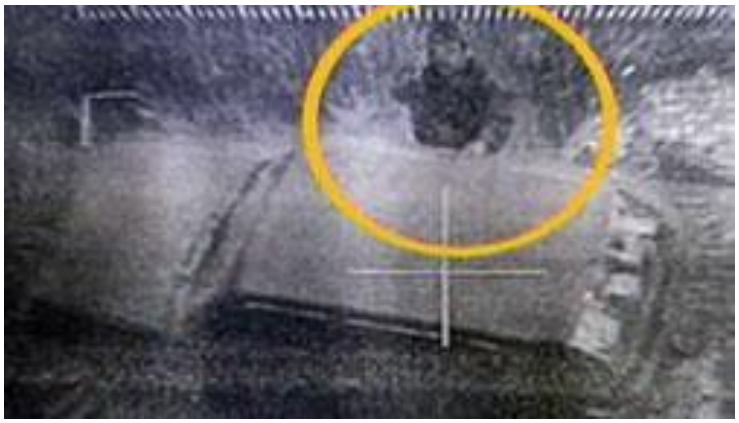
Country	Communications in foreign countries	State communications	Civilian communications
Belgium	+	+	-
Germany	+	+	+
Denmark	+	+	+
Finland	+	+	+
Greece	+	+	-
Italy	+	+	+
France	+	+	+
Australia	+	+	-
Portugal	+	+	-
USA	+	+	+
New Zealand	+	+	+
Canada	+	+	+
Netherlands	+	+	+
UK	+	+	+
Spain	+	+	+
Austria	+	+	-
Luxembourg	-	-	-
Ireland	-	-	-
Sweden	+	+	+

The Echelon System in Turkey and the Eastern Mediterranean

Former United States National Security Agency (NSA) employee Wayne Madsen has provided significant disclosures regarding the global deployment of the Echelon surveillance system. According to Madsen, two operational components of the Echelon network are located within the borders of Turkey. These installations are reportedly used to intercept and analyze communications originating from or directed toward states such as Russia, Iran, Iraq, and those situated in the Caucasus region (Kuzu, 2015). Complementary reports suggest that as many as nine Echelon facilities operate across various provinces in Turkey, including Istanbul, Sinop,

Diyarbakır, Edirne, Adana, Ağrı, İzmir, Kars, and Antalya (Öztürk, 2019). The system's presence in Turkey underscores its strategic role in regional intelligence operations, particularly in proximity to critical geopolitical zones.

Figure 7. The Moment of the Fatal Strike on Dzhokhar Dudayev (2007) (Tevhid Haber, 2019).



According to certain accounts, the location of Chechen leader Dzhokhar Dudayev was detected by the Echelon system through a listening device embedded in a Sperry Marine Satellite SP 4100 phone, reportedly gifted by then–Turkish Prime Minister Necmettin Erbakan. The satellite line, obtained from Dubai, was allegedly compromised by a concealed microchip unknown to Erbakan. Despite claims that CIA funds supported Turkish intelligence operations during this period, no direct connection has been established between the assassination and the National Intelligence Organization (MIT) (Tevhid Haber, 2019). Former NSA officer Wayne Madsen further indicated that, beyond Echelon, an additional global surveillance network known as Signet had been developed. This system possesses a superior data-processing capacity and accommodates 66 languages, including numerous dialectal variations (Kuzu, 2015; Nergis, 2014).

Figure 8. ECHELON System Diagram for NSA's Yakima Research Station (Duncan Campbell, 2019).

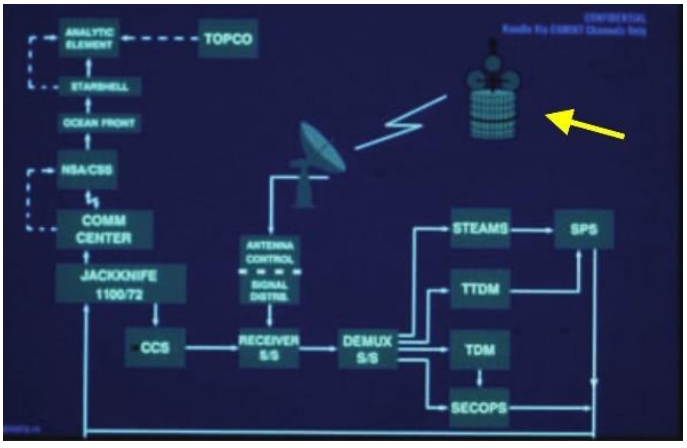


Figure 8 illustrates that the data obtained via the Satellite Intelsat IV were transmitted to the NSA through the Jackknife system's Univac 1100/72 computer processor. Figure 9 depicts

the second Echelon station located in Yakima, near Seattle, which began construction on May 4, 1973, and became operational in October 1974 (European Union, 2001). Through the Yakima Echelon station, all information was managed under the designation "Terminal Operations Control" by the NSA using the Starburst and Oceanfront communication networks, and all data subsequently came under centralized control (Cryptome, 2019).

