Trakya Üniversitesi
Mühendislik Bilimleri Dergisi

Cilt: 17 Sayı: 1 Haziran 2016

TRAKYA UNIVERSITY JOURNAL OF ENGINEERING SCIENCES

Volume: 17 Number: 1 June 2016

Trakya Univ J Eng Sci

http://dergipark.ulakbim.gov.tr/tujes
tujes@trakya.edu.tr

ISSN 2147-0308

Trakya Üniversitesi
Mühendislik Bilimleri Dergisi

Cilt: 17 **Sayı: 1** **Haziran** **2016**

Trakya University
Journal of Engineering Sciences

Volume: 17 **Number: 1** **June** **2016**

Trakya Univ J Eng Sci

http://dergipark.ulakbim.gov.tr/tujes
tujes@trakya.edu.tr

ISSN 2147-0308

Dergi Sahibi / Owner
Trakya Üniversitesi Rektörlüğü, Fen Bilimleri Enstitüsü Adına
On behalf of Trakya University Rectorship, Graduate School of Natural and Applied Sciences
Prof. Dr. Mustafa ÖZCAN

Baş Editör / Editor-in-Chief
Doç. Dr. Hacı Ali GÜLEÇ

Yardımcı Editörler / Associate Editors
Doç. Dr. Cem S. ÇETİNARSLAN
Yrd. Doç. Dr. Esma MIHLAYANLAR
Yrd. Doç. Dr. Altan MESUT
Yrd. Doç. Dr. A. Can ZÜLFİKAR

Dizgi / Design
Yrd. Doç. Dr. Altan MESUT, altanmesut@trakya.edu.tr
Taylan ŞAHİNBAŞ, taylansahinbas@hotmail.com

İletişim Bilgisi / Contact Information
Address : Trakya Üniversitesi, Enstitüler Binası, Fen Bilimleri Enstitüsü,
Balkan Yerleşkesi, 22030, Edirne / TÜRKİYE
Web site : http://dergipark.ulakbim.gov.tr/tujes
E-mail : tujes@trakya.edu.tr
Tel : +90 284 2358230
Fax : +90 284 2358237

Baskı / Publisher
Trakya Üniversitesi Matbaa Tesisleri
Trakya University Publishing Centre

ISSN 2147-0308

ISSN 2147-0308

İÇİNDEKİLER / CONTENTS

ISSN 2147-0308

http://dergipark.ulakbim.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 17(1): 1-11, 2016
ISSN 2147–0308
Araştırma Makalesi / Research Article

COMPARISON OF ENCRYPTION ALGORITHMS STRENGTH USED IN 3G MOBILE COMMUNICATION

Fatma AKGÜN[1], Ercan BULUŞ[2]

[1] Department of Computer Education and Instructional Technologies, Trakya University, Edirne-TURKEY
e-mail: fatmaa@trakya.edu.tr
[2] Department of Computer Engineering, Namık Kemal University, Çorlu/Tekirdağ-TURKEY
e-mail: ercanbulus@nku.edu.tr

Abstract: In this study, the strength of data encryption algorithms used in UMTS and CDMA2000 systems which are 3G mobile communication technologies were analyzed. At the beginning of the study, software applications were developed for KASUMI encryption algorithm which is used within UMTS system and AES encryption algorithm which is used within CDMA2000 system. Both key generation algorithms are applied to the same key values to create new key values which are used for data encryption. These new key values are tested by using test package of NIST to in order to check whether these key values are generated randomly or not. One of the key value which has high randomness is used as encryption key As a result, it was observed that AES algorithm is more successful than KASUMI algorithm in generating key values. Additionally, a key value, which has high randomization, was chosen and this key value was applied on encryption algorithm with plain text statement and as a result application of encrypted text on NIST test, it was observed that both KASUMI and AES block encryption algorithms have equally power in 3G mobile technology.
***** This paper is based on a Ph.D study titled "The Structure of Mobile Communication Technologies and Analysis of the Reliability of Data Encryption Algorithms Used in These Technologies"

Keywords: Security, Mobile communication, KASUMI, AES, NIST tests

3G Mobil Haberleşme İçerisinde Kullanılan Şifreleme Algoritmalarının Gücünün Karşılaştırılması

Özet: Bu çalışmanın amacı 3G mobil iletişim teknolojilerinden CDMA2000 ve UMTS sistemlerinde yer alan veri şifreleme algoritmalarının gücünün karşılaştırılmalı analizidir. Öncelikle UMTS teknolojisi içerisinde yer alan KASUMI şifreleme algoritması ve CDMA2000 teknolojisi içerisinde yer alan AES şifreleme algoritmaları için yazılım geliştirilmiştir. Yeni şifreleme anahtarları elde etmek için her iki anahtar üretme algoritmasına aynı anahtar değerler uygulanmış ve elde edilen yeni anahtar değerler rassallıkları test edilmek üzere NIST testlerinden geçirilmiştir. Rassalığı yüksek olan anahtar değerlerinden biri şifreleme anahtarı olarak kullanılmıştır. Çalışma sonunda, şifreleme algoritması içerisinde, açık metni şifrelemek için kullanılacak olan yeni anahtar değerlerinin üretiminde AES algoritmasının KASUMI algoritmasına oranla güçlü olduğu sonucu ortaya çıkmıştır. Çalışmada ayrıca yüksek randomizasyon veren anahtar değerlerinin kullanımı ile yapılan şifreleme işlemi sonucuna göre 3G teknolojisi içerisinde yer alan KASUMI ve AES şifreleme algoritmalarının eşit derecede şifreleme gücüne sahip olduğu ortaya çıkmıştır.
***** Bu çalışma "Mobil İletişim Teknolojilerinin Yapısı ve Bu Teknolojilerde Kullanılan Veri Şifreleme Algoritmalarının Güvenirliklerinin Analizi" adlı doktora tezinden üretilmiştir.

Anahtar kelimeler: Güvenlik, Mobil iletişim, KASUMI, AES, NIST testleri

INTRODUCTION

Due to development in science and technology, mobile communication systems in which users have the freedom of acting independently from time and space has occurred. Hardship and restrictions of cabled communication system accelerated shifting towards mobile communication system which enables wireless communication among people. The popularity and availability of wireless communications, particularly cellular, continues to grow rapidly world-wide. Mobile users are interested in services such as mobile shopping, mobile banking and mobile payments. Multimedia applications, high data rate, mobility, and cost make wireless communication one of the most useful means of communication (Schoinas, 2013). Protecting analogue information against eavesdropping is not easy but digital transmission allows for excellent level of protection. Encryption is the process where a series of bits are transformed by mathematical or logical functions into another series of bits (Payal, 2014).

In mobile communication technology, authentication algorithms and data encryption algorithms are used on the system in order to enable secure communication of users. In this way it was aimed to prevent stealing or changing data or communicating with fake users. Encryption is an essential process to ensure confidentiality over wireless channels, because wireless channels are an open medium to intruders in which they can intercept and alter the content of any transmitted information. (Zibideh & Matalgah, 2015). Encryption is carried out in order to hide a

text, voice or image for security. Plain text, encryption code and encryption algorithm is required in order to do encryption (Babbage, 2000; Balani, 2007; Chen & Guizani, 2006). The Third Generation (3G) proposal for cellular communication aimed at maintaining compatibility with Global System for Mobile Communication (GSM) as well as address security weaknesses of the GSM architecture (Schoinas, 2013).

While UMTS (Universal Mobile Telecommunications System) system which is one of 3G (3rd Generation) mobile communication technology uses KASUMI algorithm that has block cipher structure; CDMA2000 (Code Division Multiple Access 2000) system which is also called as 3G mobile communication technology uses AES (Advanced Encryption Standard) algorithm that also has block cipher structure (3GPP Task Force, 1999; Nyberg, 2004, Fibs 197, 2001). In our study, we studied data encryption reliability of both KASUMI and AES encryption algorithms with the help of NIST (National Institute of Standards and Technology) tests (Demirkol, 2007; Akyıldız et al., 2004; Bassham, 2010; Yalcin, Suykens & Vandewalle, 2004). In the practice, same text values were entered in both encryption algorithms. 10 key values were obtained in order to encrypt this text and key value which has the highest randomization among these new key values that are obtained from AES and KASUMI algorithm were taken and used in encryption.

RELATED WORKS

There are different studies upon the power of AES and KASIMU which are encryption methods used in 3G communications. Let's review the most important ones. KASUMI algorithm is an 8 round Feistel encryption and generates 64 bit output from 64 bit input using 128 bit K key. The first serious attack was done for KASUMI by Mark Blunden and Adrian Escott in 2002. They have done "related key" attack on 5 and 6 round KASUMI and succeeded in obtaining the key (Blunden & Escott, 2002). In 2005, Tanaka, Sugio and Kaneko applied differential cryptanalysis which uses efficiently chosen plain texts for 5 round KASUMI and they succeeded as well (Tanaka, Sugio & Kaneko, 2005). In another study carried out in the same year, Biham, Dunkelman and Keller did "Related-Key Rectangle" attack on full round KASUMI which is also successful theoretically (Biham, Dunkelman & Keller, 2005). In 2010, Dunkelman, Keller and Shamir attained 128 bit key for full round KASUMI by using only 4 related key with a recently designed attack which they named sandwich attack. They have done this attack with standard optimization parameters of gcc 4.3.2. Compiler on GHz, 4 MB L2 Cache, 2 GB RAM" and "T7200 Intel Core Duo 2 CPU and Linux-2.6.27 kernel" (Dunkelman, Keller & Shamir, 2010). As a result of this attack, the reliability of KASUMI has become problematic today. In 2014, Wang et al. DFA attacked on KASUMI-64 which is the base of A5/3 cryptosystem. They showed that only one 16-bit word fault is enough to perform a successful key recovery attack. They emphasized that when applying KASUMI-64, the last two rounds should be specially designed to protect against fault injection emphasize that when applying KASUMI-64, the last two rounds should be specially designed to protect against fault injection. In, 2014, Dunkelman, Keller and Shamir, described a new type of attack called a *sandwich attack*, and used it to construct a simple related-key distinguisher for 7 of the 8 rounds of KASUMI with an amazingly high probability of 2−14. By analyzing the single remaining round, they could derived the complete 128-bit key of the full KASUMI with a related-key attack which uses only 4 related keys. In 1997, NIST began to carry out study for an algorithm which is named AES that can be replaced with DES (Data Encryption Standard) algorithm. As a result of conferences, five finalist including Rijndael algorithm were determined in 1999 (Daemen & Rijmen, 1999). AES standard was done with fips-197 (Federal Information Processing Standards) published by NIST (Fibs 197, 2001). In 2006, "related-key impossible differential" attack was done by Biham, Dunkelman and Keller. The attack was done theoretically on the first 8 round of AES-192 using 192 bit key and it was successful (Biham, Dunkelman & Keller, 2006). In 2008, a successful "new impossible differential" attack was done by Lu, Dunkelman, Keller and Kim for 8 round AES-256 (Lu, et al, 2008). In 2010, a successful "single-key" attack was done on 10 round AES-256 by Dunkelman, Keller & Shamir. While full round AES-256 is not broken, it brings worry about the reliability of 10 round for being broken by such a trivial complexity. In 2012, "differential fault" analysis was done by Chong Hee Kim, but it was not successful for full round (Kim, 2012).

STRUCTURE OF KASUMI ENCRYPTION ALGORITHM

KASUMI block encryption is used for reliability and protecting integrity within UMTS. KASUMI is a powerful encryption algorithm installed on MISTY1 block encryption algorithm which was designed to meet certain security, speed, and hardware complexity requirement and including 128 bit key, 64 bit block and 8 round Feistel encryption structure.Although some algorithms are widely used in wireless systems such as KASUMI, which is used in the Global System for Mobile and the Universal Mobile Telecommunications System, it is shown that this algorithm satisfy the avalanche criterion as in other traditional encryption algorithms (Zibideh & Matalgah, 2015)

Within KASUMI algorithm (Fig.1) there are 7 bit S7 and 9 bit S9 boxes which enable minimum differential and linear probability. By using S boxes in functions of each round, algorithm was enabled to be reliable against differential and linear cryptanalysis. By applying various transactions to 128 bit startup key which is entered in algorithm, new key values to be used in each round are obtained and these new key values are used in various functions. In encryption, nested functions which are different from each other such as FO, FL and FI are used. In this way, security within algorithm is improved (Balderas & Cumplido, 2004; Dohmen & Olaussen, 2001; Wang, Dong, Jia & Zhao, 2014).

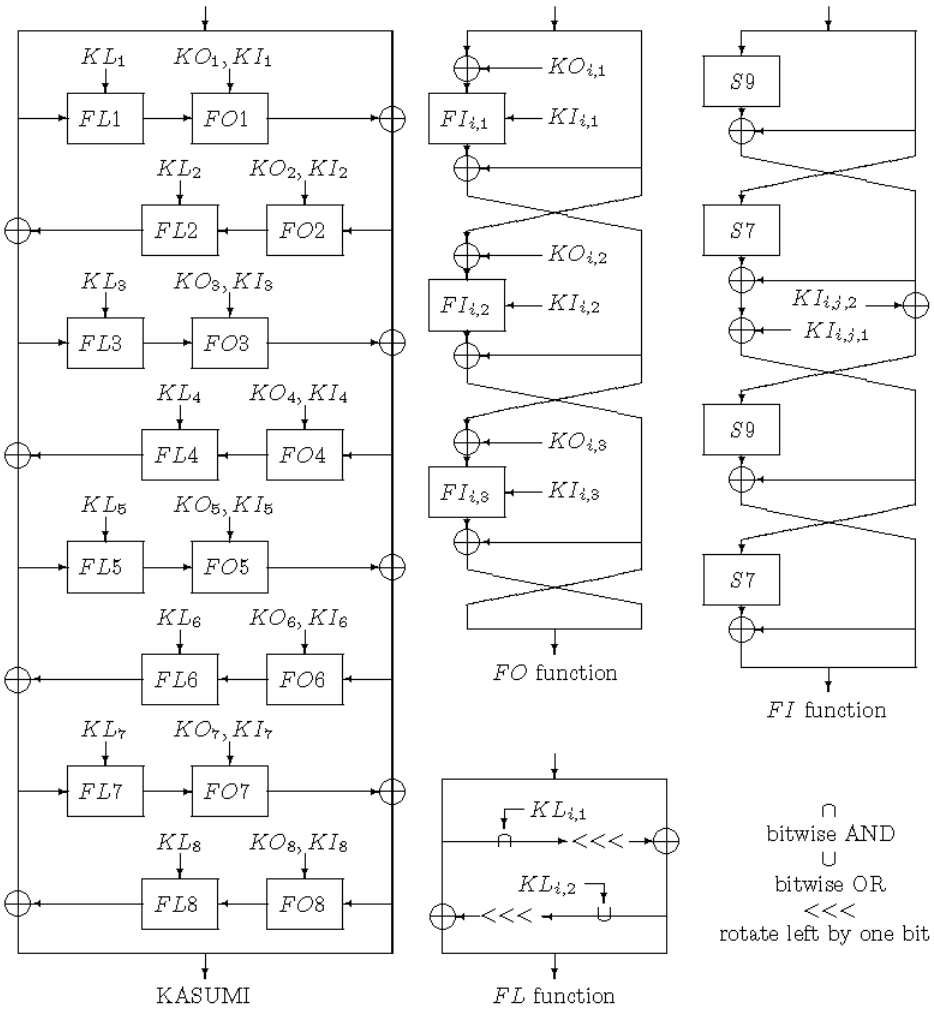


Figure 1. KASUMI Algorithm Flowchart (Dunkelman, Keller & Shamir, 2010).

Obtaining Key Values

KASUMI algorithm obtains 128 bit new key value within 128 bit key value entered in it and uses this value in the encryption. In the process of obtaining key, 128 bit key which is entered in the algorithm is separated in to 8 equals pieces, K=K1 || K2 || K3 || K4 || K5 || K6 || K7 || K8, being from j=1 to 8. Kj_I sequence is obtained from Kj. For each j integer value, Kj_I=Kj XOR Cj keys are obtained by using 1<j<8 Cj (table 1) stable values. By using these new key values, new values to be used in different functions are obtained (Table 2).

Table 1. C Values

C1	0x0123
C2	0x4567
C3	0x89AB
C4	0xCDEF
C5	0xFEDC
C6	0xBA98
C7	0x7654
C8	0x3210

Table 2. Encryption Key values

subkeys	i.round
KL_{i1}	K_i <<< 1
KL_{i2}	$K^I_{i+2\ (\mathrm{mod}\ 8)}$
KO_{i1}	$K_{i+1\ (\mathrm{mod}\ 8)}$ <<< 5
KO_{i2}	$K_{i+5\ (\mathrm{mod}\ 8)}$ <<< 8
KO_{i3}	$K_{i+6\ (\mathrm{mod}\ 8)}$ <<< 13
KI_{i1}	$K^I_{i+4\ (\mathrm{mod}\ 8)}$
KI_{i2}	$K^I_{i+3\ (\mathrm{mod}\ 8)}$
KI_{i3}	$K^I_{i+7\ (\mathrm{mod}\ 8)}$

KASUMI algorithm is an 8 round Feistel encryption and generates 64 bit output from 64 bit input using 128 bit K key. FL, FO and FI functions within the algorithm form the basic structure. 64 bit value entered within algorithm is separated into two, being the first 32 bit and the last 32 bit ($L=[63:32]$ and $R=[31:0]$). We can express the algorithm as each being i, in other words round value. Fi function transforms 32 bit input value to 32 bit output value under the control of RK_i round key (round key KL_i, KO_i and KI_i being triple key group). The function is obtained from two sub-functions structurally. FL and FO function are integrated with KL_i (which is used with FL) and KO_i-KI_i (which are used with FO) subkey. Fi function is formed in two ways being related to single and dual rounds (Blanchard, 2000; Kitsos, Galanis and Koufopavlou, 2004; Akleylek, 2008).

for 1, 3, 5 and 7 rounds;

$$f_i(I, RK_i) = FO(FL(I, KL_i), KO_i, KI_i)$$

for 2, 4, 6 and 8 rounds;

$$f_i(I, RK_i) = FL(FO(I, KO_i, KI_i), KL_i)$$

Process Steps in KASUMI Algorithm

FL Function:

FL Function takes 32 bit I input value and process it with 32 bit KL key value. While KL key is separated into two sub-keys being 16 bit $KL_{i,1}$ and $KL_{i,2}$, in round number; 32 bit I input value is separated into I=L||R 16 bit two groups. The processes below are done and 32 bit output value $O=(L^I||R^I)$ is obtained (Fig.1).

$$R^I = R \oplus ROL(L \cap KL_{i,1})$$

$$L^I = L \oplus ROL(R^I \cup KL_{i,2})$$

FO Function

FO function includes 32 bit input data and 48 bit KO_i and 48 bit KI_i values; i being the round number. 32 bit input data is separated into two parts being L and R.

48 bit sub-keys are separated into three 16 bit subkeys.

$$KO_i = KO_{i,1} \| KO_{i,2} \| KO_{i,3}$$

$$KI_i = KI_{i,1} \| KI_{i,2} \| KI_{i,3}$$

Being $1 \le j \le 3$

$$R_j = FI(L_{j-1} \oplus KO_{i,j}, KI_{i,j}) \oplus R_{j-1}$$

$$L_j = R_{j-1}$$

values are obtained in each round and at the end of 3. round final value $(L_3 \,||\, R_3)$ to be.

