PART 8

ŞÜKRAN İNCE, ŞEYDANUR KAYA, ÖZGE PALABIYIK

Cyber Security and Cyber Security Insurances in the Scope of Fundamental Caution

Siber Güvenlik ve Temel Tedbirler Kapsamında Siber Güvenlik Sigortaları

ABSTRACT

The inevitable evolution of technology has made it possible for many to become a power beyond other countries, especially in the information economy, and the information warfare[1] that have emerged with this evolution and the ever-growing cyber warfare. In this direction, the critical infrastructure systems carried out by the government or the private sector have begun to adapt to information technologies as a necessity. From medicine to economy, defense systems to vital resources, many areas have begun to be controlled on the internet, and threats have increased in the same way in the cyber world.

ÖZET

Teknolojinin önüne geçilemez evriminin başta bilgi ekonomisi olmak üzere pek çok anlamda diğer ülkelerin ötesinde bir güç olma yolunda ilerlemeyi sağladığı ve bu evrim ile birlikte ortaya çıkan bilgi savaşları[1] ve her geçen gün büyümekte olan siber savaşlardan açıkça anlaşılmaktadır. Bu doğrultuda, devlet veya özel sektör eliyle yürütülen kritik alt yapı sistemleri çağın gereği olarak giderek bilişim teknolojilerine uyum sağlamaya başlanmıştır. Sağlıktan ekonomiye, savunma sistemlerinden yaşamsal kaynaklara kadar pek çok alanın, internet üzerinden kontrol edilmeye başlanmasıyla birlikte, siber dünyadaki tehditlerde de aynı oranda artmıştır.

PART 8

This study examines the role of cyber security, the steps to be taken in the name of cyber security, the emerging national and international cyber security legislation, and the functions of cyber insurances.

KEYWORDS: Cyber Attack, Cyber Security, Cyber Threat, Insurance

I. INTRODUCTION

IN PARALLEL WITH THE CHANGING SECURITY PERCEPTIONS with globalization, the relations of correlativity and dependency have increased rapidly in the cyber sense. Cyber field services, servers, web pages, etc. the tools are interconnected and each section is located in a different physical region. Yet, these instruments work together because they are mutually dependent on each other. However, each area has different inconveniences and dominance over each area requires a different technology. As a result of the fact that cyberspace is not a physical space in large proportions, the result is that cyberspace dominance is significantly different. Because the physical tools of the cyber lane lose important dominance and it takes the place of different strategy and technology. This increased correlativity has brought about many dangers. The information dissemination brought by globalization has increased the likelihood that another state will follow the military superiority that a state has earned and that it will win the same in a short period of time.[2] All these developments bring the global world order to face the threat of cyber security. This is the way to combat the threat with conventional politics, economics and security passes to get away from identifying and providing security in cyberspace effectively meaning.

The subject we will discuss in this article, respectively; the development of cyber security, cyber especially in the international area and objective elements of the security and cyber security legislation. Afterwards, we will point out cyber security insurances and in this direction, we have opinions and evaluations about the types of cyber threats and insurance coverage and collateral.

Bu çalışmada, siber güvenliğin önemi, siber güvenliğin sağlanması adına atılması gereken adımlar, yeni gelişmekte olan ulusal ve uluslararası anlamda siber güvenlik mevzuatları ile siber sigortaların işlevleri incelenmektedir.