Figure 9. The Second ECHELON Station Intercepting the Intelsat Pacific Ocean Region Satellite: Yakima, Washington (Covername: Jackknife)(Duncan Campbell, 2019).

An examination of the documents indicates that in 1966, *Frosting*, a major strategic initiative, was first introduced as part of the Echelon system. Within the scope of this program, the *Transient* project was developed, primarily targeting the Soviet Union's *Molniya* satellite communication systems. The purpose of this project was to intercept both military and governmental communications, thereby enhancing the United States' intelligence-gathering capabilities during the Cold War period (Campbell, 1988).

Figure 10. ECHELON System Communication Infrastructure (Conceptual Representation) (Duncan Campbell, 2019).

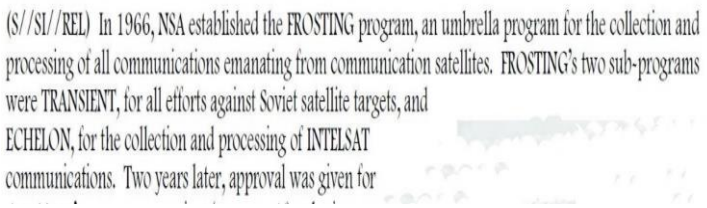
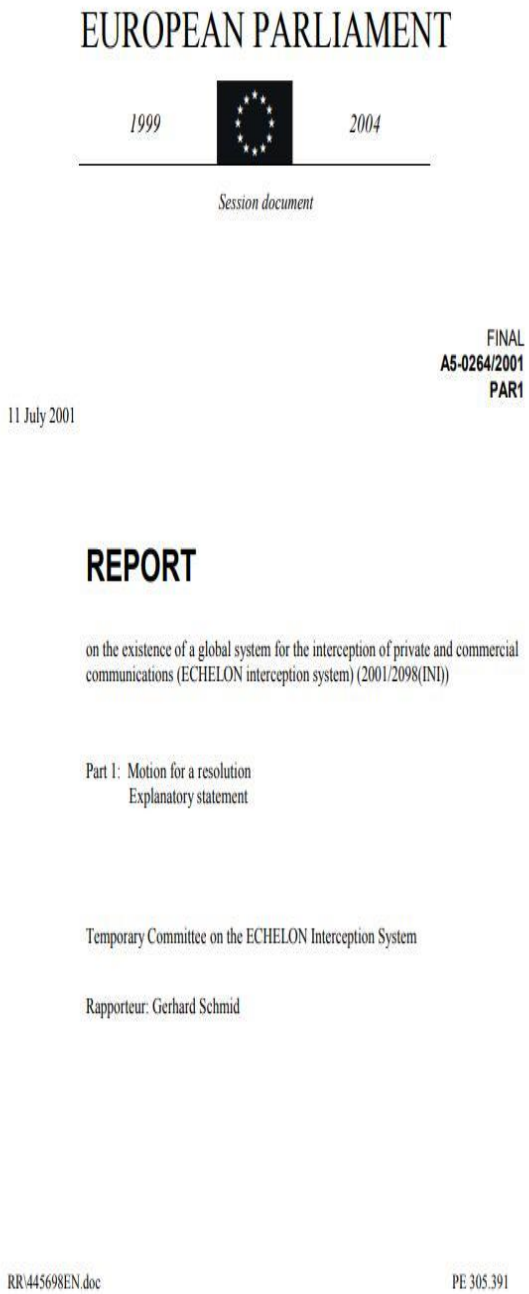

(S//SI//REL) In 1966, NSA established the FROSTING program, an umbrella program for the collection and processing of all communications emanating from communication satellites. FROSTING's two sub-programs were TRANSIENT, for all efforts against Soviet satellite targets, and ECHELON, for the collection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

Figure 11. ECHELON Global Satellite Interception Network (Illustrative Overview)(Duncan Campbell, 2019).


yes, there is an ECHELON system,

Figure 12. European Parliament Report on the ECHELON Interception System (2001) (Temporary Committee on the ECHELON Interception System, European Parliament, 2001).