FI Function

FI function uses 16 bit input value and 16 bit $KI_{i,j}$ key value. Input value is separated into two unequal parts. L0 is the first 9 bit values in the left; R0 is the first 7 bit values in the right. $KI_{i,j}$ key value is separated into two parts being 7 bit $KI_{i,j,1}$ sub-key value and 9 bit $KI_{i,j,2}$ sub-key value.

$$KI_{i,j} = KI_{i,j,1} \| KI_{i,j,2}$$

The function uses two S boxes. These are S7 box which maps 7 bit input to 7 bit output and S9 box which maps 9 bit input to 9 bit output. These boxes also use two additional functions which are called ZE() and TR().

ZE(X)= transforms 9 bit X value by adding 2 zero values to the most important part.

TR(X)= transforms 9 bit X value into 7 bit X value ignoring the most important bits.

$L_1=R_0$

$$R_1 = S9[L_0] \oplus ZE(R_0)$$

$$L_2 = R_1 \oplus KI_{i,j,2}$$

$$R_2 = S7[L_1] \oplus TR(R_1) \oplus KI_{i,j,1}$$

$L_3=R_2$

$$R_3 = S9[L_2] \oplus ZE(R_2)$$

$$L_4 = S7[L_3] \oplus TR(R_3)$$

$R_4=R_3$

The function generates 16 bit (L4 || R4) result.

STRUCTURE OF AES ENCRYPTION ALGORITHM

AES is one of the encryption techniques which is used most frequently because of its high efficiency and simplicity. It is the highly secure algorithm. AES represents the current recommended standard by NIST for encryptions (Kaul et al. 2015). AES (Fig.2) is an algorithm which encrypts 128 bit data blocks with 128, 192, 256 bit key choices. It is a broad type

of SPN algorithm. The number of round varies according to key width. While it encrypts 10 round for 128 bit key, it encrypts 12 and 14 round respectively for 192 and 256 bit keys. Every round is composed of four layers in AES algorithm. First of all 128 bit data is transformed to 4x4 byte matrix. Then, in each round bytes are displaced, lines are shifted, columns are compared XOR process is done with key values from key planning and determined for that round. In the displacement of bytes each of 16 byte values are entered into 8 bit input and 8 bit output S box. In the process of row shifting, rows are shifted in 4x4 byte matrix and in the process of column comparison values at that column are compared for any column. In the last layer of the round, encrypted data was obtained doing XOR process with key values of that round (Chung & Phan, 2002; AES, 2001).

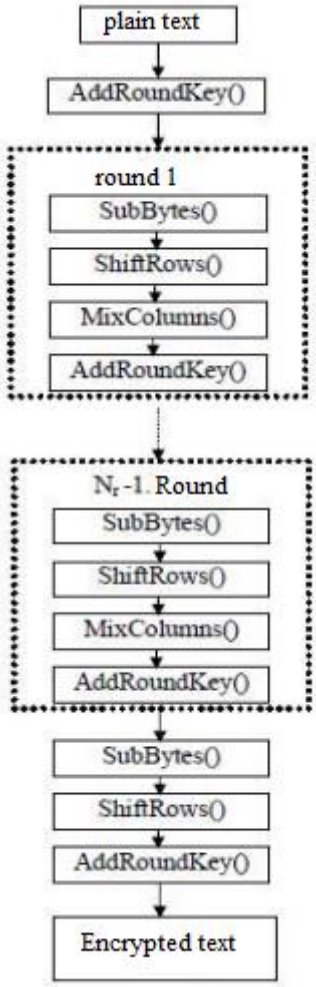


Figure 2. AES Algorithm Flowchart

Obtaining Key Values

AES encryption algorithm tries to encrypt 128 bit block data with 128 bit key value. In the beginning of encryption process, new key values are obtained from current 128 bit key values. The first 128 bit key value is divided into 4 blocks in itself. These four blocks are entered into Key Extension algorithm. Data are shifted to the left in key extension algorithm, entered into S boxes and treated with XOR process with some specific stable values. As a result, new different key values are obtained in order to use at each round of AES encryption algorithm (Fibs 197, 2001).

Sub-Bytes Function

It is a layer where S box is used. It takes the information of input matrix and passes each byte through a defined S box and obtains result. In the displacement of bytes, each 16 byte values are entered into 8 bit input and 8 bit output S box. After S box values are negated in Galois field (Galois Field - GF) GF(28), for 8 bit polynomial (m(x) = x8 + x4 + x3 + x + 1) it is obtained by entering a linear transformation. In this way inverse of each byte are found in the matrix.

Shift-Rows Function

This function takes condition matrix and shifts the last three rows to the left circularly according to specific values. In the process of shifting, while the 1st row remains same, 2nd row is shifted one time, 3rd row is shifted two times and 4th row is shifted 3 times.

MixColumn Function

This function takes condition matrix and shifts the last three rows to the left circularly according to specific values. In the process of shifting, while the 1st row remains same, 2nd row is shifted one time, 3rd row is shifted two times and 4th row is shifted 3 times.

AddRound Key Function

In this function, every round value is treated with XOR process with new key values obtained for them.

RANDOM NUMBER GENERATOR

Randomization is observed as a feature where there are not simple relations between elements, there is no specific draft, in short as inestimable feature. Randomization is one of the most common features used in order to enable privacy, dissolution in cryptography. The result of encryption should be as much inestimable as it can be in order for the attacker not to obtain actual data. Random numbers form the basis of many cryptographic practices. There are random number generators in order to use in cryptographic practices. Numbers in the output of random number generator are systems which are statistically independent from each other. It is possible to divide random number generators (RNG) into two such as actual random number generators (ARNG) and pseudo random number generators (PRNG). One of them is preferred according to the aim of practice. While the practice of actual RNG depends on the

measurement of national process such as noise, pseudo RGN uses deterministic processes such as digital algorithms (Grošek, Vojvoda & Krchnav, 2009).

Statistical Tests for Random Number Generators

These tests tell us whether the output of the generator fulfills the requirements expected from a random series. Moreover, the quality of random number generator can be commented considering test results. In order to say whether a number sequence is random or not, it must be tested. If only one test is unsuccessful the sequence is not accepted to be random. Statistical hypothesis test are used in order to do statistical deduction. A hypothesis (null hypothesis, H0) is put forwards in these tests, the inverse of this hypothesis is accepted to be alternative hypothesis, Ha. There are two different decisions to be attained as a result of statistical test: *Reject or not reject H0.*

The first decision is taken when there is a strong proof against H0. When this strong proof is not found, the second decision is taken. There is an inevitable factor of error in all statistical tests. Two different types of error, first type (alpha) error and second type (beta) error can be made as a result of the test. The first type of error happens when the decision is reject H0 while hypothesis is correct. The second type of error happens when the decision is not reject H0 while hypothesis is false. The probability of making first type error should be restricted in the hypothesis test. The probability of making first type error gives the reliability level of our test. This value is generally chosen as 0.01-0.05. The power of a statistical test is equal to the probability of not making second type error. More sampling is carried out in order to increase the power of test. While doing a statistical test; first of all H0 and Ha are determined. Then, reliability level of the test is determined. A sampling is done and test statistics and p-value related with it are calculated. Instead of controlling the probability of making first type error, p-value corresponds to the probability of test statistics being an observation value or more extreme value, on the assumption that H0 is correct. The probability which is calculated according to this definition gives p-value. If this value is smaller than the chosen reliability value H0 hypothesis is rejected. Distributions which are most commonly used in statistical tests are Normal and Chi-square distributions (Akyıldız, et al, 2004).One of the common tests is NIST 800-22 (Bassham, 2010) which are published by Institute of National Standards and Technology. This test system is generally formed in order to test data which are composed of long blocks.

NIST 800-22 Test System

The system is used in order to test data which are composed of long blocks. It has more powerful structure compared to previous tests. In other words, a system which had passed previous tests and accepted to be reliable may not pass this test. For this reason, this system is a structure which can be used in serious processes. NIST 800-22 is composed of 15 separated tests. In order for a tested bit sequence to be successful it should pass all the tests successfully. Below are the tests with brief explanations:

1. Frequency Test: analyzes 1 and 0 balance in bit sequence.

2. Block Frequency Test: analyzes 0 and 1 balance of m bit blocks.

3. Runs Test: analyzes the number of 0 and 1 blocks (runs).

4. Longest run of Ones in a Block Test: analyzes the length of 0 and 1 blocks (runs).

5. Rank Test: By using bit blocks at stable lengths, creates a matrix each one of which indicating a row and calculating the rank of matrix, linear dependence between blocks are analyzed.

6. Discrete Fourier Transform Test: Takes Fourier transformation of current bit sequence and analyzes periodicity.

7. Non-Overlapping Template Matching Test: Analyzes the recurrence of m bit block within sequence. In the event of recurrence, creates a new m-bit block beginning from the recurrent block.

8. Overlapping Template Matching Test: Analyzes the recurrence of m bit block within sequences. In the event of recurrence, a new one is created by shifting the block 1 bit.

9. Universal Test: Analyzes how far the sequence could be compressed without data loss

10. Linear Complexity Test: Analyzes the complexity of bit sequence by observing the length of LFRS (linear feedback shift register).

11. Serial Test: Analyzes the number of recurrence of 2m block. For m=1, it is equal to the first test.

12. Approximate Entropy Test: Analyzes entropy of recurrent and m and (m+1) bit blocks.

13. Cumulative Sums Test: Separating bit sequence into sequential length blocks; determines 1 and 0 balance and considers the difference of unbalance between blocks.

14. Random Excursion Test: Separating bit sequence into sequential length blocks; determines 1 and 0 balance and then analyzes the distribution of block balance.

15. Random Excursion Variance Test: Separating bit sequence into sequential length blocks; determines 1 and 0 balance and determine deviation from average value.

COMPARISON OF KEY VALUES OF KASUMI AND AES ENCRYPTION ALGORITHMS

Being the same with KASUMI algorithm used in UMTS system and AES algorithm used in CDMA2000 system; ten 16 character, 128 bit, encryption keys were entered and these 10 encryption key were transformed to be used in encryption within algorithms and randomization of the values were tested by using NIST test package (Table 3).

Table 3. Selected keys

Key 1	Yt5D*}98?fwM2&jR	**Key 6**	ewG%33bcxfsmlk99
Key 2	7ygv6tfc5rdx8265	**Key 7**	7+Gf5/%gOpEw%'3r
Key 3	9P^3%FaR#09hG21(	**Key 8**	FatmAakGUN128753
Key 4	FGd&33Sx(=&fdcxs	**Key 9**	£$k9sd\ks7@nönbf
Key 5	r35+^g3ST^1F-=o4	**Key 10**	635Fr^2XdawN^}nS

Following the application of test package, p-values were evaluated and stated graphically. Success value $\alpha = 0.01$ is taken as. Since program output applied to NIST test package could not meet adequate criteria for some of the test, p-values could not be obtained. Below is the table about key-value entered for the formation of new keys to be used in KASUMI and AES block encryption algorithms and probability values and their graphical values obtained as a result of applying NIST tests were given (Fig. 3, 4, 5, 6).

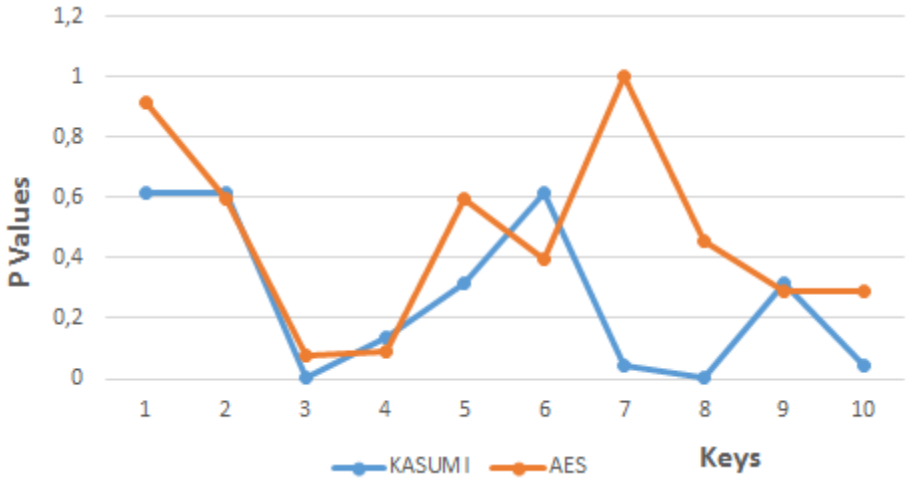


Figure 3. Frequency Test

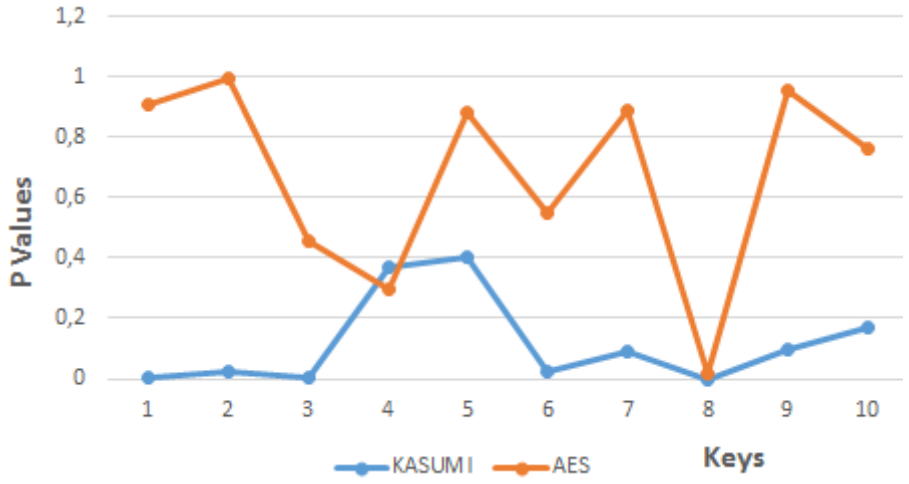


Figure 4. Longest run of Ones in a Block Test

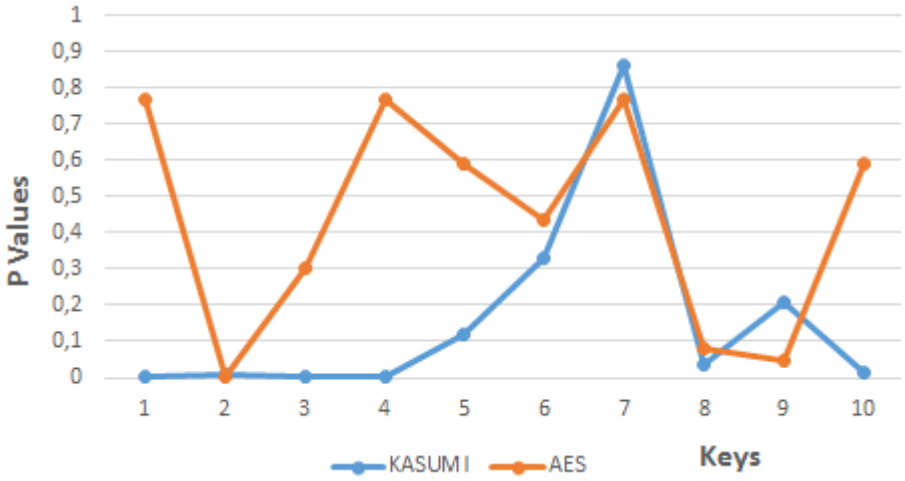


Figure 5. Discrete Fourier Transform Test

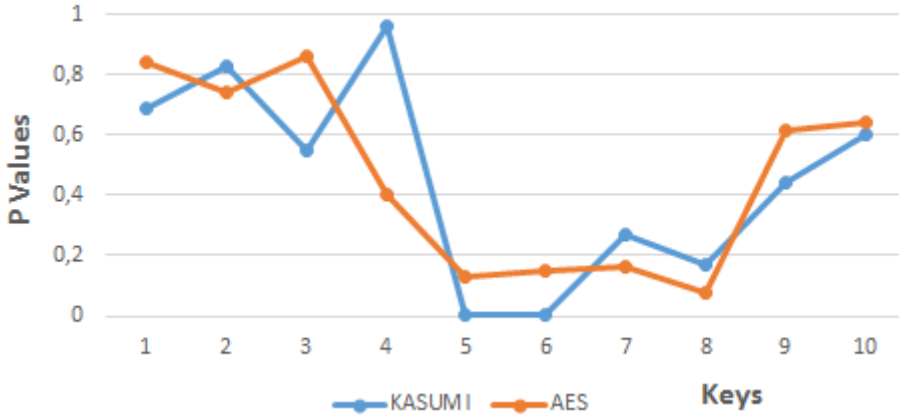


Figure 6. Cumulative Sums Test

As it can be observed from the graphics above; AES algorithm was more successful than KASUMI algorithm in the process of key generation. In Frequency Test and Cumulative Sums Test, 6 out of the 10 key values which were generated by AES algorithm, were more successful than the ones that are generated by KASUMI algorithm. In Discrete Fourier Transform Test, AES was better in 7 key values and In Longest run of Ones in a Block Test, it was better in 9 key values.

In the process of AES algorithm key generation, S-boxes which are reliable against linear and differential cryptanalysis were used. S-boxes (replacement boxes) are quite important since they are the only non-linear elements of block encryption algorithm. Therefore a good choice of S-box directly prevents the complexity of the cipher. Besides this, in key obtaining process, the key was made stronger by delaying rows and making XOR process by previous round keys. In KASUMI algorithm, as a result of processing new startup key value with specific values, new cycle key values are obtained. The key obtained in this way is weak.

COMPARISON OF ENCRYPTED TEXTS OF KASUMI AND AES ENCRYPTION ALGORITHMS

A written text was ciphered by making use of NIST test results, and using **Yt5D*}98?fwM2&jR** key-value which has high randomization in KASUMI and AES encryption algorithms which use 128 bit block. Results of encryption were applied on NIST tests and graphics were drawn for result values of each test (Fig.7, 8, 9, 10).

As a result of NIST tests, key values which have the highest randomization for both encryption algorithms were chosen and a written text was encrypted and NIST tests were applied to the encrypted text. Again depending on NIST test results, it was observed that randomization of encrypted texts generated by both AES and KASUMI encryption algorithms were at the same levels and they have different superiorities over each other in NIST test samplings.