ANAHTAR KELİMELER: Siber Saldırı, Siber Güvenlik, Siber Tehdit, Sigorta

I. GİRİŞ

KÜRESELLEŞME İLE BİRLİKTE DEĞİŞEN GÜVENLİK ALgılamaları paralelinde, siber anlamda da birbirine bağlılık, bağlantılılık ve bağımlılık ilişkileri hızla artmıştır. Siber alanda hizmetler, sunucular, web sayfaları vb. araçlar birbirine bağlıdır ve her bölüm farklı bir fiziksel bölgede yer alır. Ancak bu araçlar karşılıklı olarak birbirlerine bağımlı oldukları için birlikte çalışırlar. Bununla birlikte, her alanın farklı zorlukları vardır ve her alan üzerindeki hâkimiyet farklı bir teknoloji gerektirir. Siber uzayın büyük oranda fiziksel bir alan olmadığı gerçeğinden yola çıkarak siber alanda hâkimiyetin de önemli ölçüde farklı olduğu sonucuna ulaşılmaktadır. Çünkü siber alanda fiziksel araçlar önemli oranda hâkimiyetini kaybeder ve yerini farklı taktik ve teknolojiye bırakır. Artan bu bağlantılılık, beraberinde pek çok tehlikeyi de doğurmuştur. Küreselleşmenin getirdiği bilgi yayılımı, bir devletin kazandığı askeri üstünlüğü bir diğer devletin de takip etmesini ve aynısını kısa bir sürede kazanması, elde etmesi olasılığını arttırmıştır.[2] Tüm bu gelişmeler, küresel dünya düzenini siber güvenlik tehdidiyle yüz yüze getirmektedir. Bu tehditlerle mücadele etmenin yolu klasik siyaset, ekonomi ve güvenlik tanımlamalarından uzaklaşmak ve güvenliği siber anlamda da etkin şekilde sağlamaktan geçmektedir.

Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır.

İşbu makalemizde sırasıyla ele alacağımız konu ise; siber güvenliğin gelişimi, amacı ve unsurları başta olmak üzere uluslararası alanda siber güvenlik ve siber güvenlik mevzuatıdır. Akabinde siber güvenlik sigortalarına değinecek olup bu doğrultuda siber tehdit türlerine ve de sigorta kapsam ve teminatına ilişkin görüş ve değerlendirmelerimiz bulunmaktadır.

II. CYBER SECURITY

A. Cyber security concept and purpose

According to the definition of the United States Department of Defense, cyber space is a global field of information that is formed by a network of connected networks, which is composed of infrastructures of information technology, including Internet communication networks, embedded processors and control units.

The concept of cyber security which emerges to create safe cyber spaces for all users and to create a safe human rights environment on the cyber field means, according to the definition made by the ICTA, policies, security Technologies and Communication Authority (ICTA) in 2014; policies, security concepts, security guarantees, guidelines, risk management approaches, activities, trainings, best practices and technologies used to protect the institutions, organizations and users' assets in the cyber environment. It covers the assets of institutions, organizations and users, information processing

II. SİBER GÜVENLİK

A. Siber Güvenlik Kavramı ve Amacı

Amerika Birleşik Devletleri Savunma Bakanlığı'nın tanımına göre siber alan: İnternet iletişim ağları, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, bir birine bağlı ağların oluşturduğu bilgi ortamındaki bir küresel alandır.

Tüm kullanıcılar için güvenli siber alanları oluşturmak ve siber alanda güvenli bir insan hakları ortamı oluşturmak için karşımıza çıkan siber güvenlik kavramı ise; Bilgi Teknolojileri ve İletişim Kurumu'nun (BTK) 2014 yılında yapmış olduğu tanım ile siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür. Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon

equipment, personnel, infrastructures, applications, services, telecommunication systems and information that is transmitted and/or stored in cyber environment.

The definition of the cyber security concept is mostly based on information which is the basic material of information systems. Accordingly, in order for cyber-world to be safe, the confidentiality, integrity and accessibility of information must be ensured.[3]

Cyber attacks; when it comes to the point where all the life in a country can stop, it is understood that the security of the cyber is significant. In cyber security strategies in general; it is aimed to make the infrastructure of IT safe and resistant to attack and to provide reliable

sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

Siber güvenlik kavramının tarifi daha çok bilişim sistemlerinin temel malzemesi olan bilgi üzerinden yapılmaktadır. Buna göre siber âlemin güvenli olabilmesi için bilginin gizliliği, bütünlüğü ve erişilebilirliği sağlanması gerekmektedir.[3] Siber güvenlik stratejilerinde genel olarak; güvenli, saldırılara karşı dayanıklı ve güvenilir bir siber alanın sağlanması, bilişim sistemleri vasıtasıyla ekonomik ve sosyal refahın, güvenli iş ortamı ve ekonomik büyümenin teşvik edilmesi, bilişim ve iletişim teknolojilerinin barındırdığı risklerin kontrol altında tutulması, bilişim altyapılarının dirençli hale getirilmesi hedeflenmektedir.