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))

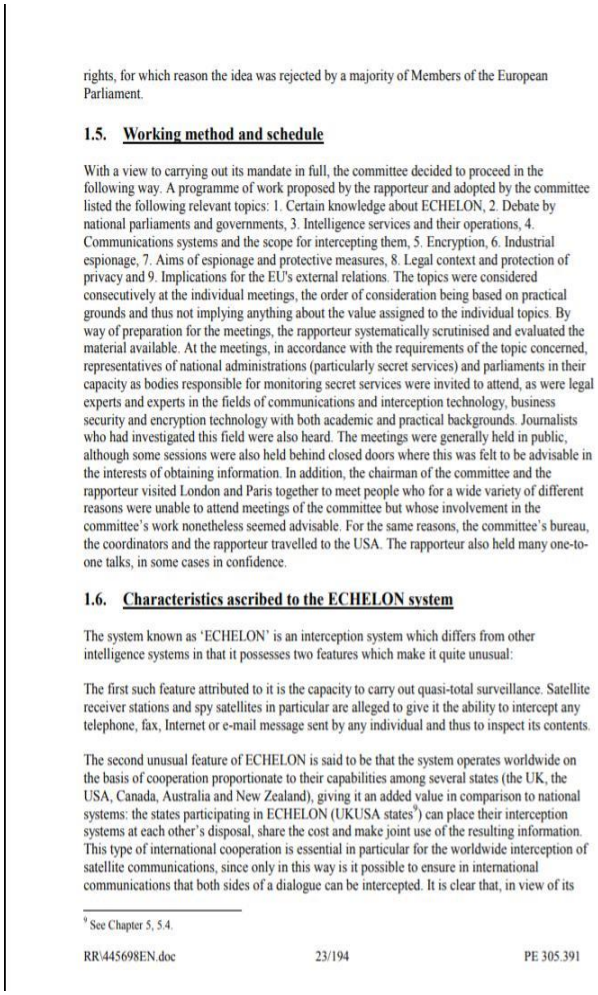
Part 1: Motion for a resolution
Explanatory statement

Temporary Committee on the ECHELON Interception System

Rapporteur: Gerhard Schmid

RR\445698EN.doc PE 305.391

Figure 13. Excerpt from the European Parliament Report on the ECHELON Interception System (2001)(Temporary Committee on the ECHELON Interception System, European Parliament, 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

Based on the available documents, it has been determined that the Echelon system was established during the Cold War era. Mike Frost, a former agent of Canada's Communications Security Establishment (CSE), evaluated the system in February 2000, describing it as a highly advanced and capable data collection network. In response to allegations that the United States had violated the European Convention on Human Rights, the European Parliament established a special oversight committee in 2000 to investigate the Echelon system (Matney, 2015). Between 2000 and 2001, the European Parliament conducted a detailed inquiry, concluding in its report dated June 11, 2001, that the system was operated by the United States and managed by the National Security Agency (NSA). The report also identified the member states where the system was active (European Union, 2001). An official statement from the NSA later confirmed the existence and authenticity of the Echelon program. However, despite partial transparency, it was disclosed in 2005 that domestic email communications were being monitored and conversations intercepted without authorization from then–U.S. President George W. Bush. It

was further noted that allied states also employed the program to access telephone and email content (Matney, 2015).

Conclusion

This study examined the Echelon intelligence system within the framework of cyber intelligence, emphasizing its foundational role in the evolution of the field. It analyzed various forms of cyber intelligence across different historical periods and demonstrated their development in parallel with technological progress. Initially limited in scope, cyber intelligence has significantly expanded over time, influencing social structures and introducing new dimensions of security vulnerability. The discussion on cybersecurity revealed that intelligence agencies and private security organizations worldwide have advanced their capabilities to protect personal data through the development of specialized systems and procedures. Furthermore, countries such as Germany, Russia, and the United Kingdom have institutionalized cybersecurity education through programs offered at universities and government institutions. Regarding the Echelon system, the findings indicate that it originated during the Cold War period and remained classified for many years. Its use by national powers as a surveillance mechanism has raised serious ethical and legal concerns, including violations of the European Convention on Human Rights and disregard for the privacy rights of individuals and states.

References

Abdurahmanlı, E. (2016). Siber istihbarat kapsamında: Echelon istihbarat sistemi. *Akademik Tarih ve Düşünce Dergisi, 3*(11), 1218–1230.