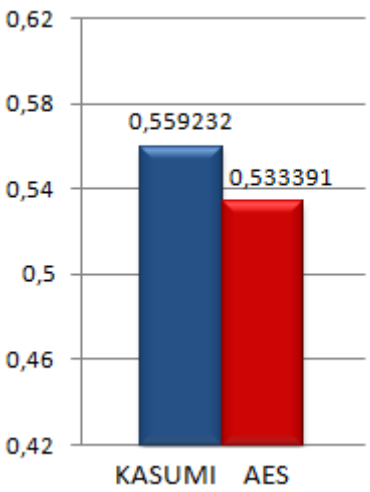


Figure 7. Frequency Test

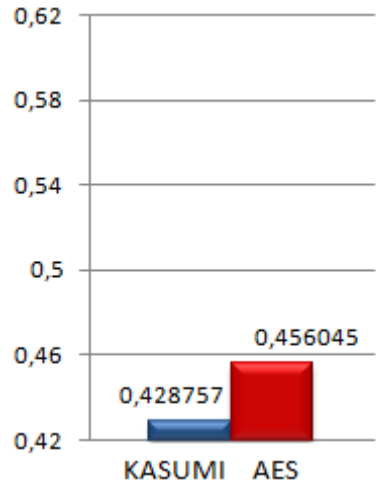


Figure 10. Discrete Fourier Transform Test

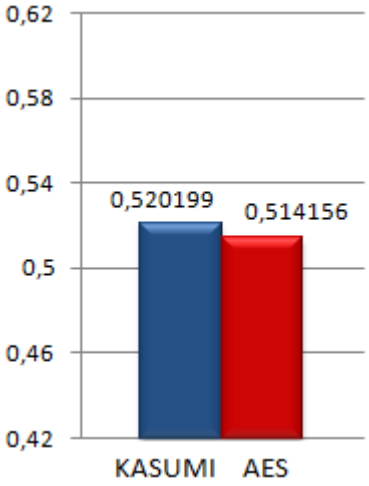


Figure 8. Runs Test

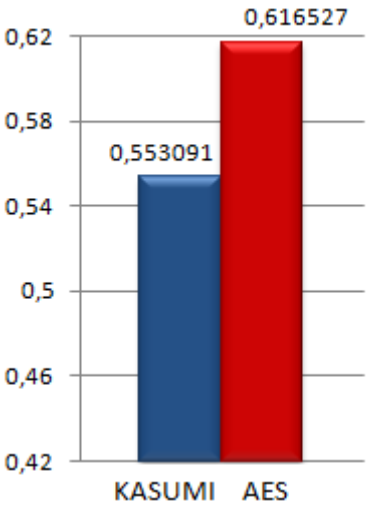


Figure 9. Longest run of Ones in a Block

CONCLUSIONS

In mobile communication technology, authentication algorithms and data encryption algorithms are used to provide secure communication between users. So in this study, the power of data encryption algorithms used in UMTS and CDMA2000 systems which are 3G mobile communication technologies were analyzed. A key value among 10 key values generated from AES and KASUMI algorithms which is observed to give good results from NIST test used for both algorithms was taken and encryption was done by using written text statement. In the applications, new key values to be used for data encryption are generated and these key values are tested by using test package of NIST in order to check whether these key values are generated randomly or not; and then one of the key value which has high randomness is used as encryption key and thereafter again NIST test package is used for testing whether acquired encrypted text values are random or not. Including the acquired test criteria results, evaluations are made on the power of encryption algorithms used in mobile communication technologies. When we apply NIST tests on key values obtained as a result of both algorithms, it was also observed from the graphic above that new key values to be used in AES algorithm have higher randomization, in other words they are more complex and reliable compared to key values to be used in KASUMI algorithm. It was observed that both algorithms have similar power in obtaining encipher text. With the results obtained, the problem of KASUMI in key generating should be reviewed. As a result, both methods have similar power when powerful keys are selected and the obtained results are shown graphically.

REFERENCES

1. 3GPP Task Force. Document 2: KASUMI specification: 3GPP confidentiality and Integrity Algorithms, 1999.
2. ADVANCED ENCRYPTİON STANDARD (AES), *Federal Information Processing Standards Publication 197,* November 26, 2001.
3. AKLEYLEK, S. On The Avalanche Properties of Misty1, Kasumi and Kasumi-R. A Thesis Submitted To The Graduate School of Applied Mathematics of Middle East Technical University, 2008.
4. AKYILDIZ, E., DOĞANAKSOY, A., KEYMAN, E. ve UĞUZ, M. *Kriptolojiye Giriş Ders Notları*. Uygulamalı Matematik Enstitüsü, Kriptografi Bölümü, ODTÜ, TÜRKİYE, 115-120, 2004.
5. BABBAGE, S. Design of Security Algorithms for Third Generation Mobile Telephony, Vodafone Ltd, *Information Security Technical Report*, 5(3), 66-73, 2000.
6. BALANI, A. Authentication and Encryption in CDMA Systems. Head-India Carrier Support Group, LG Soft India Private Limited, 2007.
7. BASSHAM, L, E. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. *NIST Special Publication 800-22,* Computer Security, April 2010.
8. BIHAM, E., DUNKELMAN, O. and KELLER, N. Related-Key Impossible Differential Attacks on 8-Round AES-192. *CT-RSA 2006*, LNCS 3860, pp. 21-33, 2006.
9. BIHAM, E., DUNKELMAN, O. and KELLER, N. Related-Key Rectangle Attack on the Full KASUMI. *Asiacrypt 2005*, LNCS 3788, pp. 443-461, 2005.
10. BLANCHARD, C. Security for the Third Generation (3G) Mobile System, *Information Security Technical Report,* 5(3), pp.55-65, 2000.
11. BLUNDEN, M. and ESCOTT, A. Related Key Attacks on Reduced Round. *LNCS*, Vol.2355, 277-285, 2002.
12. CHEN H. H. and GUIZANI M. Next Generation Wireless Systems and Networks, *John Wiley & Sons*, ISBN- 13 978 -0-470-02434-8 (HB), 2006.
13. CHUNG, R. and PHAN, W. Mini Advanced Encryption Standard (Mini-AES): A Testbed for Cryptanalysis Students. *Cryptologia*, 26(4), 283-306, 2002.
14. BALDERAS, T. and CUMPLIDO, R. An Efficient Hardware Implementation of the KASUMI Block Cipher for Third Generation Cellular Networks. *In: Proc. GSPx,* 2004.
15. DAEMEN, J. and RIJMEN, V. AES Proposal: Rijndael, Document version 2, 1999.
16. DEMIRKOL, A.Ş. Kaotik Osilatör Girişli Adc Tabanlı Rastgele Sayı Üreteci, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Basılmamış Yüksek Lisans Tezi, 2007.
17. DOHMEN J. R. and OLAUSSEN L. S. UMTS Authentication and Key Agreement. Graduate Thesis, Agder University College, Grimstad - Norway, 2001.
18. DUNKELMAN, O. KELLER, N. and SHAMİR, A. A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony. *Journal of Cryptology*, 824–849, 2014.
19. DUNKELMAN, O., KELLER, N. and SHAMIR, A. A practical-time attack on the KASUMI cryptosystem used in GSM and 3G telephony. *Crypto 2010*, LNCS 6223, pp. 393-410, 2010.
20. DUNKELMAN, O., KELLER, N. and SHAMIR, A. Improved Single-Key Attacks on 8-Round AES-192 and AES-256. *ASIACRYPT 2010:* 158-176, 2010.
21. FIPS 197. November 26, 2001 Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.
22. GROŠEK, O., VOJVODA, M. and KRCHNAV, R. A new matrix test for randomness. *Computing*, 85:21–36, 2009.
23. KAUL, V., BHARADI, V. A., CHOUDHARI, P., SHAH, D. and NARAYANKHEDKAR, S. K. Security Enhancement for Data Transmission in 3G/4G Networks, *International Conference on Computing Communication Control and Automation*, 2015.
24. KIM, C. H. Improved Differential Fault Analysis on AES Key Schedule. *IEEE Transactions on Information Forensics and Security*, 7(1), 2012.
25. KITSOS, P., GALANIS, M.D. and KOUFOPAVLOU, O. High-Speed Hardware Implementations of the Kasumi Block Cipher. *Circuits and Systems-ISCAS '04*, Vol 2. 549-52, 2004.
26. LU, J., DUNKELMAN, O., KELLER, N. and KIM, J. New impossible differential attacks on AES, *Indocrypt 2008*, LNCS 5365, 279-293, 2008.
27. NYBERG, K. Cryptographıc Algorithms for UMTS. *European Congress on Computational Methods in Applied Sciences and Engineering*, ECCOMAS 2004, 8-13, 2004.
28. PAYAL, V. N. GSM: Improvement of Authentication and Encryption Algorithms. *International Journal of Computer Science and Mobile Computing*, 3(7), 393-408, 2014.
29. SCHOINAS, P. Secure military communications on 3G, 4G and WiMax. Naval PostGraduate School, Monterey, California, Thesis, 2013.
30. TANAKA, H., SUGIO, N. and KANEKO, T. A Study on Higher Order Differential Cryptanalysis of 64 bit block cipher Kasumi. *Journal of the National Institute of Information and Communications Technology*, Vol.52, 129-134, 2005.
31. WANG, Z., DONG, X., JIA, K. and ZHAO, J. Differential Fault Attack on KASUMI Cipher Used in GSM Telephony. *Hindawi Publishing Corporation Mathematical Problems in Engineering*, Article ID 251853, 2014.

32. YALÇIN, M. E., SUYKENS, J. A. K. and VANDEWALLE, J. True Random Bit Generation From a Double-Scroll Attractor. *Circuits and Systems I: Regular Papers, IEEE Transactions on*, 51 Issue: 7, 1395 - 1404, 2004.

33. ZIBIDEH, W. Y. and MATALGAH, M. M. Modified Data Encryption Standard Encryption Algorithm with Improved Error Performance and Enhanced Security in Wireless Fading Channels. *Security and Communıcatıon Networks*, 565-573, 2015.

http://dergipark.ulakbim.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 17(1): 13-21, 2016
ISSN 2147–0308
Araştırma Makalesi / Research Article

SİBER GÜVENLİKTE LİSANSÜSTÜ EĞİTİM: DENİZ HARP OKULU ÖRNEĞİ

Mehmet Bilge Kağan ÖNAÇAN[1], Hasan ATAN[2]

[1] Deniz Harp Okulu, Bilgisayar Mühendisliği, İstanbul
konacan@dho.edu.tr
[2] İstanbul Şehir Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul
hasan.atan@outlook.com

Özet: İnternet kullanımının hayatın her alanında yaygınlaşmasına paralel olarak siber uzaydaki tehditlerin sayısında da artış gözlenmektedir. Kişi, kurum ve devletlerin siber uzaydaki saldırılardan maddi ve manevi etkilendiği ve zarara uğradığı görülmektedir. Bu tür zararlardan korunabilmek için siber güvenlik farkındalığının artırılması, bilgi ve bilinç seviyesinin yükseltilmesi gerekmektedir. Bunu başarmak için de hem son kullanıcıların bilgilendirilmesi ve bilinçlendirilmesini hem de siber güvenlik alanında nitelikli, uzman personel ihtiyacının karşılanmasını sağlayacak eğitim ihtiyacı ortaya çıkmaktadır. Bu çalışmada dünyadaki, ABD'deki ve Türkiye'deki Siber Güvenlik eğitimleri incelenmekte ve Deniz Harp Okulu (DHO)'ndaki Siber Güvenlik Yüksek Lisans Programı hakkında bilgi verilmektedir. Anılan programın siber güvenlik alanında özellikle uzman personel yetiştirilmesine önemli katkı sağlayacağı değerlendirilmektedir.

Anahtar Kelimeler: Siber Güvenlik Eğitimi, Siber Güvenlik Uzmanı, Siber Tehdit, DHO DEBİM, Müfredat.

Graduate Education in Cyber Security: The Case of Naval High School

Abstract: It is observed that an increase in the number of threats in cyber space in parallel with widespread usage of internet in all areas of life. It is seen that people, corporations and governments are being affected and suffered from the attacks on cyber space financially and morally. To be protected from cyber attacks, it is required to increase the level of knowledge, consciousness and awareness about cyber security. In order to manage this, the need of education for both the last users and the qualified specialists is arised. In this study, the cyber security educations in the World, USA and Turkey are analysed and information about cyber security master program in Turkish Naval Academy is given. It is evaluated that the mentioned program would provide the important contribution to educate especially the qualified specialists in the area of cyber security.

Keywords: Cyber Security Education, Cyber Security Specialist, Cyber Threats, DHO DEBIM, Curriculum.

GİRİŞ

Tüm dünyada internet kullanım oranı son yıllarda hızlı bir şekilde artmaktadır. Türkiye de internetin bu hızlı büyümesinden payını almıştır. Kişi başına düşen bilgisayar ve internet kullanım oranı dünyanın birçok ülkesi gibi Türkiye'de de hızla artmaktadır. Uzmanlar, sonraki dönemde de bu artışın devam edeceğini değerlendirmektedir.

İnternet kullanımının bu denli artması ve özellikle sosyal medya başta olmak üzere birçok internet platformlarında her türlü bilginin paylaşılıyor olması gizlilik, mahremiyet ve içeriği suç teşkil eden problemleri de beraberinde getirmektedir. Kaspersky Lab tarafından yürütülen "2013 Finansal Siber Tehditler" çalışmasına göre Türkiye özellikle finansal siber suçların oranının en fazla olduğu ülkeler arasında yer almaktadır (Kaspersky Lab, 10 Nisan 2014).

İnternet kullanımının ve internet platformlarında işlenen suçların gün geçtikçe artması, bilgi güvenliğine daha fazla önem verilmesini zorunlu kılmaktadır. Kişi, kurum ve devletlerin bu platformlarda işlenen her türlü illegal fiillerden maddi ve manevi etkilenmemesi için gereken önlemlerin alınması gerekmektedir. Bu önlemlerin başında hem son kullanıcıların siber güvenliğe ilişkin olarak bilgilendirilmesi ve bilinçlendirilmesi hem de siber güvenlik alanında nitelikli personel ihtiyacının karşılanması gelmektedir. Bunun için eğitime ve eğiticilere ihtiyaç duyulmaktadır. Türkiye'de bilgi teknolojilerine ilişkin eğitimler veren birçok eğitim programı bulunmakla birlikte siber suçlar konusunda derinleşmiş uzman sayısı sınırlıdır oysa siber suçlarla mücadele özel eğitim (Varol, 8-10 Aralık 2015:1) ve uzmanlaşmış eğiticiler gerektirmektedir.

Türkiye'de birçok kamu ve özel kurumun siber suçlarla mücadele için siber güvenlik alanında nitelikli personele ihtiyacı bulunmaktadır. Bu ihtiyacı karşılamaya yönelik son yıllarda hem üniversitelerde hem de özel eğitim kurumlarında eğitim programları hazırlanmakta ve verilmektedir. Bu kapsamda gerek Türk Silahlı Kuvvetlerinin gerekse ülkemizin diğer kurumlarının/firmalarının ihtiyaç duyabileceği nitelikli personel ihtiyacını karşılamak amacıyla 2015 yılında Deniz Harp Okulu (DHO)'nda Siber Güvenlik Yüksek Lisans programı açılmıştır. Söz konusu

programın yanı sıra, siber güvenliğe ilişkin farkındalığın artırılmasına yönelik faaliyetlere de devam edilmektedir.

Bu makalenin ikinci bölümünde siber uzay, siber tehdit, siber savaş ve siber güvenlik kavramları açıklanmış, üçüncü bölümünde siber güvenlikte eğitimin önemi ile dünyadaki, ABD'deki ve Türkiye'deki eğitim faaliyetleri anlatılmış, dördüncü bölümünde DHO'ndaki Siber Güvenlik Yüksek Lisans Programı hakkında detaylı bilgi verilerek siber güvenliğe ilişkin farkındalığın artırılmasına yönelik faaliyetler özetlenmiş, son bölümünde sonuç ve değerlendirmeler sunulmuştur.

SİBER GÜVENLİĞE İLİŞKİN TEMEL KAVRAMLAR

Tüm dünyada olduğu gibi Türkiye'de de bilgisayar ve internet kullanımı son yıllarda önemli ölçüde yaygınlaşmaktadır. TÜİK Hane halkı Bilişim Teknolojileri Kullanım Araştırması'na göre Türkiye'de 16-74 yaş grubundaki bireylerde bilgisayar ve internet kullanım oranları, 2014 yılında sırasıyla %53,5 ve %53,8 iken bu oranlar 2015 yılı Nisan ayında sırasıyla %54,8 ve %55,9 olmuştur (TÜİK, 2015) . Bunun yanında Türkiye'de internet kullanım oranlarının 4.5G teknolojisinin yaygınlaşması ile beraber daha da artacağı değerlendirilmektedir.

İnternet kullanımının her geçen gün artmasıyla birlikte bu ortamda her türlü bilgi paylaşılır olmuştur. Bilgi çağının en önemli gücünün bilginin kendisi olduğu göz önünde bulundurulursa bilgi casusluğu, siber korsanlık vb. yasadışı eylemlerde ve siber uzaydaki tehditlerde her geçen gün artış gözlemlenmektedir. Son dönemlerde ise siber savaşlar gündemden düşmemektedir. Çıkabilecek bir üçüncü dünya savaşının siber uzayda yaşanması ihtimali uluslararası politikayı da şekillendirmektedir (Bıçakçı, 2014: 103). Bu sebeple siber güvenlik konusunda gereken önlemleri almak ve olası zararlara karşı hazırlıklı olmak gerekmektedir.

Siber Uzay

Siber uzay, tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortamı (UDHB, 2016: 7) ifade etmektedir. En genel anlamda, insanların birbirine bağlı bilişim sistemleriyle etkileştiği ve birbirine bağlı bilişim sistemlerinin birbirleri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alan siber uzay olarak tanımlanmaktadır. Araştırmacılardan birçoğu sadece internet ortamına bu ismin verilmesinin uygun olduğunu düşünmektedir. Oysaki siber uzay bütün bilişim sistemlerini ve kullanıcıları içine alan bir evrendir (Bıçakçı, 2014: 106).

Günümüzde neredeyse tüm haberleşme, bilgisayarlar üzerinden siber uzayda gerçekleşmektedir. E-devlet uygulamalarında, enerji altyapılarında, ticari alanlarda, savunma sanayinde, finans sektöründe ve bunun gibi akla gelebilecek her türlü alanda bilgisayarlara, bilgisayar ağlarına ve uygulamalarına duyulan ihtiyaç günden güne artmakta ve bununla doğru orantılı olarak da siber uzay büyümekte ve paralelinde ise siber güvenliğin önemi gitgide artmaktadır. Kişi başı kullanılan internet cihazı sayısının eskiye nazaran bir hayli artması ve nesnelerin interneti (internet of things- IoT) kavramının da literatüre girmesiyle beraber önümüzdeki yıllarda internet kullanımının bir hayli artacağı tahmin edilmektedir. İnternet ağına yönelik ürünler geliştiren Cisco'nun tahminlerine göre hali hazırda kullanılmakta olan internete bağlı cihazlar ve önümüzdeki yıllarda bağlanacak olan cihazların toplamının 2020'li yıllarda 40 milyarı bulması beklenmektedir (Akın, 2015). Bunun sonucu olarak da insan sayısının yaklaşık yedi milyar olduğu dünyamızda kişi başına düşen internete bağlı cihaz sayısının ortalama altı olacağı değerlendirilmektedir. İnternete olan bağımlılığın bu denli hızla arttığı düşünüldüğünde yakın gelecekte kişisel mahremiyetin ve siber güvenliğin öneminin de hızlı bir şekilde artış göstereceği öngörülmektedir.