cyber space, to control the economic and social welfare through information systems, to encourage safe working environment and economic growth, to control the risks of information and communication technologies and to make knowledge infrastructures resistant. At the point where cyber threats are increasing rapidly and jeopardizing security, many states are investing heavily in building security staffs, creating quality staff and providing infrastructure services. The areas that states need to secure primarily in the cyber area are; information technology, energy, financial affairs, food, health, water, transportation, public security, defense, nuclear biological and chemical facilities.[4] These areas are based on basic critical infrastructures, and the need to ensure effective safety of cyber security differs from other security measures, and the possibility of critical infrastructures being considered as a possible result of a cyber attack may be damaged. Critical infrastructure systems; deterioration of the confidentiality and integrity of the information contained therein is a system that can cause loss of life, economic harm and deterioration of public order.

Today, almost all critical infrastructures contain little or no information and communication technology and intersect with these technologies in different ways. Dams are controlled and monitored by critical infrastructure information technologies such as power generation and distribution plants. Critical infrastructures such as telecommunication are all made up of information and communication technologies.

Critical infrastructures are constructs with a large number of complex dependencies. Information and communication technologies have initiated dependencies between some critical infrastructures and have significantly increased some existing dependencies. For example, a failure in the dams, a stoppage of electricity production, problems with electricity generation cause the functionality of the Internet infrastructure to deteriorate; the interruptions on the internet will affect many critical infrastructures, being in the first place banking. For this reason, one of the most important goals of cyber security is to ensure the safety of the vital and critical infrastructures in question on a national basis.

In addition, the types and methods of crime committed with the developing technology of globalization have developed and the developing technology will continue to increase in parallel. All these show that; provision of cyber security is not only nationally limited, it is also an

Siber saldırılar bir ülkedeki bütün hayatı durdurabilecek noktaya geldiğinde siber güvenliğin önemi anlaşılmaktadır. Siber tehditlerin hızla artarak güvenliği tehlikeye düşürmesi noktasında birçok devlet güvenlik politikalarını hayata geçirmek adına kalifiye kadroları oluşturma, altyapı hizmetlerini sağlamak gibi büyük yatırımlar yapmaktadır. Devletlerin temel olarak siber alanında öncelikli olarak güvenliklerini sağlamaları gereken alanlar; bilişim, enerji, mali işler, gıda, sağlık, su, ulaşım, kamu güvenliği, savunma, nükleer biyolojik ve kimyasal tesislerdir.[4] Söz konusu alanlar temel kritik altyapılardan olup, siber güvenliğin etkin şekilde sağlanması gerekliliğinin sair güvenlik önlemlerinden farkı, olası bir siber saldırı sonucunda sayılan kritik altyapıların zarar görmesi ihtimalidir. Kritik altyapı, sistemleri içerisinde bulunan bilgilerin gizlilik ve bütünlüğünün bozulması can kaybı, ekonomik zarar ve kamu düzeninin bozulmasına sebep olabilecek sistemlerdir.

Günümüzde hemen hemen bütün kritik altyapılar, bilgi ve iletişim teknolojilerini az veya çok içermekte ve bu teknolojiler ile değişik şekillerde kesişmektedir. Barajlar, enerji üretim ve dağıtım santralleri gibi kritik altyapılar bilgi teknolojileri tarafından kontrol edilmekte ve izlenmektedir. Telekomünikasyon gibi kritik altyapılar ise tümüyle bilgi ve iletişim teknolojilerinden oluşmaktadır.

Kritik altyapılar, fazla sayıda ve karmaşık bağımlılık ilişkisi içinde olan yapılardır. Bilgi ve iletişim teknolojileri bazı kritik altyapılar arasındaki bağımlılıkları başlatmış, hâlihazırdaki bazı bağımlılıkları ise ciddi şekilde artırmıştır. Örneğin barajlardaki bir arıza, elektrik üretiminin durmasına, elektrik üretimindeki problemler internet altyapısının işlevselliğinin bozulmasına neden olurken; internetteki kesintiler ise başta bankacılık olmak üzere birçok kritik altyapıyı etkileyecektir. Bu sebeple, siber güvenliğin en önemli amaçlarından biri, bahse konu hayati ve kritik altyapıların ulusal bazda güvenliğinin sağlanmasıdır.