Aydın, N. (2016, 2 Ağustos). Intelligence, agent, and interception. *Antalya Bugün.* https://antalyabugun.com/tr/makale/istihbarat-

Berberakis, S. (2017, 3 Nisan). European Commission: The British bases in Cyprus should be on the table in the Brexit negotiations. *BBC News.* https://www.bbc.com/turkce/haberler-

Campbell, D. (1988, 12 Ağustos). Somebody's listening. *CRYPTOME.* http://cryptome.org/jya/echelon-dc.htm

Campbell, D. (2001). European Parliament resolution on the existence of a global system for the interception of private and commercial communications (ECHELON interception system). http://www.duncancampbell.org/men

Campbell, D. (2019, 16 Eylül). NSA: Yes, there is an ECHELON system. http://www.duncancampbell.org/content/nsa-yes-there-echelon-system

Çağlayan, Y. (2016). *Sociological warfare.* Timaş Yayınları.

CIA Botswana (Pty) Ltd. (2019, 10 Eylül). Cyber Intelligence Agency – Contact. https://www.ciabotswana.com/contact/

Crowley, S. (2014, 17 Ocak). Obama's speech on N.S.A. phone surveillance. *The New York Times.* 14 Ağustos 2019 tarihinde https://www.nytimes.com/2014/01/18/us/politics/obamas-s

DW. (2017, 21 Mart). How Germany's foreign intelligence agency recruits young hackers. *DW News.* https://www.dw.com/en/how-germanys-foreign-intelligence-agency-recruits-young-

DW Akademie. (2017, 21 Mart). How Germany's foreign intelligence agency recruits young hackers. *DW News.*https://www.dw.com/en/how-germanys-foreign-intelligence-agency-

European Parliament. (2001). *Temporary Committee on the ECHELON Interception System: Characteristics ascribed to the ECHELON system.* http://www.duncancampbell.

Federal'naya sluzhba bezopasnosti (FSB). (2018, 25 Ekim). History of the Federal Security Service. http://www.fsb.ru/fsb/history.htm

FSB Akademisi. (2019, 10 Eylül). Rusya Federasyonu Federal Güvenlik Servisi Akademisi. http://www.academy.fsb.ru/i_faculty_ib.html

FSB (ФСБ России). (2018, 25 Ekim). Федера́льная слу́жба безопа́сности: История. http://www.fsb.ru/fsb/history.htm

Gazete Vatan. (2011, 21 Nisan). Efsane lideri Erbakan'ın telefonundan vurmuşlar! *Gazete Vatan.* http://www.gazetevatan.com/efsane-lideri-erbak

Gün, Ç. (2014). *The role and importance of intelligence in determining national security policies* [Yüksek lisans tezi, Turkish Military Academy]. Ankara.

Herman, M. (1999). *Intelligence power in peace and war.* Cambridge University Press.

Kuzu, A. (2015). *MİT, MOSSAD, CIA, GLADIO.* Kariyer Yayıncılık.

Matney, L. (2015, 4 Ağustos). Uncovering ECHELON: The top-secret NSA/GCHQ program that has been watching you your entire life. *TechCrunch.* https://techcrunch.com/2015/08/03/

MI5 Careers. (2019, 10 Eylül). Working at MI5: Video transcripts. https://www.mi5.gov.uk/career

Milliyet Gazetesi. (2014, 14 Ağustos). He asked Obama: Are you listening to Erdogan? *Milliyet.* http://www.milliyet.com.tr/dunya/

Nergis, S. (2014, 15 Ekim). Who gave Dudayev that phone? *TimeTürk.* https://www.timeturk.com/tr/2014/10/15/dudayev-e-o-telefonu-kim-goturdu.html

Özalp, Y. (2015, 22 Ocak). Cyber intelligence and security policies. *WordPress.com.*https://derinstrateji.files.wordpress.com/2015/01/siber-stihbarat-ve-gvenlik-

Özdağ, Ü. (2016). *Intelligence theory.* Kripto Yayınları.

Tevhid Haber. (2007, 27 Nisan). The last image of martyr Chechen leader Dudayev. *Tevhid Haber*. http://www.tevhidhaber.com/sehid-cecen-lid

Tevhid Haber. (2019, 30 Eylül). Last view of martyr Chechen leader Dudayev [Photo and video]. *Tevhid Haber*. http://www.tevhidhaber.com/sehid-cecen-lider-dudayevin-son-

Temporary Committee on the ECHELON Interception System. (2001, 11 Temmuz). Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) *European Parliamen.* http://www.duncancampbell.org/

Turkish Forum Dünya Türkleri Birliği. (2017, 31 Mart). Technical tracking file: The giant intelligence ear! The secret ECHELON project, ECHELON bases, and the new world order. *Turkish Forum.* https://www.turkishnews.com/tr/content/2017dev-