Siber Tehdit

Dünyanın en hızlı büyüyen ve en büyük siber güvenlik şirketlerinden biri olan Kaspersky Lab tarafından yapılan "2013 Finansal Siber Tehditler" çalışmasına göre siber suçluların, kişisel çevrimiçi hesaplara erişimi giderek artmaktadır. 2013 yılında, kötü amaçlı finansal yazılımların kullanıldığı siber saldırıların sayısı bir önceki yıla göre %27,6 artışla 28,4 milyona yükselmiştir. Türkiye, Afganistan, Bolivya, Peru, Kamerun, Moğolistan, Myanmar, ve Etiyopya'da yaşanan finansal siber suç vakaları toplam rakamın %12'sinden fazlasını oluşturmaktadır (Kaspersky Lab, 2014).

Siber uzayda yer alan her türlü bilgi, yazılımsal ve donanımsal kaynaklar gibi her türlü hizmet aracı bu ortamdaki varlıkları ifade etmektedir. Örneğin bir kurumdaki her personelin e-posta kullanıcı adı ve şifresi, o personele ait varlıkları ifade etmektedir. Siber uzayda yer alan her türlü insani ve yazılımsal açıklıklar vasıtasıyla varlıklara erişim, varlıkların niteliğinin değiştirilmesi, varlıklara zarar verilmesi vb. sağlayan etkenler ise "siber tehdit" olarak ifade edilmektedir. Sıklıkla karşılaşılan siber tehditlere örnek olarak servis dışı bırakma saldırıları (denial of service- DOS), virüs, solucan vb. zararlı yazılımlar, zararlı e-postalar ve yetkisiz erişim saldırıları verilmektedir (Bıçakçı, 2015; Güngör, 2015).

Söz konusu siber tehditlerin yıkıcı etkilerine karşı bireyler, kurumlar ve devletler tarafından alınabilecek bir takım önlemler bulunmaktadır (Öğün ve Kaya, 2013; Yılız, 2014; Bayoğlu, 2016). Bu önlemler kısaca aşağıdaki şekilde sıralanabilmektedir:

- Ulusal politika ve stratejiler geliştirilmeli ve gerekli yasal ortam oluşturulmalıdır (Yılmaz ve Sağıroğlu, 2013: 158).

- Kişisel mahremiyetin sağlanması maksadıyla kişilerde bilgi güvenliği farkındalığının arttırılması sağlanmalıdır (Yılmaz ve Sağıroğlu, 2013: 159). Bu amaçla özellikle ilköğretimde, internet ile çok hızlı bir şekilde tanışan çocuklara bilgi güvenliği farkındalığı kazandıracak dersler verilmelidir. Nitekim bilgisayarlar ve internet hayatın ayrılmaz bir parçası olmuş durumdadır ve "Z Nesli" olarak adlandırılan kuşak gelişen teknolojinin tesirinde büyümektedir.

- Ülkelerin siber savunmasını gerçekleştirebilmek amacıyla Siber Savunma Birimleri kurulmalı ve çalışma alanları belirlenmelidir.

- Her türlü yabancı yazılıma (buna işletim sistemleri de dahil) önyargı ile bakılmalı ve yerli yazılımların geliştirilmesi için gereken teknolojik hamleler gerçekleştirilmelidir (Türkay, 20 Nisan 2016).

- Siber Güvenlik için milli çözümler üretilmeli, eğitim ve koruma hizmeti verilmelidir (Türkay, 20 Nisan 2016). Kurumların network, sistem ve güvenlik altyapısında kullanılan güvenlik duvarları, saldırı tespit sistemleri, network cihazları vb. cihazların yazılım ve donanımları yerli imkanlarla geliştirilmelidir.

- Ülke çapında siber güvenlik tatbikatları yapılmalıdır (UDHB, 2013)

- Kişisel bilgisayarlarda yazılım güncellemelerinin yüklenmesi, anti-virüs uygulamalarının çalıştırılması vb. önlemler alınmalıdır (Bayoğlu, 2016).

- Ülkelerin siber güvenliğini sağlayabilecek nitelikli personel yetiştirilmesi amacıyla üniversitelerde siber güvenlik eğitimleri yaygınlaştırılmalı, siber güvenlik konusunda akademisyenler yetiştirilmelidir (UDHB, 2013).

Bu kapsamda Türkiye'de bu güne kadar gerçekleştirilen ve gerçekleştirilmeye devam edilen önemli faaliyetler şu şekilde sıralanabilir:

- TSK Siber Savunma Merkezi Başkanlığı kurulmuştur (2012) (Oğuz vd., 2015: 1-5).

- TUBİTAK Siber Güvenlik Enstitüsü kurulmuştur (2012) (Oğuz vd., 2015: 9).

- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı bünyesinde Siber Güvenlik Kurulu oluşturulmuştur (2012) (BTK, 2013: 6).

- Ulusal Siber Olaylara Müdahale Merkezi kurulmuştur (2013) (Bıçakçı vd., 2015: 14).

- Çeşitli kamu, özel ve sivil toplum kuruluşlarının ortaklaşa katkısıyla Siber Güvenlik tatbikatları düzenlenmiştir (2014) (Bıçakçı, 2014: 126).

- Ulusal Siber Güvenlik Stratejisi ve 2016-2019 Eylem Planı oluşturulmuştur (2016) (UDHB, 2016: 6).

- Çeşitli devlet ve özel üniversitelerde siber güvenlik bölümleri açılmıştır.

Siber Savaş

Siber savaş, bir devletin, başka bir devletin bilgisayar sistemlerine veya ağlarına hasar vermek ya da kesinti yaratmak üzere gerçekleştirdiği sızma faaliyetleridir (Mil, 2015: 400). Bir başka ifade ile siber savaş, bilgisayar ve iletişim teknolojisinin saldırı ve savunma amaçlı olarak kullanılmasıdır (Yayla, 2014: 182). Günümüzde savaşların sadece harp meydanlarında değil siber uzayda da gerçekleşiyor olması, olası 3. Dünya Savaşı'nın en önemli cephelerinden birinin siber cephe olacağı ihtimalini de güçlendirmektedir. Siber uzayda dünya çapında şu ana kadar gerçekleşen siber savaşlara; 2007 yılında Rusya-Estonya Siber Savaşı, 2008 yılında Rusya-Gürcistan Siber Savaşı, 2010 yılında Wikileaks belgelerinin internete sızdırılması, yine 2010 yılında İran nükleer çalışmalarını engellemeye yönelik üretilen Stuxnet Solucanı ve özellikle Google'a karşı düzenlenen Aurora saldırıları, 2012 yılında Türk Hava Yolları (THY)'na yönelik saldırılar, 2015 yılında Türkiye'nin Rusya'nın uçağını düşürmesi sonucu Türkiye-Rusya arasında gerçekleşen siber saldırılar örnek olarak gösterilebilir (Emre, 2012). Birçok ülke günümüzde yaşanan ve gelecekte de artacak olan siber tehditlere karşı kendisini müdafaa etmek amacıyla gerek istihbarat teşkilatları gerekse özerk kurum bünyelerinde siber güvenlik birimleri kurmakta ve bu alanda faaliyetlerini artırmaktadırlar.

Siber tehlikeler, siber saldırı ve siber savaşlarla sınırlı değildir. İşin mahremiyet ve hukuki boyutlarını da unutmamak gerekmektedir. İnsanların sanal ortamda rahat hareket edebilmesi, her türlü hakaret ve yorum yazabilmesi sonucunu doğurmuştur. Bunun ise çeşitli hukuki yaptırımları mevcuttur. Bunun yanında sosyal platformlarda herkese açık paylaşılan verilerin artması insanların mahrem bilgilerinin farkında olmadan saldırganların eline geçmesine sebep olabilmektedir. Bilgileri ele geçiren saldırganlar bu bilgilerle kişilere sosyal mühendislik saldırılarında bulunabilmektedirler. Bütün bunlara ek olarak özgür bir ortam sunduğu ve çok daha büyük bir kitleye ulaşabildiği gibi gerekçelerle internetin çeşitli platformlarında suç içerikli eylemler gerçekleştirilmektedir. Bu türden faaliyetler ise özellikle sansürsüz ve özgür internet sağladığı düşünülen Dark-Net (Tor-Network) bünyesinde gerçekleştirilmektedir. Dark-Net'in insanlara her türlü suçun rahatça işlenebileceği bir ortam sunduğu düşünülmektedir. Dark-Net bünyesinde; Firefox, Chrome, İnternet Explorer vb. tarayıcılarla erişilemeyen ve sadece Tor Tarayıcı ile erişim sağlanan, internetin gizli bir katmanı olarak düşünülebilir. Bünyesinde uyuşturucu ticareti, kor-

san yayıncılık, çocuk pornografisi, kiralık katil siteleri vb. aklınıza gelebilecek her türlü illegal içeriği barındırmakta ve bu türden illegal işlerin izlenemeden yapılabildiği bir ortam olduğu düşünülmektedir. Fakat The Dark Net kitabının yazarı Jamie Bartlett Eylül 2015 TEDTalks konferansında Dark-Net'in Amerikan Deniz Kuvvetleri'nin istihbarat projesi olarak geliştirildiğini ve sonradan yaygınlaştırıldığını söylemesi üzerine, Dark-Net üzerinden yapılan illegal işlerin izlenemediği düşüncesinin de yanlış olduğu kanaati ortaya çıkmıştır (Bartlett, 2015). Ayrıca bu iddia ABD'nin istihbarat çalışmaları kapsamında siber uzaya verdiği önemi de göstermektedir.

Diğer taraftan yeni geliştirilen teknolojinin ilk kullanıldığı alanlardan biri olan, bilginin ve hızlı karar almanın önem taşıdığı savaş ortamında bilgisayar ve iletişim teknolojileri yoğun olarak kullanılmaktadır. Günümüz savaş sahasında siber ortamın güvenliğini sağlamak, aynı zamanda bu alanı kullanarak düşmanın silah sistemlerini etkisiz hale getirmek için devletler önemli çalışmalar yürütmektedirler (Yayla, 2014: 182). Savaş harekat ortamında kullanılan savaş yönetim sistemleri ve sensör sistemleri çoğunlukla ileri teknoloji ürünü elektronik sistemlerdir. Siber saldırılara açık olan söz konusu sistemlerin siber saldırıya maruz kalma olasılığı yüksektir. Bu sebeple anılan sistemlerin kullanıcısı ve yöneticisi olan Silahlı Kuvvetler personelinin siber güvenliğe ilişkin bilgi ve bilinç seviyesinin yüksek olması gerekmektedir.

Görülüyor ki internetin bu denli yaygınlaşması her türlü, söz ve fiilin siber uzayda rahatça gerçekleştirilmesine, mahremiyet içeren bilgilerin elden ele dolaşmasına, suç içerikli eylemlerin daha rahat gerçekleştirilmesine sebep olmaktadır. Bütün bunlar ise siber güvenlik, siber hukuk, bilgi güvenliği farkındalığı ve siber uzayda mahremiyet gibi konuların gitgide önem kazanmasına vesile olmaktadır. Bu konularda gerekli önlemlerin alınması ve yatırımların yapılması gerek kişilerin ve kurumların, gerekse devletlerin geleceği açısından önemlidir.

Siber Güvenlik

Siber Uzay'ın her geçen gün büyümesi ve her türlü siber tehdide açık olması siber ortamda güvenliğin önemini arttırmaktadır. Siber güvenlik, siber ortamı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen bilginin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmalarının devreye alınmasını ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesini ifade etmektedir (UDHB, 2016). Siber güvenlik ifadesi ilk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için kullanılmıştır (Öğün ve Kaya, 2013: 163).

Siber güvenlik kavramı açıklanırken, sıklıkla birlikte bahsedildiği ve zaman zaman da karıştırıldığı bilgi güvencesi (information assurance), bilgisayar güvenliği (computer security) ve bilgi güvenliği (information security) kavramlarına burada değinmenin faydalı olacağı değerlendirilmektedir. Bilgi güvencesi, siber güvenliği; siber güvenlik de bilgisayar güvenliğini kapsayan kavramlardır. Bilgi güvencesi; bilginin ve bilgi sistemlerinin gizliliğini, kontrolünü, bütünlüğünü, doğruluğunu, hazır bulunurluğunu ve işe yararlılığını sağlayacak şekilde tasarlanan teknik ve yönetimsel kontroller kümesidir. Bilgisayar güvenliği ise bilgisayarın üzerindeki bilgi sistem varlıklarının ve bilginin gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlayan önlemler ve kontrollerdir (McGettrick, 2013: 11-14). Bilgi güvenliği, bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden korunma veya bilgilere yapılacak olan izinsiz erişimleri engelleme işlemidir ("Bilgi Güvenliği", 2016). Bilgi güvencesinde, bilgi sistemindeki bilgi güvenliğini sağlamak için gerekli olan teknik ve süreçsel gereksinimler daha stratejik düzeyde ele alınırken bilgi güvenliği kavramı ise daha taktik düzeyde bir anlam içermektedir (Güngör, 2015: 10).

Ülkeler arasındaki siber savaşlar, kişisel mahremiyeti alt üst eden casus yazılım ve sosyal platformlar, ticaret hacminin önemli bir oranının internet üzerinden dönmesi, hastane/eczane vb. her türlü tıbbi ortamın verilerinin internette yer alması, endüstriyel alanda birçok hizmetin internet üzerinden dönmesi, enerji altyapılarında bilgisayar ve SCADA sistemlerine olan bağımlılık, kısacası hayatımızın her safhasında bilgisayarların ve bilgisayar altyapılarının yer alması bizi yaşadığımız yüzyılda en büyük ekonomik ve güvenlik tehditlerinin siber uzayda gerçekleşeceği sonucuna ulaştırmaktadır. Siber uzayda yaşanacak bu nevi tehditler siber güvenliğin ve siber güvenlik eğitiminin önemini her geçen gün artıracaktır.

SİBER GÜVENLİK EĞİTİMİ

Teknoloji çağında bilgisayarlar, akıllı telefon ve uygulamaları, sosyal medya gibi hayatı kolaylaştıran her türlü gelişme beraberinde güvenlik ve mahremiyet problemlerini de getirmiştir. Bu problemler sadece bireyleri değil, yeri geldiği zaman tüm toplumu ve ulusal güvenliği tehdit eder boyutlara kadar ulaşabilmekte, bireylere, topluma ve devlete maddi ve manevi zararlar verebilmektedir. Bilgi toplumunun yaşadığı bu problemleri minimize etmek amacı ile her bireyin ve kurumun bilgi güvenliği farkındalığının artırılması gerekmektedir. Söz konusu farkındalığı sağlayabilmenin, siber tehditler ve bu tehditler neticesinde oluşan problemleri önlemenin veya en azından etkisini azaltmanın en etkin yollarından biri de eğitimdir. Gerek bireysel olarak bireyin kendisini

gerekse kurumsal olarak kurum personelini siber güvenlik konusunda eğitmek ve güncel bilgilerle donatmak artık kaçınılmaz hale gelmiştir (Öğün ve Kaya, 2013:173).

Diğer taraftan hem siber güvenlik eğitimlerini verebilecek hem de siber tehlikelerle mücadele edebilecek ve siber savaşlarda etkin rol alabilecek nitelikli personel ihtiyacı ortaya çıkmıştır. Bu bağlamda çeşitli özel eğitim kurumlarında ve üniversitelerde bu konu teknik ve sosyal boyutları ile birlikte işlenmeye, tartışılmaya ve araştırılmaya başlamıştır. Ülkemizde bu konuda kişisel ve kurumsal eğitim veren özel kurumlar bulunmakla beraber son yıllarda ihtiyaç duyulan nitelikli eleman sayısını arttırmak ve siber dünyada doğabilecek tehditlere çözümler sunabilmek amacıyla çeşitli özel ve devlet üniversitelerinde de Siber Güvenlik üzerine çalışmalar yoğunlaşmıştır.

Bilgisayar eğitimcileri, bilgisayar araştırmacıları ve profesyonellerinin alandaki zorluklar, yenilikler ve eğitim müfredatlarına ilişkin düşüncelerini paylaştıkları, bilgisayar bilimleri alanındaki en eski ve en geniş mesleki kuruluş olan (ACM Digital Library, 2016) Hesaplama Makineleri Derneği (Association for Computing Machinery), kısaca ACM'nin 2013 yılında hazırlamış olduğu "Siber Güvenlik Eğitim ve Öğretimi için Müfredat Kılavuzu"nda siber güvenlik dersine ilişkin müfredatın ana konuları/bilgi alanları;

- Adli bilişim (digital forensics)
- Penetrasyon testleri (penetration testing)
- e-Kanıt (e-evidence)
- Hudut savunma (perimeter defense)
- Güvenli yazılım geliştirme ve yazılım güvenliği (secure coding and software security)
- Güvenlik yönetimi (management of security)

olarak belirlenmiştir (McGettrick, 2013: 14). Bilgi güvenliği alanına odaklanmış bir araştırma firması olan Securosis ise "bilgi güvenliği"ni;

- Ağ güvenliği (network security)
- Uç/son nokta/kullanıcı güvenliği (endpoint security)
- Veri güvenliği (data security)
- Uygulama güvenliği (application security)
- Kimlik ve erişim yönetimi (identity and access management)
- Güvenlik yönetimi (security management)
- Sanallaştırma ve bulut (virtualization and cloud)

olarak yedi alt kategoriye ayırmış ve ardından bu kategorileri 32 alt başlığa bölmüştür (Securosis.com, 2016).

Kessler ve Ramsay (2014), Milli Güvenlik programı için yapmış oldukları siber güvenlik eğitimi müfredat önerisinde; "Bilgi Güvenliğinin Temelleri", "Bilgisayar ve Ağ Teknolojileri", "Bilgi Güvenliği Araçları ve Teknikleri", "Adli Bilişime Giriş", "Siber Suç ve Siber Hukuk" ve "Siber Uzayda Savaş, Terörizm ve Diplomasi" olmak üzere altı temel ders belirlemişlerdir.

Dünyadaki ve ABD'deki Siber Güvenlik Eğitim Faaliyetleri

Siber uzayda yaşanan vakaların ve siber tehditlerin her geçen gün artması tüm dünya ülkelerini olumsuz etkilemektedir. Yaşanan olumsuzlukları asgariye indirgeyebilmek için ise nitelikli personel ihtiyacının karşılanması gerekmektedir. Bu amaçla dünyanın çeşitli bölgelerinde birçok ülke üniversiteler bünyesinde siber güvenlik eğitimi vermektedirler. Bu ülkeler ve üniversitelere Estonya'da Tallinn University of Technology, Avustralya'da Edith Cowan University, İskoçya'da Edinburgh Napier University, Hollanda'da 3TU (Dutch Technical Universities – TU Delft, TU Eindhoven, University of Twente), Hindistan'da Amrita Vishwa Vidyapeetham, İngiltere'de City University of Londan, De Montfort University, University of York örnek olarak sıralanabilir. Dünyada siber güvenlik alanında yüksek lisans düzeyinde eğitim veren bu üniversitelerin geniş bir listesine Wikipedia Master of Science in Cyber Security (https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security) başlığı altında erişilebilmektedir.