Ayrıca, küreselleşmenin getirdiği gelişen teknoloji ile birlikte işlenen suç türleri ve yöntemleri de gelişmiştir ve gelişen teknoloji paralel olarak artmaya devam edecektir. Tüm bunlarda göstermektedir ki; siber güvenliğin sağlanması salt ulusal anlamda sınırlı olmamakla birlikte, kişisel verilerin ve mahremiyetinin korunmasında, şebekelerin güvenliğinin ve güvenilirliğinin sağlanmasında ve siber suçlarla mücadelede önemli bir unsurdur.

important element in the protection of personal data and privacy, in ensuring the safety and reliability of networks and in fighting cyber crime. Cyber security are aimed to minimize cyber threats and attacks, as well as information and communication systems (BIS) within the scope of the security vulnerabilities.

B. Components of Cyber Security

The studies carried out on the national and international level show that; certain elements need to be completed in order to ensure full security of cyber security. These are development of national policy and strategy, establishment of legal framework, development of technical measures, determination of institutional structure, provision of national cooperation and coordination, development of capacity, awareness raising, international cooperation and harmony.

While all these efforts are being made in the provision of cyber security, it is necessary to consider the protection of fundamental rights and freedoms, compliance with the requirements of a democratic society, observance of the principle of proportionality, the involvement of all stakeholders in decision-making processes, the handling of legal, technical, administrative, economic, political and social dimensions through a holistic approach, the balance between security and usability, to take into account the legislation of other countries and to ensure compatibility as much as possible and to ensure international cooperation.

1. Domestic policy and the development of the strategies

On the national flat, there are plans for make provisions for the construction of corporative and individual cyber safety. There are many studies in our country for avoid the cyber war and safety.

Cyber warfare, in essence; digital and technological means of war, as in a physical fight in cyber warfare concept disabling infrastructure, including the notions of intelligence gathering and propaganda distribution. The cyber warfare scenarios described as conspiracy theories or myths are now becoming real. The cyber war has become a serious danger that should be taken seriously because the cyber-attacks made over the internet are carried to the virtual world.

Siber güvenlik, siber tehdit ve saldırıların yanı sıra bilgi ve iletişim sistemleri(BIS) bünyesinde yer alan güvenlik açıklarını da en aza indirmeyi amaçlamaktadır.

B. Siber Güvenliğin Unsurları

Ulusal ve uluslararası alanda yapılan çalışmalar göstermektedir ki; siber güvenliğin tam anlamıyla sağlanabilmesi için belirli unsurların tamamlanması gerekmektedir. Bunlar; ulusal politika ve stratejinin geliştirilmesi, yasal çerçevenin oluşturulması, teknik tedbirlerin geliştirilmesi, kurumsal yapılanmanın belirlenmesi, ulusal işbirliği ve koordinasyonun sağlanması, kapasitenin geliştirilmesi, farkındalığın artırılması, uluslararası işbirliği ve uyumun sağlanmasıdır.

Siber güvenliğin sağlanmasında tüm bu çalışmalar yapılırken, temel hak ve hürriyetlerinin korunması, demokratik toplum düzeninin gereklerine uyulması, ölçülülük ilkesine uyulması, karar alma süreçlerine tüm paydaşların katılımının sağlanması, bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması, güvenlik ile kullanılabilirlik arasında denge kurulması, diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması, uluslararası işbirliğinin sağlanması hususlarının dikkate alınması gerekmektedir.

1. Ulusal Politika ve Stratejilerin Geliştirilmesi

Gerek bireysel, gerek kurumsal siber güvenliğin inşası doğrultusunda alınması gereken önlemler için öncelikle ulusal boyutta adımlar atılmaktadır. Siber güvenliğin ulusal boyutta sağlanması ve siber savaşların önlenmesi amacıyla ülkemizde de çeşitli çalışmalar yürütülmektedir.

Siber savaşlar, özünde; dijital ve teknolojik yollarla yürütülen bir savaş yöntemi anlamına gelmekle birlikte; fiziksel bir savaş kavramında olduğu gibi siber savaş da alt yapıyı devre dışı bırakma, istihbarat toplama ve propaganda dağıtımı kavramlarını içermektedir. Komplo teorileri ya da efsane gibi anlatılan siber savaş senaryoları günümüzde gerçek olmaya başlamıştır. İnternet üzerinden yapılan siber saldırıların hava kara deniz ve uzaydan sonra sanal dünyaya taşınması sebebiyle siber savaş artık önemsenmesi gereken ciddi bir tehlike haline gelmiştir.

Turkey's transition to an information society has started on the 1960s with the use of e-systems. As an example; one of the 12 systems in the world, the first computer can be given at the General Directorate of Highways (October 30, 1960). In addition to that it is to understand from different sources when the internet comes into use: that in 1963 the Directorate General for State Hydraulic Works (DSI) and Is Bank had computers; the Istanbul Technical University and Middle East Technical University have arranged the first cours; that the Ministry of Interior has started the population and citizenship and the General Director started the central population project in the 1970th, the computer boom occured in 1980th, 1993 between the Middle East Technical University and the US granted Internet about a leased line and about the different employments in 1995.

Until today, three national cyber security exercises have been done in Turkey. In 2008 TR-BOME was organized by TUBITAK and ICTA in 2001 and 2013. Participants included participants in the fields of finance, education, health, law and defense, as well as those working in the field of information technology.

Türkiye'nin bilgi toplumuna geçiş için e-sistemlerin kullanımına başlaması, 1960'lı yıllara dayanmaktadır. Buna örnek olarak; Dünya'daki 12 sistemden birisi olan ilk bilgisayar Karayolları Genel Müdürlüğü'nde bulunması verilebilir (30 Ekim 1960). Ayrıca 1963'te DSİ ve İş Bankası'nın bilgisayar sahibi olduğu; İTÜ ve ODTÜ'nün 1964 ve 1965 yıllarında ilk kursları tertip ettiği; 1970'li yılların başında İçişleri Bakanlığı Nüfus ve Vatandaşlık İşleri Genel Müdürlüğünün Merkezi Nüfus İstatistikleri Projesini (MERNİS) başlattığı, 1980'lerin ortasında bilgisayarlar ortaya çıkışında patlama yaşandığı, 1993 yılında ilk defa Orta Doğu Teknik Üniversitesi ve ABD arasında kiralık bir hat üzerinden internet bağlantısı sağlandığı ve 1995'te internetin kullanılmaya başlandığı çeşitli kaynaklardan anlaşılmaktadır.

Günümüze kadar Türkiye'de üç adet ulusal siber güvenlik tatbikatı olmuştur; 2008'de TR-BOME, 2001 ve 2013'te TÜBİTAK ile BTK tarafından düzenlenmiştir. Katılımcılar arasında bilişim teknolojileri alanında çalışanların yanı sıra, finans, eğitim, sağlık, hukuk ve savunma sektörlerinden de katılımcılar olmuştur.

PART 8

Along with the process of transition to all information society in our country and in the world, a great increase in the proportion of harmful software that contains personal, commercial and political motivations against this process has occurred; the institutions and institutions of the countries have been the targets of the cyber attacks. The National Cyber Safety Strategy and the 2013-2014 Action Plan, which were published in the Official Gazette No. 28683 dated June 20, 2013 in accordance with the decision taken by the Council of Ministers, aimed to make the necessary regulations in the field of national cyber safety. The aim of the said action plan is to ensure the security of all infrastructure, information systems operated by the public or private sector, ensuring the security of all services, processes and data provided by public institutions and organizations through the use of information technology and the systems used in their presentation, to determine the strategic cyber security actions aiming at returning the systems to nor-

Ülkemizde ve dünyada yaşanan tüm bu bilgi toplumuna geçiş süreci ile birlikte, bu sürece karşı olarak kişisel, ticari ve politik motivasyonlar barındıran zararlı yazılımların oranında büyük artış meydana gelmiş; ülkelerin kurum ve kuruluşları siber saldırıların hedefi olmuştur.