Bunların dışında ABD'de de çok sayıda kamu ve özel üniversitelerde siber güvenlik alanında eğitimler verilmektedir. 2014 yılında HP Enterprise Security sponsorluğunda Ponemon Institute tarafından yapılan "Siber Güvenlik için En İyi Okullar- Best Schools for Cybersecurity" araştırmasına göre ABD'de siber güvenlik alanında eğitim veren en iyi üniversiteler;

- University of Texas, San Antonio,
- Norwich University,
- Missisipi State University,
- Syracuse University,
- Carnegie Mellon University,
- Purdue University,
- University of Southern California,
- University of Pittsburgh,
- George Mason University,
- West Chester University of Pennsylvania,

- U.S. Military Academy, West Point,
- University of Washington

olarak gösterilmektedir. Araştırma yapılırken dikkate alınan kriterler ise akademik mükemmellik, uygulama imkanları, fakültenin tecrübe ve uzmanlığı, öğrenci ve mezunların altyapı ve tecrübesi, üniversite siber güvenlik komitesinin alandaki itibarı olarak sıralanabilir (Ponemon Institute, 2014).

Bunların dışında açık kaynaklardan yapılan araştırmalar sonucu özellikle ABD Harp Okulları incelendiğinde, ABD Deniz Harp Okulu'nda Siber Harekat (Cyber Operations) Ana Bilim Dalı'nın kurulduğu, diğer Harp Okullarında siber güvenlik kapsamında bölüm bulunmadığı görülmektedir. ABD'deki tüm Harp Okullarında öğrencilerin oluşturduğu çalışma gruplarının mevcut araştırma merkezlerinden yararlanarak Siber Harekat kapsamında araştırma ve proje çalışmaları yapmaları teşvik edilmektedir. Ayrıca ABD Deniz Harp Okulu'nda birinci sınıfta tüm öğrencilere siber güvenlik dersi verilmekte olduğu, her yarıyıl konferanslar yapıldığı ve sınavlara iştirak edildiği bilinmektedir.

ABD'deki tüm üniversiteler siber güvenlik alanında artan personel ihtiyacını karşılamak maksadıyla genel olarak lisansüstü ve sertifikasyon programları ile iyi eğitimli mezunlar yetiştirmeyi amaçlamaktadır. Sertifika ve lisansüstü programların yanında Maryland Üniversitesi gibi bazı üniversitelerin siber güvenlik lisans programı da bulunmaktadır ("Cybersecurity Education at UMD", 2016).

Türkiye'de Siber Güvenlik Eğitim Faaliyetleri

Siber tehditlerin günden güne artması siber güvenlik uzmanlarına duyulan ihtiyacı da günden güne artırmaktadır. Bu konuda ihtiyaç duyulan nitelikli personelin yetiştirilmesi maksadıyla ülkemizde çeşitli üniversiteler siber güvenlik alanında eğitim vermeye başlamışlardır. Henüz lisans düzeyinde ülkemizde bu eğitim verilmese de doktora ve yüksek lisans düzeyinde eğitimler verilmektedir. Araştırmacılar tarafından;

- Doktora derecelerinin, gelecek nesil siber güvenlik eğitimi ve akademik araştırmalarını desteklemekle birlikte endüstri ve devlet kurumları için ihtiyaç duyulan ileri derecede uzmanlığı ve liderliği sağlayacağı;
- Yüksek lisans derecelerinin ise, gelişmiş yeteneklere sahip siber güvenlik işgücü sağlamak için esas teşkil ettiği, bilgisayar biliminde veya ilişkili bir alanda yapılan sağlam bir lisans derecesi üzerine inşa edilen, iki yıllık ek eğitimin, siber güvenliğe ilişkin ileri konularda özel bilgi, beceri ve yetenek sağlayacağı ifade edilerek üniversitelerin bilgisayar profesyonelleri için, hukuk, işletme, ekonomi vb. toplumsal konular için ve siber güvenlik operasyonları için yüksek lisans programları açması gerektiğine vurgu yapılmaktadır (McGettrick, 2013: 2-3).

Bu kapsamda Siber Güvenlik alanında ülkemizde eğitim veren üniversiteler ve ilgili programlardan bazıları şu şekilde listelenebilir:

- DHO Deniz Bilimleri ve Mühendisliği Enstitüsü (DEBİM)'nde Siber Güvenlik Yüksek Lisans Programı
- Hava Harp Okulu Havacılık ve Uzay Teknolojileri Enstitüsü (HUTEN)'nde Siber Güvenlik Yüksek Lisans programı
- TÜBİTAK'ın üniversiteler ile siber güvenlik konusunda eğitim programları yürüttüğü; BİLGEM ve Şehir Üniversitesi ortaklığı çerçevesinde, Şehir Üniversitesi Fen Bilimleri Enstitüsünde Bilgi Güvenliği Mühendisliği yüksek lisans (tezli ve tezsiz) programı,
- MEDİPOL Üniversitesinde Elektrik, Elektronik ve Siber Sistemler Doktora programı,
- Yaşar Üniversitesi Fen Bilimleri Enstitüsünde Bilgisayar Mühendisliği Ana Bilim Dalı altında Siber Güvenlik Yüksek Lisans programı
- Gazi Üniversitesi Fen Bilimleri Enstitüsünde Bilgi Güvenliği Mühendisliği Yüksek Lisans ve Doktora Programları
- İstanbul Teknik Üniversitesinde Bilgi Güvenliği Mühendisliği ve Kriptoloji Yüksek Lisans ve Doktora programları,
- Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsünde Siber Güvenlik Yüksek Lisans programı
- Gebze Teknik Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Siber Güvenlik Yüksek Lisans programı

Bunun yanında internetin yaygınlaşması ile beraber bilişim suçlarında (TBMM BİAK, 2013) ve dolayısıyla adli bilişim vakalarında artış gözlemlenmektedir. Adli Bilişim denildiğinde, internet ortamında daha genel bir ifade ile siber uzayda işlenebilen suçlarla mücadele ve bilgi güvenliği üzerine çalışmaların yapıldığı durumlar kastedilmektedir (Varol vd., 2013). Bu türden vakalar ile mücadele için gerekli uzmanların yetişmesi amacıyla ülkemizde çeşitli eğitim kurumları Adli Bilişim eğitimi vermektedir. Varol'un (2013) çalışmasında Adli Bilişim alanında ülkemizde eğitim veren kurumlar aşağıdaki şekilde listelenmiştir:

- Polis Akademisi Güvenlik Bilimleri Fakültesi/Enstitüsü
- Gazi Üniversitesi Bilişim Enstitüsü Adli Bilişim Anabilim Dalı
- Mustafa Kemal Üniversitesi Bilişim Teknolojisi Yüksekokulu
- Hacettepe Üniversitesi Adli Bilişim Araştırma ve Uygulama Merkezi

- Fırat Üniversitesi Adli Bilişim Mühendisliği Bölümü

Yakın gelecekte daha yoğun olarak karşılaşılması muhtemel siber savaşlar göz önünde bulundurulduğunda Türk Silahlı Kuvvetleri (TSK) personelinin Siber Güvenlik alanındaki yetişmiş insan gücü ihtiyacının karşılanması gerekmektedir. Bu kapsamdaSiber Güvenlik uzmanlarının yetiştirilmesi maksadıyla, detayları sonraki bölümde açıklanmış olan, DHO'nda açılan Siber Güvenlik Yüksek Lisans Programı, 2015-2016 Eğitim ve Öğretim yılında eğitime başlamıştır.

DHO SİBER GÜVENLİK YÜKSEK LİSANS PROGRAMI

DHO Bilgisayar Mühendisliği Bölüm Başkanlığı altında açılan ve 2015-2016 Eğitim ve Öğretim yılında eğitime başlayan Siber Güvenlik Yüksek Lisans Programının (tezli), öncelikle deniz harekat ortamında siber saldırıya açık olan savaş yönetim sistemleri ve sensör sistemlerinin kullanıcısı ve yöneticisi olan Deniz Kuvvetleri Komutanlığı (Dz.K.K.lığı) personelinin siber güvenlik konusunda bilgilenmesi, bilinçlenmesi ve uzmanlaşmasını sağlamak olmak üzere Türkiye'de Siber Güvenlik alanında nitelikli personel yetiştirilmesi sürecine katkı sağlamayı amaçlamaktadır. DHO Siber Güvenlik Yüksek Lisans programında bu amacı gerçekleştirmek maksadıyla;

- ACM'nin belirlemiş olduğu siber güvenlik dersi müfredatı ana konuları,
- A.B.D. Deniz Kuvvetleri Lisansüstü Okulu (Naval Post Graduate School)'nda verilen yüksek lisans ve sertifika programları,
- TÜBİTAK ile siber güvenlik eğitimi kapsamında işbirliği yapan üniversitelerin programları,
- TSK'daki konu ile ilgili otoritelerin öngörüleri,
- Halihazırda DHO'nda görevli öğretim üyelerinin uzmanlık alanları göz önünde bulundurularak güncel yaklaşımlara uygun bir müfredat oluşturulmuştur. Bu kapsamda verilmekte olan dersler Tablo 1'de sunulmuştur.

Programa Öğrenci Kabulü

Programa 2015-2016 Eğitim ve Öğretim yılında bir asker öğrenci kabul edilmiştir. 2016-2017 Eğitim ve Öğretim yılından itibaren programa, Harp Okulları ve Üniversitelerin Bilgisayar Mühendisliği lisans programlarından mezun olmuş hem asker hem de sivil öğrenciler kabul edilecektir. Başvuru koşulları ve tarihi ile kontenjanlar DHO resmi örün (web) sayfasından duyurul(acak/makta)dır.

Tablo 1. DHO DEBİM Siber Güvenlik Yüksek Lisans Ders Programı

DERS İSİMLERİ	DERS SAATİ (Ders + Laboratuvar)	DERS DÖNEMİ
Bilgi Sistemleri Güvenliği	2+2	1
Bilgisayar Ağları ve Haberleşme Güvenliği	2+2	1
Bilgi Yönetimi ve Güvenlik Politikaları	2+2	1
Güvenli Yazılım Geliştirme	2+2	1
Seminer	3+0	1
Zararlı Yazılımlar	2+2	2
Kablosuz Ağ Güvenliği	2+2	2
Adli Bilişim	2+2	2
Siber Güvenlik için Veri Madenciliği Uygulamaları	2+2	2
Yüksek Lisans Tezi	1+0	3 ve 4

Derslerin Yürütülmesi

Dersler, DEBİM dershanelerinde ve DHO bünyesinde kurulmuş olan Siber Güvenlik Laboratuvarında işlenmektedir. Diğer taraftan Gebze Teknik Üniversitesi ile yapılan işbirliği protokolü gereği, anılan üniversitenin Bilgisayar Mühendisliği Bölüm Başkanlığı bünyesinde açılan Siber Güvenlik Programı'ndan da dersler alınabilmektedir. Görülen lüzum üzerine Türkiye'de Siber Güvenlik alanında uzmanlığı ve derinliği olan doktoralı personel ve/veya akademik personelin de Siber Güvenlik Yüksek Lisans programı kapsamında DEBİM'de ders vermesi sağlanmaktadır.

DHO'nda Siber Güvenliğe İlişkin Faaliyetler ve Hedefler

DHO'nun stratejik planında "siber güvenlik alanında Türkiye'de marka olmak" hedefi yer almaktadır. Bu kapsamda okulda; öğrenciler ve personelin siber güvenliğe ilişkin farkındalığını artırmak maksadıyla faaliyetler düzenlenmektedir. Bu faaliyetler arasında; tüm öğrencilere zorunlu siber güvenlik dersi verilmesi, siber güvenlik alanında derinleşmiş uzmanlar tarafından konferanslar sunulması, okuldaki uygun mahallere afişler asılması, uzaktan eğitim dersleri açılarak çevrimiçi sınavlar uygulanması, e-postalar ile bilgilendirmeler yapılması, öğrenci ve öğretim elemanlarının siber güvenliğe yönelik seminer/ konferans/ sempozyum/ yarışmalara katılımının teşvik edilmesi, savunma sanayi firmaları ve/veya üniversiteler ile koordineli seminer/ konferans/ sempozyum planlanması vb. sayılabilmektedir. Diğer taraftan okuldaki öğretim elemanları, konuya ilişkin

uzmanlıklarının/derinliklerinin artırılması maksadıyla, yurtiçi ve yurtdışı eğitim imkanlarından yararlandırılmaktadır. Ayrıca, Dz.K.K. lığı'nın siber güvenlik alanında yetişmiş personel ihtiyacını karşılamak maksadıyla Bilgisayar Mühendisliği Bölüm Başkanlığı altında Siber Güvenlik Ana Bilim Dalı kapsamında 2018-2019 Eğitim ve Öğretim yılından itibaren lisans seviyesinde Siber Güvenlik eğitimi verilmesi planlanmaktadır.

SONUÇ

Siber uzayın gitgide büyümesi varlıklar üzerindeki siber tehditleri, mahremiyet problemlerini ve siber hukukun önemini artırmaktadır. Her geçen gün siber uzaya yeni varlıklar eklenmekte ve bu varlıklar hayatımızın ayrılmaz bir parçası haline gelmektedir. Siber varlıkların insan hayatına getirdiği yeniliklerin bilinçsiz kullanılması ve kullanım sırasında yeterli ölçüde önlemlerin alınmaması insanın bu teknolojiden önemli oranda zarar görmesine yol açabilmektedir. İnsanların karşılaşabileceği teknolojik zararları asgariye indirgeyebilmek için ise bir takım önlemlerin alınması gerekmektedir.

Devlet bazında, kurumsal ve kişisel bazda alınabilecek önlem silsilesinin en büyük ayağını teknolojinin bilinçli kullanılması ve nitelikli personel yetiştirilmesi oluşturmaktadır. Bunları sağlamak için ise özellikle örgün eğitim kurumlarında, gelişen teknoloji ve güncel siber tehditleri de ihtiva eden bir müfredat ile eğitim faaliyetleri düzenlenmelidir. Bu tür çalışmaların gerçekleştirilmesi amacıyla dünyada ve ülkemizde son yıllarda birçok üniversitede ilgili bölümler açılmaktadır.

Bu kapsamda DHO Bilgisayar Mühendisliği bünyesinde açılan Siber Güvenlik Yüksek Lisans Programı Deniz Kuvvetlerinin ihtiyaç duyduğu nitelikli siber güvenlik personelinin yetiştirilmesi için gerekli öğretim elemanı ve altyapı ihtiyaçlarını bünyesinde barındırmaktadır. Bilgi güvenliğinin önemi nin nesnelerin interneti (Internet of Things-IoT) gibi teknolojilerin yaygınlaşmasıyla daha da artacağı göz önünde bulundurulduğunda DHO ve diğer üniversiteler bünyesinde açılan siber güvenliğe yönelik bölümlerin gelecekte de artacak olan nitelikli siber güvenlik personeli ihtiyacını karşılama noktasında önemli bir görev üstlenmekte olduğu değerlendirilmektedir.

KAYNAKLAR

1. ACM Digital Library, http://lib.baskent.edu.tr/ACM Tanıtım Dokumani.pdf, (Erişim Tarihi: 29.05.2016).
2. AKIN, A., (21 Kasım 2015), "Siber Savaş ve Siber Güvenlik Nedir?", http://www.stratejikanaliz.com/analizler/harp-ve-strateji/siber-savas-ve-siber-guvenlik-nedir/#axzz3wUUj1An8, (Erişim Tarihi: 10.05.2016).
3. BARTLETT, J., (2015), "How the mysterious dark net is going mainstream", https://www.ted.com/talks/jamie_bartlett_how_the_mysterious_dark_net_is_going_mainstream?language=en, (Erişim Tarihi: 29.04.2016).
4. BAYOĞLU, B., (2016). "Kişisel Bilgisayarlar İçin Temel Güvenlik Adımları", TÜBİTAK Ulusal Bilgi Güvenliği Kapısı, http://www.bilgiguvenligi.gov.tr/son-kullanici-kategorisi/kisisel-bilgisayarlar-icin-temel-guvenlik-adimlari.html, (Erişim Tarihi: 19.06.2016).
5. BIÇAKÇI, S., (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, ss. 101-130.
6. BIÇAKÇI, S., Ergün, D. ve Çelikpala, M., (2015), "Türkiye'de Siber Güvenlik", *EDAM Siber Politika Kağıtları Serisi 2015/1*, ss.1-35.
7. Bilgi Güvenliği, (2016), https://tr.wikipedia.org/wiki/Bilgi_güvenliği, (Erişim Tarihi: 29.05.2016).
8. Cybersecurity Education at UMD, Maryland Cybersecurity Center, http://www.cyber.umd.edu/education, (Erişim Tarihi: 02.06.2016).
9. EMRE, B., (2016), "Siber Savaşlar: 5.Boyutta Savaş", http://www.siberguvenlik.org.tr/2013/01/siber-savaslar-5-boyutta-savas.html, (Erişim Tarihi: 03.05.2016).
10. GÜNGÖR, M., (2015), Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı Uzmanlık Tezi.
11. Kaspersky Lab., (2014), "28 milyon finansal siber saldırının çoğu Türkiye'de", http://www.kaspersky.com/tr/about/news/virus/2014/28-milyon-finansal-siber-saldirinin-cogu-Turkiyede, (Erişim Tarihi: 13.05.2016).
12. KESSLER, G.C. ve RAMSAY, J.D., (2014), "A Proposed Curriculum in Cybersecurity Education Targeting Homeland Security Students", *47th Hawaii International Conference on System Science*.
13. Master of Science in Cyber Security, (2016), https://en.wikipedia.org/wiki/Master_of_Science_in_Cyber_Security, (Erişim Tarihi: 02.06.2016).
14. MCGETTRICK, A., (30 Ağustos 2013), "Toward Curricular Guidelines for Cybersecurity Education and Training: Report of a Workshop on Cybersecurity Education and Training", https://www.acm.org/education/TowardCurricularGuidelinesCybersec.pdf , (Erişim Tarihi: 29.05.2016).

15. MİL, H.İ., (2015), Sosyal Güvenlik Kurumundaki Siber Güvenlik Yönetimi Uygulamalarının İncelenmesi ve Değerlendirilmesi, *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, Nisan 2015, Yıl: 7, Sayı: 13, ss. 398-416.

16. OĞUZ, S., CEYHAN, E.B. ve SAĞIROĞLU, Ş., (2015), "Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler", http://iscturkey2016.org/wp-content/uploads/2016/03/paper.pdf, (Erişim Tarihi: 02.05.2016).

17. ÖĞÜN, M.N. ve KAYA, A., (2013), "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri*, Sayı 18, ss.163-173.

18. Ponemon Institute, (2014), "Best Schools for Cybersecurity Research Report" , http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf, (Erişim Tarihi: 04.06.2016).

19. Scada, https://tr.wikipedia.org/wiki/ SCADA, (Erişim Tarihi: 19.06.2016).

20. Securosis.com'dan aktaran PEKEN, M.M., (2015), "Bilgi Güvenliği Nedir ve Nasıl Sınıflandırılır?", https://www.sibergah.com/genel/bilgi-guvenligi-nedir-ve-nasil-siniflandirilir, (Erişim Tarihi: 29.05.2016)

21. TBMM Bilişim ve İnternet Araştırma Komisyonu (BİAK) Raporu, (2013), http://www.biakraporu.org, (Erişim Tarihi: 06.05.2016).

22. TÜRKAY, İ., (20 Nisan 2016), "Kamu Bilişim Zirvesi 2016'nın Değerlendirilmesi", http://www.vergialgi.net/ekonomi-maliye/kamu-bilisim-zirvesi-2016-nin-degerlendirilmesi, (Erişim Tarihi: 20.04.2016).