Bakanlar Kurulunca alınan karar doğrultusunda 20 Haziran 2013 tarihli 28683 Sayılı Resmi Gazete 'de yayınlanarak yürürlüğe giren Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planını ile ulusal siber güvenlik alanında ihtiyaç duyulan düzenlemelerin yapılması hedeflenmektedir. Söz konusu eylem planının amacı, kamu kurum ve kuruluşlarınca bilgi teknolojileri üzerinden sağlanan her türlü hizmet, işlem ve veri ile bunların sunumunda kullanılan sistemlerin güvenliğinin sağlanmasına, kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerinin güvenliğinin sağlanmasına, siber güvenlik olaylarının etkilerinin en düşük düzeyde kalmasına, olayların ardından sistemlerin en

mal operation as soon as possible after the events, and to establish an infrastructure for the more effective investigation of the crimes committed by judicial authorities and law enforcement.

Off to 2016 the National Strategy for Cyber Safety become established and entered into force in 2016-2019. This plan comprises all components of cyber safety, inclusive the small and middle industry, all private and juristic persons, as well as public information systems and critical infrastructure information systems, which are pursued bye public or private sectors. The preparations for the strategy are fulfilled with the participation of 73 public institutions and 126 experts of public institutions, amongst others user from critical infrastructures, from the information sector, univercities and civil persons fulfill a mind platform.[5]

2. Creation of the statutory framework

There have been a number of attempts by state institutions and individuals to take precautions against the threats of cyber space. However, in order for these initiatives to produce real solutions, legal legislation and regulations need to be created and put into practice.

In this context, the US, Austria, Denmark, France, Germany, Greece, Finland, Italy, Turkey, Sweden, Switzerland, Australia, Canada, India, Japan, Spain, Portugal, England, in countries such as Malaysia and Singapore cyber security-related stringent sanctions and regulations that contain restrictions have begun to be established.

In Turkey also increased awareness of cyber security, various studies have been done recently with intensive exposure to cyber attacks and take the state needs to engage in initiatives related to cyber security measures. These activities include; Cyber Security Action Plans, National Information Security Program, National Information Security Gate, Legal Works, Cyber Security Intervention Teams and Units, Cyber Security Exercises, Conferences and Workshops and activities and formations carried out within TSK.[6]

The statutory framework of the studies build an important role in the cyber safety. Although there are not laws in matters of cyber safety, our country starts with studies in this sector and enhanced. In this case in the turkish criminal law numbered 5237 there are provisions

kısa sürede normal çalışmalarına dönmesine yönelik stratejik siber güvenlik eylemlerinin belirlenmesine ve oluşan suçların adli makam ve kollukça daha etkin araştırılmasının ve soruşturulmasının sağlanmasına yönelik bir altyapı oluşturmaktır.[5]

2016 yılı itibariyle ise, 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019 dönemi için hazırlanmış ve yürürlüğe girmiştir. Bu plan, kamu bilişim sistemlerine ve kamu ya da özel sektör tarafından işletilen kritik altyapılara ait bilişim sistemlerine ilave olarak küçük ve orta ölçekli sanayi, tüm özel ve tüzel kişiler de dâhil olmak üzere ulusal siber uzayın ülkemiz ölçeğindeki bütün bileşenlerini kapsamaktadır. Strateji hazırlıkları geniş katılım sağlanarak gerçekleştirilmiştir. Geçmiş eylem planı eylem sorumluları ile yapılan toplantıların ardından kamu kurumları, kritik altyapı işletmecileri, bilişim sektörü, üniversiteler ve sivil toplum kurumlarını temsilen 73 kurum ve kuruluştan toplam 126 uzmanın katılımı ile Ortak Akıl Platformu gerçekleştirilmiştir.

2. Yasal Çerçevenin Oluşturulması

Siber alanda oluşan tehditlere karşı devlet kurum ve bireylerin tedbirlere yönelik bir takım girişimleri oluşmaya başlamıştır. Fakat söz konusu girişimlerin gerçek çözüm üretebilmesi için yasal mevzuat ve düzenlemelerin oluşturularak uygulamaya geçirilmesi gerekmektedir.

Bu bağlamda, ABD, Avusturya, Danimarka, Fransa, Almanya, Yunanistan, Finlandiya, İtalya, Türkiye, İsveç, İsviçre, Avustralya, Kanada, Hindistan, Japonya, İspanya, Portekiz, İngiltere, Malezya ve Singapur gibi ülkelerde siber güvenlikle ilgili sıkı yaptırımlar ve kısıtlamalar içeren düzenlemeler oluşturulmaya başlanmıştır.