23. Türkiye İstatistik Kurumu, (2015), "Hanehalkı Bilişim Teknolojileri Kullanım Araştırması", http://www.tuik.gov.tr/PreHaberBultenleri.do?id=18660, (Erişim Tarihi:15.05.2016).

24. UDHB, (2013), Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, https://www.btk.gov.tr/File/?path=ROOT%2f1%2fDocuments%2fSayfalar%2fBTDNewFolder%2fSiber+G%C3%BCvenlik%2f2_1_Strateji+Eylem+Plan%C4%B1+2013-2014.pdf, (Erişim Tarihi: 19.06.2016).

25. UDHB, (2016), 2016-2019 Ulusal Siber Güvenlik Stratejisi, T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı, http://www.udhb.gov.tr/doc/ siberg/2016-2019guvenlik.pdf, (Erişim Tarihi: 04.05.2016).

26. VAROL, A., (8-10 Aralık 2015), "Türkiye'de Adli Bilişim Eğitimi ve Denetimli Serbestlik Uygulamaları", *Türkiye'de Denetimli Serbestlik 10. Yıl Sempozyumu*, ss.1-13, İstanbul.

27. VAROL, C., Cooper, P.A. ve Varol, A., (20-21 Mayıs 2013), "Türkiye'de Adli Bilişim Eğitimi", *1st International Symposium on Digital Forensics and Security (ISDFS'13)*, Elazığ.

28. YILDIZ, M., (2014), Siber Suçlar ve Kurum Güvenliği, T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı Uzmanlık Tezi, Kasım 2014, http://www.udhb.gov.tr/images/hizlierisim/efcecbe1f21e9fe.pdf, (Erişim Tarihi: 19.06.2016).

29. YILMAZ, S. ve Sağıroğlu, Ş., (2013), "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri", *6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, ss.158-166, Ankara.

http://dergipark.ulakbim.gov.tr/tujes
Trakya University Journal of Engineering Sciences, 17(1): 23-34, 2016
ISSN 2147–0308
Araştırma Makalesi / Research Article

EDİRNE BABA DEMİRTAŞ (TİMURTAŞ) MAHALLESİ GELENEKSEL KONUTLARI: MİMARİ ÖZELLİKLERİ, POTANSİYELLERİ VE SORUNLARI

Arif MISIRLI[1], Esin BENİAN[2]
[1,2]Trakya Üniversitesi, Mimarlık Fakültesi, Mimarlık Bölümü, Edirne, Türkiye
esinbenian@yahoo.com.tr

Özet: Edirne'nin Osmanlılar tarafından fethedilmesinden sonra, yerleşmenin yoğun olduğu Kaleiçi bölgesi dışında yeni mahalleler oluşturulmaya başlanmıştır. Dönemin ileri gelenleri tarafından kurulan bu mahallelerden biri de Baba Demirtaş Mahallesi'dir. Kentsel sit sınırları içerisindeki mahalle, Edirne kent merkezinin ve Kaleiçi'nin yakınında konumlanmakta; dünya mirası Selimiye Camii ve Külliyesi'nin de geçiş ve etkileşim bölgesi sınırlarında yer almaktadır. Organik dokuya sahip mahalle, konumu dışında, Osmanlı dönemi kale dışı yerleşmelerine örnek teşkil etmesi ve bünyesinde anıtsal nitelikli tarihi yapılar ile geleneksel konutları barındırması açısından da önem taşımaktadır. Ancak zamanla kentleşme, trafik, kullanıcı değişmesi, bilinçsiz kullanım, denetimsiz yapılaşma gibi faktörler dokunun bozulmasına ve geleneksel konutların azalmasına neden olmuştur. Oysaki kültürel kimliği sergilemek adına geleneksel dokuların ve konutların korunarak günlük yaşama katılmaları sağlanabilir. Özellikle Selimiye Camii ve Külliyesi gibi dünya mirası bir yapının yaşatılması ve sergilenmesinde çevresiyle birlikte ele alınmış olduğu göz önünde bulundurulduğunda, mahalledeki tarihi ve geleneksel yapılar da önem kazanmaktadır. Mahallenin ve mevcut geleneksel konutların önemine dikkat çekmek üzere hazırlanan bu çalışmada, mahalle sınırları içinde bulunan geleneksel konutların mimari özellikleri incelenmiş; potansiyelleri ve sorunları tespit edilmiştir.

Anahtar Kelimeler: Edirne, Baba Demirtaş Mahallesi, geleneksel konut mimarisi.

The Traditional Houses of Edirne Baba Demirtaş (Timurtaş) District: Its Architectural Characteristics, Potentials and Problems

Abstract: After the conquest of Edirne by the Ottomans, new districts have been established around the Kaleiçi district where settlement was heavily populated. One of the districts set up by the notables of the era is Baba Demirtaş district. This district which is within the urban conservation boundaries, is located within the vicinity of Edirne town center and Kaleiçi district and stands in the boundaries of transition and interaction zones of world heritage Selimiye Mosque Complex. With its organic structure, in addition to its location, it is important because it is an example of a settlement outside the fortress in the Ottoman period and hosts monumental historical buildings and traditional houses. In the course of time, factors such as urbanization, traffic, change of users, unconscious utilization and uncontrolled structuring has resulted in the deterioration of structure and decline in the number of traditional houses. Yet, in order to exhibit cultural identity, reservation of traditional structures and houses should be integrated into daily life. When exhibition and perpetuation of a world heritage such as the Selimiye Mosque Complex is considered with its surroundings, traditional and historical buildings in the district become increasingly important. This study which has been conducted to call attention to the district and its existing traditional houses, reviews the architectural properties of the district and its traditional houses and determines its potentials and problems.

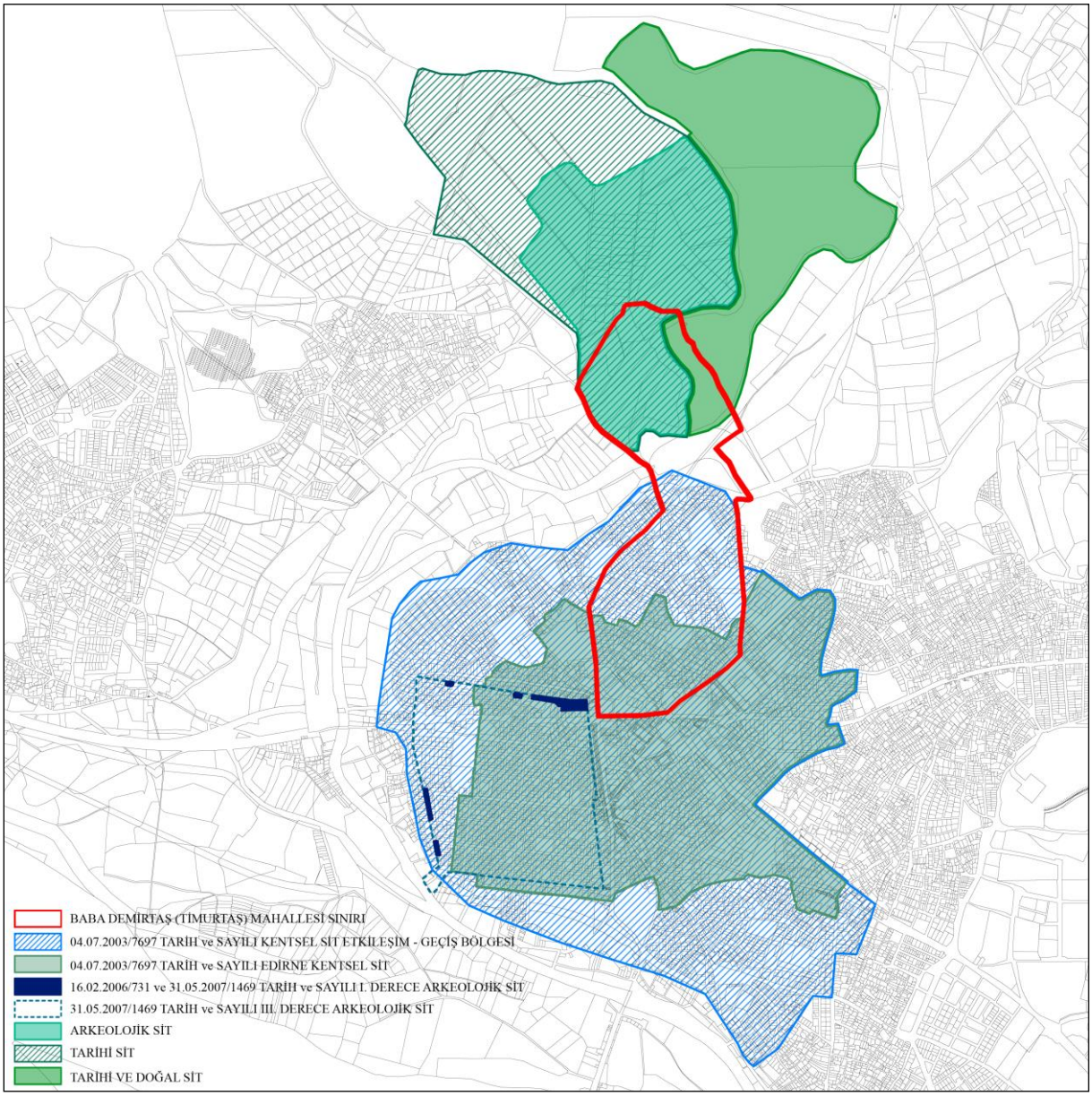
Keywords: Edirne, Baba Demirtaş District, traditional dwelling architecture.

GİRİŞ

Fiziksel ve toplumsal çevrelerin süreç içerisindeki gelişim ve değişimi, farklı yaşam biçimlerinin; hatta yeni mimari üslupların oluşumunda rol oynamaktadır. Oluşan her mimarlık üslubu, ait olduğu dönemin ve toplumun özelliklerini yansıtması açısından büyük önem taşımaktadır.

Mimarlıkta en fazla ürün verilen tasarım alanı, konutlardır. Toplumu oluşturan bireylerin barınma ihtiyacını karşılamak üzere tasarlanan konutların biçimlenişine dikkat edildiğinde dönemlerinin, ait oldukları toplumların yaşam şeklinin, bulundukları bölgelerin ve yer aldıkları çevrelerin belirleyici rol oynadığı görülmektedir. Bu bağlamda, geleneksel konutlar da ait oldukları dönemin mimari anlayışını, malzeme ve tekniklerini; toplumların da sosyo-kültürel ve sosyo-ekonomik yapısını yansıtan öğeler olarak karşımıza çıkmaktadır. Ancak 20. yüzyılda hız kazanan endüstrileşmeye bağlı olarak modernleşme, küreselleşme, kentleşme gibi faktörlerin yanı sıra toplumların yaşam biçimlerinin ve beğenilerinin değişmesi, trafiğin yoğunlaşması, kullanıcı değişimi, bilinçsiz kullanım ve denetimsiz yapılaşma vb. birtakım faktörler geleneksel konutların azalmasına, tarihi dokuların da bozulmasına neden olmuştur. Oysaki gelişim ve değişimlerin paralelinde, kültürel kimliği sergilemek adına, geçmişin günümüz izleri olan geleneksel dokuların ve konutların korunarak günlük yaşama katılımlarını sağlamak mümkündür.

Bu çalışmada, Edirne Baba Demirtaş Mahallesi geleneksel konutları ele alınmıştır. Konutların seçiminde, içinde bulundukları mahallenin konumu büyük rol oynamıştır. Söz konusu mahallenin çalışma alanı olarak tercih edilmesinde, güney bölümünün kentsel sit; yapılaşma olmayan kuzey bölümünün ise tarihi, arkeolojik, tarihi ve doğal sit sınırları içerisinde yer alması (Şekil 1) yanı sıra Osmanlı dönemi kale dışı yerleşmelerine örnek teşkil etmesi, kent merkezinin ve Kaleiçi'nin yakınında konumlanması, dünya mirası Selimiye Camii ve Külliyesi'nin geçiş ve etkileşim bölgesi sınırlarında bulunması, bünyesinde geleneksel konutların yanı sıra anıtsal nitelikli tarihi yapıları da barındırması etken olmuştur. Mahallenin ve mahalle sınırları içerisindeki mevcut geleneksel konutların önemine dikkat çekmek üzere hazırlanan çalışmada, geleneksel konutların mimari özellikleri incelenmiş; potansiyelleri ve sorunları tespit edilmiştir.

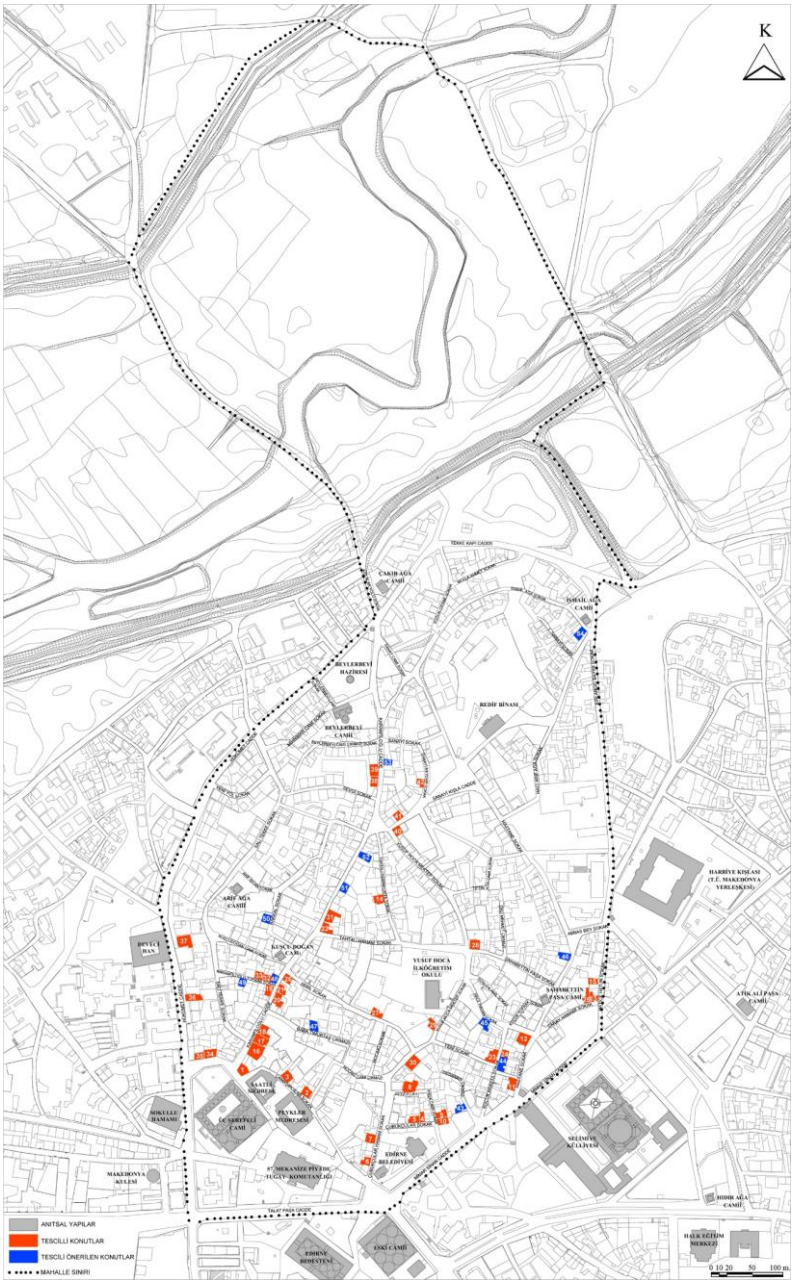


Şekil 1. Baba Demirtaş Mahallesi'nin Konumu ve Sit Sınırları (Edirne Kentsel Sit ve Etkileşim Geçiş Bölgesi 1/5000 Ölçekli Nazım İmar Planı ile 1/1000 Ölçekli Revizyon ve İlave Koruma Amaçlı Uygulama İmar Planı Notları'nda ayrı olarak bulunan haritalardan birleştirilerek yeniden hazırlanmıştır)

BABA DEMİRTAŞ (TİMURTAŞ) MAHALLESİ: TARİHÇESİ, KONUMU VE DOKU ÖZELLİKLERİ

Edirne'nin Osmanlıların hakimiyetine girmesinden sonra, yerleşmenin yoğun olduğu Kaleiçi bölgesi dışında yeni mahalleler oluşturulmaya başlanmıştır (Darkot, 1993). Organik dokuya sahip Baba Demirtaş Mahallesi de kale dışı bölgesinde kurulan mahallelerden biridir. Günümüzde Baba Demirtaş Mahallesi, 15. yüzyılda kurucularının isimlerine veya meslek gruplarına göre adlandırılmış olan (Baba Timurtaş Mahallesi, Arif Ağa Mahallesi, Havacagi/Hocagi Mahallesi, Kurtçu/Kuşçu Doğan Mahallesi, Beylerbeyi Sinan Bey İmareti Mahallesi, Şahabettin Paşa Mahallesi, Fazlullah Paşa Mahallesi, Tarakçı Mahallesi, Kiremitçi Halil Mahallesi) birçok mahalleyi bünyesinde toplamış (Kazancıgil, 1999) olup bünyesindeki mahalle isimlerini de sokak adları olarak devam ettirmektedir. Mahalle kurucularının yaşadıkları dönemler dikkate alındığında, Baba Demirtaş Mahallesi'nin 15. yüzyılın başlarında kurulmaya başlandığı; özellikle Sultan II. Murad döneminde geliştirildiği ileri sürülebilir.

Baba Demirtaş Mahallesi, Edirne kent merkezine yakın konumda, tarihi kent dokusu içinde yer almaktadır. Üç Şerefeli Camii'nin de içinde yer aldığı mahalle, Eski Cami'nin kuzeyinde, Selimiye Camii ve Külliyesi'nin kuzeybatısında konumlanmaktadır (Şekil 2). Mahallenin bir bölümü (güneyi), Selimiye Camii Külliyesi UNESCO Dünya Mirası Edirne Alan Yönetim Başkanlığı'nca belirlenen geçiş ve etkileşim bölgesinde bulunmaktadır.



Şekil 2. Baba Demirtaş Mahallesi Sınırları ve Mahalledeki Yapılaşma Durumu

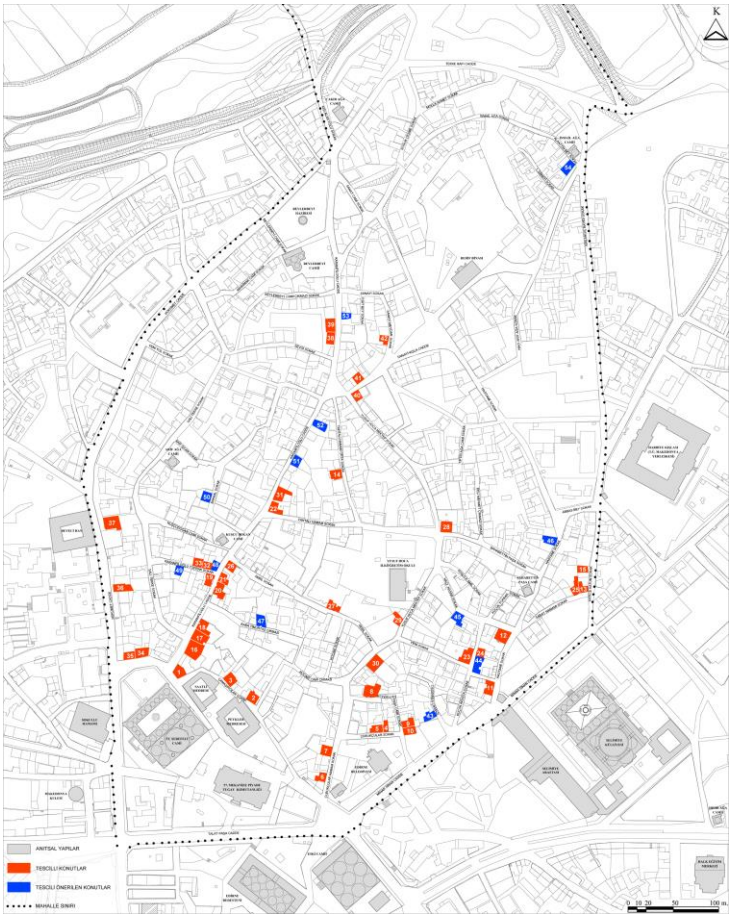
Mahallenin kuzey yarısını, yeşil alan ve Eski Saray'ın bir bölümü oluşturmaktadır (Şekil 2). Yapılaşmanın yoğun olduğu güney yarısını ise kuzeyde, Tekke Kapı Caddesi; doğuda ve kuzeydoğuda, Hükümet Caddesi; güneyde, Talat Paşa Caddesi; güneybatıda, Mimar Sinan Caddesi; batıda da Hatice Hatun Sokak ve Kırlangıç Bayırı Sokak çevrelemektedir.

Mahalle sınırları içerisinde, geleneksel konutlar haricinde, Osmanlı Dönemi'ne ait 7 cami (Kuşçu Doğan Camii, Şahabettin Paşa Camii, İsmail Ağa Camii, Arif Ağa Camii, Beylerbeyi Camii, Üç Şerefeli Cami, Çakırağa Camii), 2 medrese (Saatli Medrese, Peykler Medresesi), 10 çeşme (Merzifonlu Kara Mustafa Paşa Çeşmesi, Yusuf Hoca Çeşmesi, Ömer Efendizade Çeşmesi, Çamaşırcılar Sokak Çeşmesi, Muhammet İbn-i Ahmet Çeşmesi, Hacı Yusuf Çeşmesi, Saraçhane (Sinan Ağa) Çeşmesi, Beylerbeyi (Kuru) Çeşmesi, Karanfiloğlu Çeşmesi, Soğuk Çeşme), 2 askeri yapı (Daire-i Müşir/Tümen Karargahı -günümüzde 54. Mekanize Piyade Tugay Komutanlığı- ve Redif Dairesi), 1 eğitim binası (Yusuf Hoca İlköğretim Okulu), 1901 tarihli Belediye Binası ve Cumhuriyet Dönemi'ne ait Sağlık İşleri Binası gibi tarihi özellikler taşıyan farklı tipte yapılar da mevcuttur.

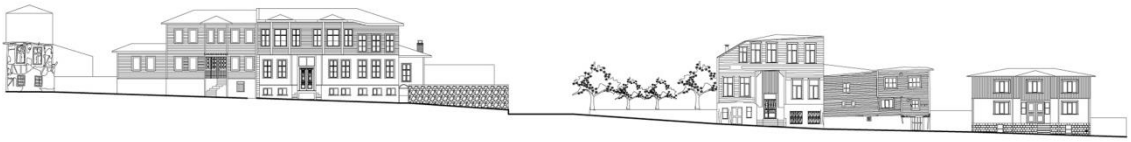
Yapılan incelemelerde, organik dokuya sahip olduğu görülen mahallede, eğri (Küçük Toprak Sokak, Süslü Kamil Sokak, Salı Tekke Sokak vb.) ya da düz (Çubukçular Sokak, Yeni Sokak, Hocaki Sokak gibi) sokakların yanı sıra çıkmaz sokakların da (Baba Timurtaş Çıkmazı, Değirmen Çıkmazı, Hocaki Camii Çıkmazı ve Deli Mehmet Çıkmazı) bulunduğu; ancak düz sokakların yoğunlukta olduğu tespit edilmiştir. Ayrıca sokaklarda yükselme, alçalma, daralma ve genişlemelerin varlığı da söz konusudur.

BABA DEMİRTAŞ (TİMURTAŞ) MAHALLESİ GELENEKSEL KONUTLARININ MİMARİ ÖZELLİKLERİ

Mahalle sınırları içerisinde, yapılaşmanın yoğun olduğu güney bölümde, geleneksel özelliklere sahip 54 konut belirlenmiş olmakla birlikte bunlardan 42'sinin tescilli olduğu tespit edilmiştir (Şekil 3). Günümüze ulaşan geleneksel konutların çoğunlukla Karanfiloğlu Caddesi (Şekil 4), Çubukçular Sokak ve Feyzullah Paşa Camii Sokak'ta konumlandığı; sözü edilen sokaklar haricinde ise dağınık olarak yer aldıkları belirlenmiştir. Ayrıca sokak üzerinde bitişik nizam ve bahçe içinde ayrık nizam olmak üzere iki farklı şekilde konumlandıkları; bitişik nizam yapıların arka bahçelerinin de mevcut olduğu tespit edilmiştir.



Şekil 3. Baba Demirtaş Mahallesi Güney Bölümü (Yapılaşmanın Yoğun Olduğu Bölüm): Sokaklar, Anıtsal Yapılar, Tescilli ve Tescili Önerilen Geleneksel Konutlar

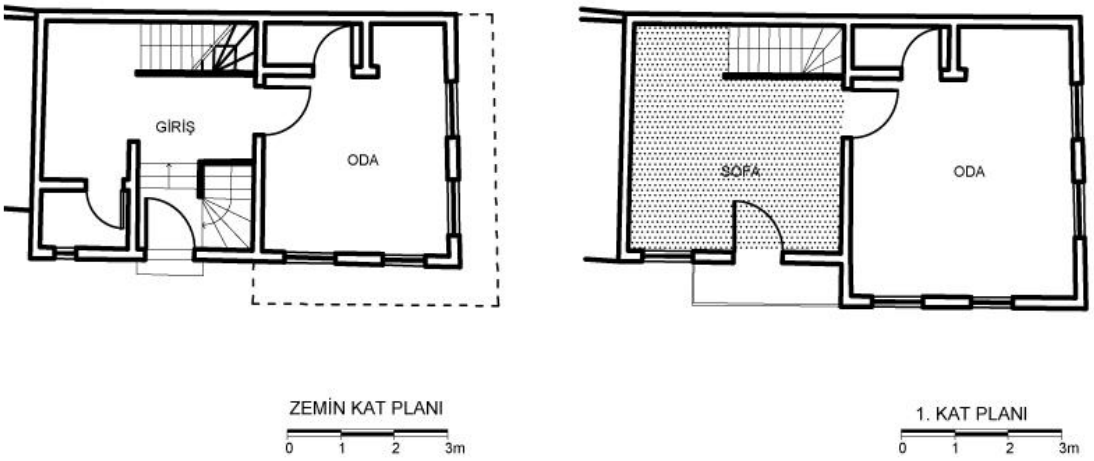


Şekil 4. Karanfiloğlu Caddesi Silüeti (Soldan Sağa 26-21-20-18-17-16 No'lu Konutlar)
(T.Ü. Mimarlık Fakültesi Mimarlık Bölümü Restorasyon Arşivi)

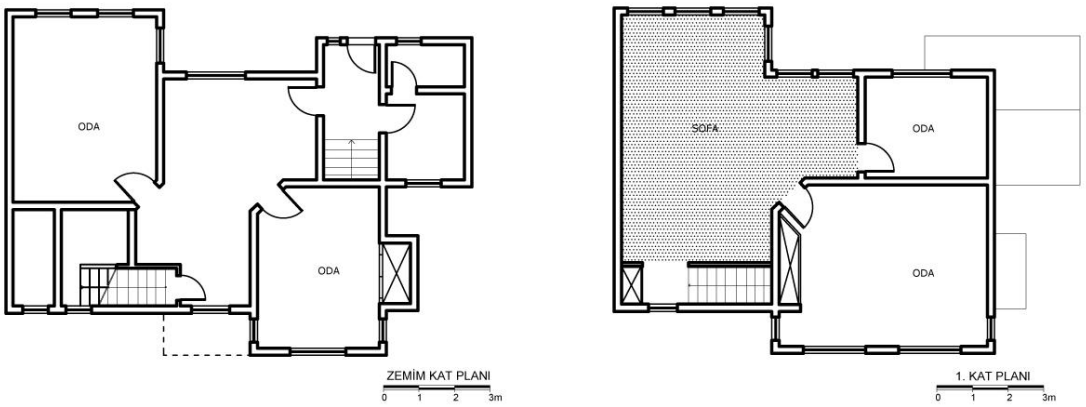
Aşağıda, alan içerisindeki geleneksel konutların mimari özelliklerinin incelenmesinde plan, cephe ve taşıyıcı sistem özellikleri ele alınmıştır.

Plan Özellikleri: Baba Demirtaş Mahallesi'nde yer alan konutların plan şemasının belirlenmesinde en etkin rol oynayan mekân öğeleri, odalar ve sofadır. Geleneksel Türk konutunun biçimlenmesinde de bu iki öğe dikkate alındığında, mahalledeki geleneksel konutların geleneksel Türk evinin "iç sofalı plan" tipi özelliklerini yansıttıkları görülmektedir. Bu çalışmada konutlar -plan tipolojisi açısından- sofalar ve cihannümalar dikkate alınarak incelenmiş; sofalılar da -sofanın konumu göz önünde bulundurularak- sofa yanda ve sofa ortada olmak üzere 2 gruba ayrılmıştır. Ancak ele alınan 54 konuttan 41'inin plan özellikleri incelenebilmiş; diğerlerine girilememiştir. Günümüzde ticari amaçla kullanılmakta olan 11 No'lu yapının da geçirdiği onarımlar sonrasında özgün plan özelliklerini kaybettiği belirlenmiştir. Aşağıda, sayfa sayısının sınırlı olması nedeniyle, tüm konutların plan çizimlerine yer verilememiş; örnekleme ikişer konut planı ile sınırlı tutulmuştur.

***Sofa yanda*:** Bu plan tipinde sofa, tek yönden bir ya da birkaç oda ile çevrilidir. İncelenen 41 konutun 10'unda (6, 10, 15, 17, 25, 26, 32, 35, 48 ve 53 No'lu konutlar) sofanın yanda yer aldığı tespit edilmiş; ancak aşağıda iki konut planı üzerinden örneklenmiştir (Şekil 5).



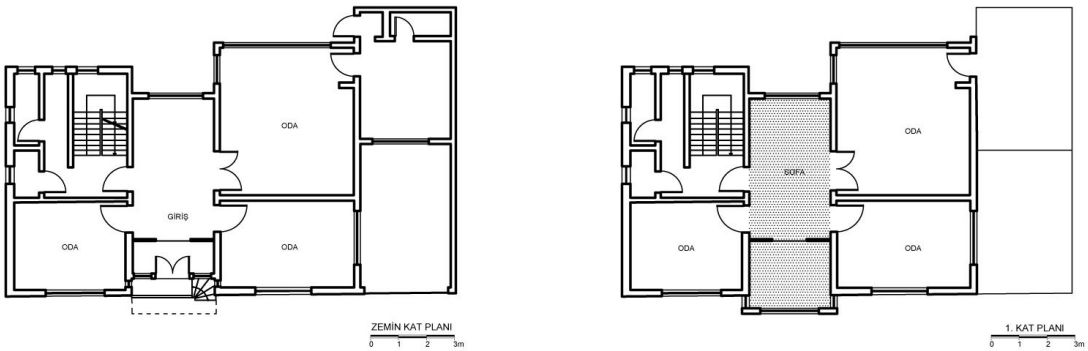
26 No'lu Konut Planları



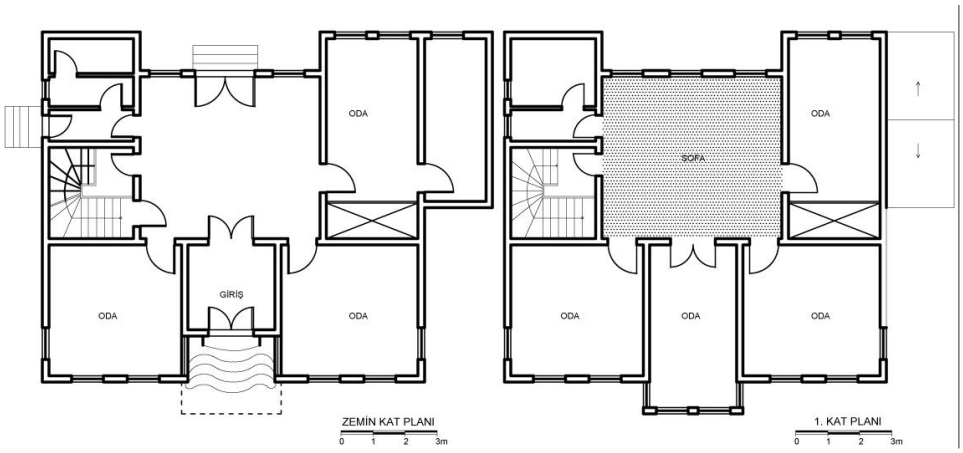
17 No'lu Konut Planları

Şekil 5. Yan Sofalı Konut Örnekleri (Mısırlı, 2014)

***Sofa ortada*:** Bu plan tipinde sofa, iki ya da üç yönden odalarla çevrilidir. İncelenen 41 konutun 27'sinde (1, 3, 4, 5, 8, 9, 12, 13, 16, 18, 19, 20, 21, 22, 23, 28, 31, 33, 37, 38, 39, 40, 42, 47, 49, 50 ve 51 No'lu konutlar) sofanın ortada yer aldığı tespit edilmiştir (Şekil 6).



16 No'lu Konut Planları



3 No'lu Konut Planları

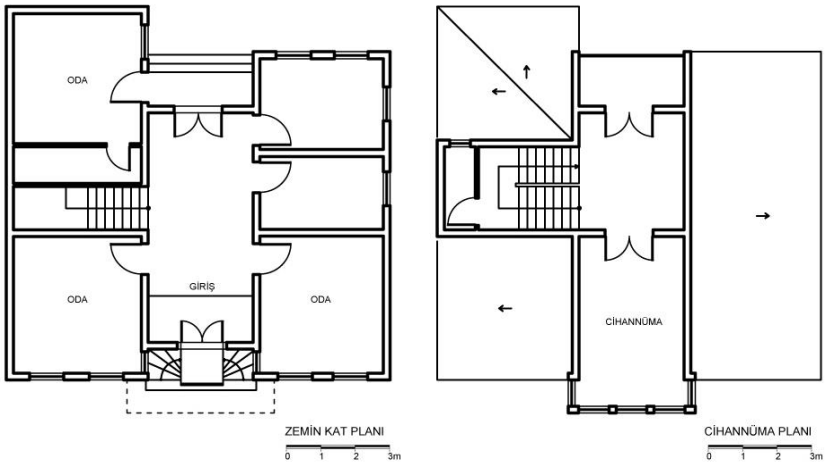
Şekil 6. Orta Sofalı Konut Örnekleri (Mısırlı, 2014)

***Cihannümalı*:** Bu plan tipinde zemin kat üzerinde tek mekândan oluşan cihannüma yer almaktadır. İncelenen 41 konuttan sadece 3'ünün (2, 7 ve 34 No'lu konutlar) cihannümalı olduğu tespit edilmiştir (Şekil 7).

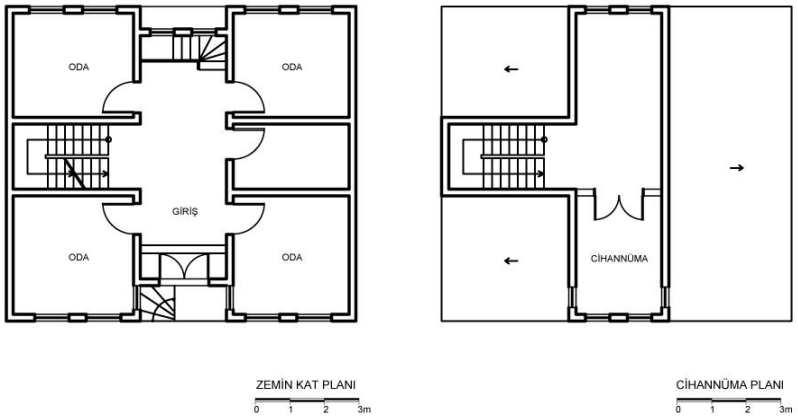
İncelenen konutlarda sofaların genellikle dikine dikdörtgen; odaların ise kareye yakın dikdörtgen plana sahip oldukları görülmektedir. Sofaların işlev değişikliğine uğramalarına rağmen odalar ile servis mekanları arasında geçiş mekanı niteliği taşıdığı; odaların ise özgün kullanımlarını kaybettikleri söylenebilir. Çift ya da yanda tek çıkmalı cephe düzenine sahip yapılarda, çıkmalar odaların genişletilmesiyle elde edilmiş; odaların genişliğine göre pencereler de tekli veya ikili düzende yerleştirilmiştir. İç mekan mimari elemanı olarak bazı odalarda sadece dolapların yer aldığı tespit edilmiştir. Odaların tavanlarında -özellikle ortada- yer alan ahşap profilli süslemeler, duvarlarında da kalem işi bezemeler ve resimler dikkat çekmektedir.

Sınıflandırmada etken olan cihannüma ise genellikle birinci ya da ikinci kat üzerinde, yapının sokağa ya da avluya bakan cephesinde konumlanmış olup üç yanı pencerelidir. Cihannümaların manzaraya sahip en özel mekan olduğu söylenebilir. Fakat günümüzde özgün işlevlerini yitirdikleri görülmektedir.

Sofa ve cihannüma haricinde, konutlar tek katlı ve iki katlı olmak üzere de gruplandırılabilir. İki katlı konut planlarında merdivenin konumunun etkin rol oynadığı söylenebilir. Merdivenler sofada, iki oda arasında ya da oda sırası sonunda olmak üzere üç farklı şekilde uygulanmış olarak karşımıza çıkmaktadır. Bununla birlikte formuna göre bir değerlendirme yapıldığında I, L ve U forma sahip merdivenler mevcuttur (Şekil 8, 9, 10). Bodruma ulaştıran merdivenler taş iken üst katlara ulaştıran merdivenler ahşaptır. Merdiven altı boş bırakıldığı gibi bazı konutlarda kapatılmış ve depo olarak işlevlendirilmiştir. Merdiven korkulukları ahşap malzemeden yapılmıştır. Bazı korkuluklarda ahşap oyma tekniklerine ve süslemelere de rastlanmaktadır.