Türkiye'de de siber güvenlik bilincinin artması, son zamanlarda yoğun siber saldırılara maruz kalınması ve siber güvenlik tedbirleri ile ilgili girişimlerde bulunmanın ihtiyaç halini almasıyla birlikte değişik çalışmalar yapılmaktadır. Bu faaliyetler; Siber Güvenlik Eylem Planları, Ulusal Bilgi Güvenliği Programı, Ulusal Bilgi Güvenliği Kapısı, Yasal Çalışmalar, Siber Güvenlik Müdahale Ekipleri ve Birimleri, Siber Güvenlik Tatbikatları, Konferanslar ve Çalıştaylar ve de TSK bünyesinde icra edilen faaliyetler ve oluşumlar şeklinde sıralanabilir.[6]

Bu çalışmalardan yasal çerçeve oluşturma süreci, siber güvenlik tedbirleri konusunda önemli yer tutmaktadır.

about individual-related data and informatics space pain. The law numbered 5651, which is about the regulation of publication and the abatement of the crime in the internet and the law numbered 5070 contains the electronic signature law.

3. Improvement of technical measures

Some of the important cyber attacks and incidents which took place in Turkey are as following: the explosion which happened after the cyber attack to Bakü-Tiflis-Ceyhan pipeline in 2008, an hazardous software affecting the computers of Atatürk Airport in 2009, the site of the Ministry of Telecommunicitaions has been deactivated in 2011 after cyber attacks, power cut in 2015 affecting 79 provinces apart from Van and Hakkari which take their electricity from Iran, not getting access to the websites of banks, notaries and the government and to mobile applications after 10 days of cyber attacks in 2015, the cyber attack made to the hospitals of the Ministry of Health and the information in the database being stolen and erased in 2016. It is quite easy to conclude that by the usage of various technics, tactics and strategies that the cyber power provide, it is possible to create many dangers, damage and loss to the security of the country by the cyber attacks which may be realised, only by examining the given ones among thousands of cyber attacks and incidents including the ones which haven't been noticed yet or haven't been declared because of reasons such as privacy, loss of prestige etc. and haven't been reflected to open sources.

The cyber attacks which took place indicate that the legal measures for ensuring the cyber security are necessary but they are not sufficient. Expecting everything from law, jurisdiction and law enforces is not a right approach. For this reason, the softwares, equipments and business processes should be more secured by increasing their quality. For that, it should be ensured that the security standards such as ISO/IEC 15408 and TS ISO/IEC 27001 and technical guides are developed, applied and used. It should be taken into consideration that ensuring the security of the softwares, equipments and business processes can create a dissuasive effect and also create preventiveness in fights against crimes.[7]

4. Determining the institutional structuring

In the direction of applying and supervising the security measures, firstly there are the measures which should

Mevcut yasaların siber güvenlik tedbirleri açısından olmaması sebebiyle, ülkemiz bu alanda yasal çalışmalara başlamış ve geliştirilmeye devam edilmektedir. Bu kapsamda, 5237 Sayılı Türk Ceza Kanunu'na ("TCK") eklenmiş olan "Bilişim Alanında Suçlar", kişisel verilerin korunmasına yönelik hükümler, 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" ve 5070 sayılı "Elektronik İmza Kanunu yer almaktadır.

3. Teknik Tedbirlerin Geliştirilmesi

Türkiye'de yaşanmış önemli siber saldırı ve olayların bazıları; 2008'de Bakü-Tiflis-Ceyhan boru hattına siber saldırı sonrası patlama meydana gelmesi, 2009'da zararlı bir yazılımın Atatürk Havalimanı bilgisayarlarını etkilemesi, 2011'de saldırılar sonrasında Telekomünikasyon İletişim Başkanlığı'nın sitesinin devre dışı kalması, 2015'te elektriğini İran'dan alan Van ve Hakkâri hariç 79 ili etkileyen elektrik kesintisi, 2015'te, 10 gün süreli saldırılar sonucu birçok banka, noter ve devlet kurumunun internet sitesine ve mobil uygulamalara erişim sağlanamaması, 2016'da Sağlık Bakanlığı hastanelerine yönelik siber saldırılar ile veri tabanındaki bilgilerin çalınması ve silinmesi şeklindedir. Henüz farkına varılmayan veya gizlilik, saygınlık kaybı vb nedenlerle açıklanmayan ve açık kaynaklara yansımayanlarla birlikte, yaşanan binlerce önemli siber olay ve saldırının arasından sadece bunlara bakılarak, siber gücün sağladığı imkânlarla çeşitli teknik, taktik ve stratejilerin kullanılmasıyla gerçekleştirilecek siber saldırılarla ülke güvenliği için çok büyük tehlikeler, hasar ve zararlar yaratabileceği sonucuna kolaylıkla ulaşılabilmektedir.