2 No'lu Konut Planları



7 No'lu Konut Planları

Şekil 7. Cihannümalı Konut Örnekleri (Mısırlı, 2014)

Şekil 8. I Formda Merdiven (47 No'lu Konut)*

Şekil 9. L Formda Merdiven (15 No'lu Konut)

Şekil 10. U Formda Merdiven (28 No'lu Konut)

Tipoloji açısından etkin rol oynamamakla birlikte servis mekânları olan mutfak, tuvalet ve banyonun birçok yapıda özgünlüğünü kaybettiği; ancak birkaç yapıda orijinal örneklerinin bulunduğu tespit edilmiştir. Bu mekânlara ait ocak, mermer kurna, hela taşı gibi özgün mimari elemanlara nadir olarak rastlanmıştır (Şekil 11, 12, 13).

Şekil 11. Ocak
(18 No'lu Konut)

Şekil 12. Tuvalet ve Hela Taşı
(19 No'lu Konut)

Şekil 13. Mermer Kurna
(18 No'lu Konut)

Cephe Özellikleri: Mahalle içindeki geleneksel konutların cephe karakterini belirleyen en önemli unsur çıkmalardır. Bununla birlikte girişler, pencereler, giriş kapıları, yatay silmeler ve köşe dikmeleri, çıkma altı elemanları, çatı biçimlenişi ve saçaklar da cephe karakterinin oluşumunu sağlayan diğer elemanlardır. Konutlar cephe özellikleri açısından çıkmalı, çıkmasız, cihannümalı ve köşe yapılar olmak üzere 4 grupta incelenmiştir. İnceleme sonucunda 54 konuttan 26'sının çıkmalı (3, 4, 5, 6, 8, 9, 10, 11, 13, 15, 16, 17, 20, 21, 22, 25, 28, 31, 32, 33, 40, 41, 42, 47, 49 ve 52 No'lu konutlar), 22'sinin (14, 18, 19, 23, 24, 27, 29, 30, 35, 36, 37, 38, 39, 43, 44, 45, 46, 48, 50, 51, 53 ve 54 No'lu konutlar) çıkmasız, 3'ünün (2, 7 ve 34 No'lu konutlar) cihannümalı, 3'ünün de (1, 12 ve 26 No'lu konutlar) köşe yapı olduğu tespit edilmiştir.

Cephede çıkması bulunan konutlar çıkma sayısına, formuna ve konumuna göre alt kategorilere ayrıldığında, 12'sinin tek (3, 6, 9, 16, 17, 21, 32, 33, 41, 42, 49 ve 52 No'lu konutlar) (Şekil 14), 9'unun (5, 10, 11, 20, 22, 28, 31, 40 ve 47 No'lu konutlar) çift (Şekil 15), 2'sinin (13 ve 15 No'lu konutlar) testere (Şekil 16), 3'ünün de (4, 8 ve 25 No'lu konutlar) tüm kat çıkmalı (Şekil 17) olduğu belirlenmiştir. Çıkmalı konutların genellikle iki kattan oluştuğu görülmektedir.

Şekil 14. Tek Çıkmalı (3 No'lu Konut)

Şekil 15. Çift Çıkmalı (10 No'lu Konut)

Şekil 16. Testere Çıkmalı (13 No'lu Konut)

Şekil 17. Tüm Kat Çıkmalı (25 No'lu Konut)

Çıkmasız yapılar, tek veya iki katlıdır. Sadece 36 No'lu konut çıkmasız (Şekil 18) olup üç katlı inşa edilmiştir. Bu tipteki yapılarda tüm cephenin aynı düşey düzlemde olduğu ya da girişin girintide yer aldığı görülmektedir.

Mahallede zemin kat üzerinde orta çıkmalı/cihannümalı konutlar (2, 7 ve 34 No'lu konutlar) (Şekil 19) da mevcuttur. Bodrum katın da mevcut olduğu bu tip konutlarda basamaklarla yükseltilmiş girişler dikkat çekmektedir. Köşe yapıların ise iki cephesinde de farklı tipte çıkmalar görülmektedir.

Şekil 18. Çıkmasız (36 No'lu Konut)

Şekil 19. Cihannümalı (34 No'lu Konut)

Çıkmalar dışında geleneksel konutlarda dikkat çeken ikinci öğe, girişlerdir. Yapıların 41'ine giriş doğrudan sokaktan, 4'üne (13, 15, 19 ve 29 No'lu konutlar) bahçeden, 8'ine (5, 12, 20, 21, 23, 28, 44 ve 54 No'lu konutlar) ise hem doğrudan sokaktan hem de bahçeden sağlanmaktadır. Doğrudan sokaktan sağlanan girişler, 31 konutta niş içinde; 19 konutta nişsiz (Şekil 20) olmak üzere iki tiptedir. Bahçeden geçerek ulaşılan 4 yapının da girişi nişsizdir. Niş içindeki girişlerde ise merdivenlerin formu, bir yandan (Şekil 21), iki yandan (Şekil 22) ve önden (Şekil 23) olmak üzere üç farklı tiptedir.

Şekil 20. Nişsiz (1 No'lu Konut)

Şekil 21. Merdiven Bir Yandan (22 No'lu Konut)

Şekil 22. Merdiven İki Yandan (2 No'lu Konut)

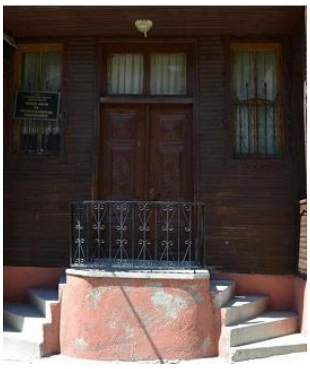
Şekil 23. Merdiven Önden (3 No'lu Konut)

Özgün giriş kapıları ahşaptır. Tek kanatlı (Şekil 24), çift kanatlı (Şekil 25), çift kanatlı+tepe pencereli (Şekil 21, 22, 23), çift kanatlı+iki yanı pencereli (Şekil 26), çift kanatlı+iki yanı pencereli+tepe pencereli (Şekil 27) olarak 5 farklı tipte örnekleri bulunmaktadır. Ancak süreç içerisinde bazı konutlarda özgün ahşap kapıların metal kapılar olarak değiştirildiği; bu nedenle sayılı orijinal örneğin günümüze ulaştığı söylenebilir.

Şekil 24. Tek Kanatlı (15 No'lu Konut)

Şekil 25. Çift Kanatlı (47 No'lu Konut)

Şekil 26. Çift Kanatlı+İki Yanı Pencereli (16 No'lu Konut)



Şekil 27. Çift Kanatlı+ İki Yanı Pencereli+Tepe Pencereli (5 No'lu Konut)

Pencereler ise tekli (Şekil 28), ikili (Şekil 29), üçlü (Şekil 30) ve beşli (Şekil 31) düzendedir. Bununla birlikte birden fazla pencere düzenine sahip konutların varlığı da söz konusudur. Tekli düzendeki pencereler kare veya 1×2 oranında dikine dikdörtgen; ikili, üçlü ve beşli düzenleri oluşturan pencereler ise 1×1.5, 1×2 oranında dikine dikdörtgendir. Çift kanatlı ve giyotin pencere olarak tasarlanmışlardır. Kepenk ve parmaklık kullanımının yaygın olmadığı söylenebilir.

Şekil 28. Tekli Pencere Düzeni (22 No'lu Konut)

Şekil 29. İkili Pencere Düzeni (3 No'lu Konut)

Şekil 30. Üçlü Pencere Düzeni (5 No'lu Konut)

Şekil 31. Beşli Pencere Düzeni (15 No'lu Konut)

Ahşap karkas yapılarda karşılaşılan yatay silmeler, katlar arasında duvar boyunca devam eden düz bir ahşap eleman şeklindedir (Şekil 32). Ayrıca bodrum kat hizasında taş silmelere ve katlar arasında profilli ahşap silmelere de rastlanmaktadır (Şekil 33). Cephelerdeki köşe dikmeleri genellikle sıvanmayıp açıkta bırakılmıştır. Çıkmalar ahşap veya metal eliböğründelerle desteklenmiştir (Şekil 34, 35).

Şekil 32. Duvar boyunca devam eden düz ahşap yatay silmeler ve ahşap köşe dikmeleri (Solda 25 No'lu Konut, Sağda 13 No'lu Konut)

Şekil 33. Bodrum kat hizasında taş; katlar arası profilli ve ahşap köşe dikmeleri (12 No'lu Konut)


Şekil 34. Ahşap Eliböğründe Örnekleri
(Solda 22 No'lu Konut, Sağda 12 No'lu Konut)


Şekil 35. Metal Eliböğründe Örnekleri
(Solda 28 No'lu Konut, Sağda 3 No'lu Konut)

Taşıyıcı Sistem Özellikleri: Konutlardan bodrum+bir kat olanların genellikle yığma; bodrum+iki kat olanların ise bodrum katlarının yığma, üst katlarının ahşap karkas olarak inşa edildiği belirlenmiştir. Bu konutlarda, zemin katta ve üst katlarda mekanları bölen duvarlar ahşap karkas sistem olup araları tuğla ya da kerpiç malzeme ile doldurulmuş; üzerleri de sıvanmıştır. Sıvanın döküldüğü yerlerde, ara bölücü duvarlarda ve özellikle çıkma duvarlarında ahşap rabıta kaplama gözlenmiştir.

Çatılar, kırma veya beşik çatı olup oturtma çatı sistemi ile çözülmüştür. Çatı örtüsü özgün hali ile alaturka kiremittendir. Değişmiş ya da müdahale görmüş olanlar marsilya tipi kiremit ile örtülmüştür.

Döşemeler, ahşap kirişlerin üzerine yerleştirilmiş ahşap rabıtalardan oluşmaktadır. Konutların üst kat döşemesini taşıyan ahşap kirişler açıkta bırakıldığı gibi ahşap malzeme ile kaplananlar da mevcuttur.

Çıkmalı yapılardaki çıkmalar, bulundukları katın ahşap kirişlerinin uzatılması ile taşıtılmış; ahşap ya da metal eliböğründeler ile de desteklenmiştir.

Konutlardaki merdivenlerden bodrum kata ulaştıranlar, taş; üst katlara ulaştıranlar, ahşap konstrüksiyon ile oluşturulmuştur.

SORUNLAR VE POTANSİYELLER

1950'li yıllarda anıtsal eserlerin görsel algılarını engelleyen sivil yapıların yıkılması ve 1960'lı yıllarda betonarme yapı uygulamalarının başlaması geleneksel doku karakterinin değişikliğe uğramasında etken olmuştur. Aşağıda, bu durumdan etkilenmekle birlikte günümüzde varlığını sürdürmeye çalışan Baba Demirtaş Mahallesi geleneksel konutlarının sorunlarına ve potansiyellerine değinilmektedir.

Sorunlar: Geleneksel konutların en önemli sorunlarından biri, atıl kalarak süreç içerisinde yıkılmaları; hatta yok olmalarıdır. Çalışma alanında da bakımsızlıktan harap olmuş, çok az izi kalmış; hatta geçmişteki varlığı, tescillenmiş boş parsellerden öğrenilen konutlar mevcuttur.

En önemli sorunlardan bir diğeri işlev değişikliğine uğramalarıdır ki söz konusu mahalle içerisinde işlev değişikliği sonucu orijinalliğini yitirmiş yapılar karşımıza çıkmaktadır. Özellikle kamu yapıları olarak yeniden işlevlendirilmiş olan konutların plan tiplerinin değişikliğe uğradığı, geleneksel dokuya uygun olmayan çeşitli eklere maruz kaldığı görülmektedir. Örneğin, yapılara giriş veya merdiven eklenmesi, mevcut birimlerin parçalanarak yeni bölümler kazanılmaya çalışılması sonucu yapı tipolojilerinde bozulmalar meydana gelmiştir. İşlev değişikliğine uğramamış konutlarda ise konfor problemleri özellikle plan tipinde değişimlere sebep olmuştur. Bu durumun orijinalliğin yitirilmesinde büyük rol oynadığı söylenebilir. Mimari eleman eklerinin yanı sıra cephelerde yer alan yağmur oluğu, klima, kablo, tabela vb. öğeler de cephelerin etkisini zayıflatmakta; görsel kirlilik yaratmaktadır.

Geleneksel konut cephelerinde gözlenen çatlaklar, derz boşalmaları, malzeme bozulmaları, zemin ve çatıdan kaynaklanan su problemleri yanı sıra değiştirilmiş, kaldırılmış veya eklenmiş çatı, baca, kapı ve pencere gibi elemanlar yapı ölçeğindeki sorunlar arasında yer almaktadır. Ayrıca geleneksel konutların orijinalliğini olumsuz etkileyen faktörler arasında da çatı kaplama malzemelerinin değiştirilmesi, ahşap elemanların boyanması, cephe elemanlarındaki malzeme ve biçim değişiklikleri sayılabilir.

Yapıların içinde ise bakımsızlık ve ilgisizlik nedeniyle uzun süreli doğal etkenlerin yarattığı tahribatlar, malzeme bozulmaları, tavan düzleminde oluşan sehim, zemin oturmaları, su yalıtımının yapılamamasından kaynaklanan bozulmalar, plan ve mekan bölünmeleri, mimari elemanların kaldırması, eklenmesi veya değiştirilmesi gibi sorunlar görülmektedir.

Potansiyeller: Çalışma alanı içerisinde çok sayıda müstakil yapının bulunması ve bu yapıların insan boyutları ile uyumlu olması alanın kente nefes aldırmasında önem taşır. Geleneksel konutlar, anıtsal yapılar ve geleneksel özellik taşımamakla birlikte alan ile uyumlu müstakil konutlar, sokak silüetine

katkı sağlayan cepheleriyle çalışma alanı için potansiyel oluşturmaktadırlar.

Sayısı az olmakla birlikte özgünlüğünü korumuş konutların cepheleri yanı sıra detayları, geçmiş ile günümüz arasındaki kültürel bağı kurması açısından önem taşımaktadır. Ayrıca orijinal cephe düzenine sahip geleneksel konutların kısmen geleneksel özelliğe sahip olan konutların geleneksel dokuya uygun onarılmasında ve yeni yapılaşma kriterlerini belirlemede de önem taşıdığı söylenebilir.

İncelenen geleneksel konutlar arasında yer alan ve 'Beyaz Ev' olarak adlandırılan yapının Bahailer tarafından kutsal mekan olarak kabul edilmesi ise bölgenin turist potansiyelini arttırmaktadır.

Baba Demirtaş Mahallesi geleneksel konutlarının çoğu özgün planları, cepheleri, mimari elemanları ve sahip oldukları kimlikleri ile gelecek kuşaklara iletilme potansiyeline sahiptir. Boş konutların korunması; hatta doğru şekilde işlevlendirilerek yaşatılması durumunda alanın değeri daha da artacaktır.

SONUÇ VE DEĞERLENDİRME

Tarihi değerler açısından -anıt eserler hariç- oldukça ihmal edilmiş Edirne kenti, geleneksel konutlarını büyük ölçüde yitirmiştir. Buna rağmen günümüzdeki mevcut geleneksel konutların, Kaleiçi yerleşimi haricinde, bir kale dışı yerleşimi olan Baba Demirtaş Mahallesi'nde de varlıklarını sürdürmeye çalıştıkları görülmektedir.

Baba Demirtaş Mahallesi, Edirne'nin Osmanlılar tarafından fethedilmesinden sonra kale dışında gelişen ilk mahallelerden biri olması, kentsel sit sınırları içinde yer alması ve Osmanlı dönemi cami gelişiminin evrelerini sergileyen yapılara yakın konumlanması açısından önem taşıdığı gibi düz, eğri ve çıkmaz sokakları ile organik dokuya sahip olması, Osmanlı dönemi kale dışı yerleşimlerinin özelliklerini sergilemesi ve ızgara planlı Kaleiçi yerleşiminden farklılık göstermesi açısından da önem taşımaktadır.

Mahallenin özgün değerleri arasında yer alan geleneksel konutlar ile cami, medrese, çeşme gibi anıtsal yapılar mahalle sokaklarını zenginleştiren öğelerdir. Mahalle sokaklarının birçoğundan Selimiye Camii, Üç Şerefeli Cami ve Eski Cami gibi anıtsal yapılardan en az birinin görülmesi ise alanın görsel değerlerine büyük katkı sağlamakta; sokaklara da kendine özgü bir karakter kazandırmaktadır. Mahalle bünyesindeki geleneksel konutlar ise ahşap kaplamalı ya da sıvalı cepheleri, tek, çift, tüm kat ya da testere çıkmaları, niş içindeki girişleri, gösterişli giriş sahanlıkları ve uzunlamasına dikdörtgen pencere düzenleri ile dikkat çekmekte; plan ve cephe düzlemindeki çeşitlilik de mahallenin kendine özgü mimari niteliğini sergilemektedir. Özellikle Karanfiloğlu Caddesi'nde yer alan sıralı geleneksel konutlar ve köşe konutlar alanın görsel değerlerini arttırmaktadır.

Tarihi dokuyu oluşturan geleneksel konutlar ait oldukları dönemin mimari, sosyal ve kültürel değerlerini yansıtan öğeler arasında sayılabilir. Mahalle içerisindeki geleneksel konutların da özgün karakterleri ve sahip oldukları kimlikleri ile döneminin özelliklerini yansıttıkları söylenebilir. Nitekim günümüzde kentleşmeyle gelen hızlı değişim sonucu birbirine benzer nitelikte ve görünümde yapıların çoğalması, kültürel kimliğin zedelenmesine ve dokunun bozulmaya başlamasına neden olmuştur. Oysaki Akın'ın da belirttiği gibi, geleneksel dokuyu oluşturan tarihi konutlar, geçmişin tanıkları olarak bulundukları çevreye özgün bir boyut katmaktadırlar (Akın, 1988).

Geçmişin izleri ya da geçmişin günümüz sunumları olarak kabul edebileceğimiz geleneksel konutların yaşamın içine alınarak korunmaları gerekliliği kültürel sürekliliğin sağlanabilmesi, yöresel ve geleneksel mimarinin geleceğe aktarılabilmesi, yeni nesillerin tarihi doku içerisinde gezerken ya da geleneksel konutları izlerken geçmişi düşünebilmeleri/düşleyebilmeleri adına önem taşımaktadır. Bu nedenle koruma çalışmalarının sadece bölgedeki geleneksel konutların mimari özelliklerini değil dokuyu da içerecek nitelikte geniş kapsamlı olması gerektiğinin altı çizilmelidir.

KAYNAKLAR

1. AKIN, N., "Türkiye'de Tarihi Çevre Koruma, Örnekler ve Sorunlar", Mimarlık Dergisi, Sayı. 288, s. 40-43, 1988.
2. DARKOT, B., "Edirne Coğrafi Giriş", s.1-12, 1993. [EDİRNE-Edirne'nin 600. Fethi Yıldönümü Armağan Kitabı, 349 (fotoğraflar hariç), Türk Tarih Kurumu Basımevi, Ankara].
3. KAZANCIGİL, R., "Edirne Mahalleleri Tarihçesi (1529-1990)", 1999, Edirne Valiliği Yayınları No:7, İl Kültür Müdürlüğü Yayınları No: 4, İstanbul, 181, 1999.
4. MISIRLI, A., "Tarihsel Çevre ve Mimari Oluşum Üzerine Bir Alan Çalışması: Edirne Baba Timurtaş Mahallesi", Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Edirne, 2014.
5. Trakya Üniversitesi Mimarlık Fakültesi Mimarlık Bölümü Restorasyon Arşivi
6. Tüm fotoğraflar: Arif Mısırlı Arşivi 2012