Yaşanan siber saldırılar göstermektedir ki; siber güvenliğin sağlanması noktasında hukuki tedbirler gereklidir ancak yeterli değildir. Her şeyi hukuktan, yargıdan ve kolluk kuvvetlerinden beklemek de doğru bir yaklaşım olarak görülmemektedir. Bu itibarla, özellikle yazılım, donanım ve iş süreçlerinin kalitesinin artırılarak daha güvenli kılınması gerekmektedir. Bunun için de ISO/IEC 15408 ve TS ISO/IEC 27001 gibi güvenlik standartlarının, benzer nitelikteki teknik rehber ve kılavuzların geliştirilmesi, uygulanması ve kullanılması sağlanmalıdır. Yazılım, donanım ve iş süreçlerinin daha güvenli kılınmasının siber saldırganları caydırıcı etki yaratabileceği ve suçla mücadelede önleyiciliği sağlayabileceği de göz önünde bulundurulmalıdır. [7]

be provided by institutions and organizations to individuals and nongovermental organizations. In order to realise the mentioned measures and to solve the problems which can occur, firstly the state structuring should be ensured.

The Judgement with regard to the Conduct, Management and Coordination of the National Cyber Security Work made by the Council of Ministers on 11/06/2012, (decision no:2012/3842) has been entered in force by being published in the Official Gazette no:28447, on 20/10/2012. According to this judgement, Cyber Security Council has been formed, duties and authorities in the field of cyber security are given to the Ministry of Transport, Maritime Affairs and Communications and it has been decided that working groups and temporary commissions about cyber security can be formed.

4. Kurumsal Yapılanmanın Belirlenmesi

Siber güvenlik tedbirlerinin uygulanması ve denetlenmesi doğrultusunda öncelikle bireylere, sivil toplum kuruluşlarına, kurum ve kuruluşların sağlaması gereken tedbirler mevcuttur. Söz konusu tedbirlerin hayata geçirilmesi ve bu yolda doğabilecek sorunların çözümlenmesi için öncelikle devlet yapılanması sağlanmalıdır.

Bakanlar Kurulunca alınan 11.6.2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20.10.2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanarak yürürlüğe girmiştir. Bu karar gereğince; Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.

PART 8

The content of the mentioned Judgement of the Council of Ministers has been legislated by Annexe-1 added to the Electronic Communication Law no:5809 dated 5/11/2008 by the Code no: 6518 published on 06/02/2014 and new duties about cyber security are given to the Institution of Information Technologies and Communication, by the clauses added to the Electronic Communication Law no:5809. [8]

USOM has been established within the scope of the Ministry of Telecommunications according to the National Cyber Security Strategy mentioned above and the 4th article of the 2013-2014 Course of Action titled "The Establishment of the Center of Intervention to National Cyber Incidents (USOM) and the Formation of the Intervention Teams to Sectoral and Corporate Cyber Incidents (SOME)".[9]

İlgili Bakanlar Kurulu Kararı'nın içeriği, 06.02.2014 tarihinde yayımlanan 6518 saylı kanun ile 5.11.2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen Ek Madde 1 ile kanunlaştırılmış, 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen ek fıkralar ile Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir.[8]

Yukarıda da belirtilmiş olan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı'nın "Ulusal Siber Olaylara Müdahale Merkezinin (USOM) Kurulması ve Sektörel ve Kurumsal Siber Olaylara Müdahale Ekiplerinin (SOME) Oluşturulması" başlıklı 4. eylem maddesi uyarınca, Telekomünikasyon İletişim Başkanlığı (TİB) bünyesinde USOM kurulmuştur. [9]

USOM, ülkemizde siber güvenlik olaylarına müdahalede ulusal ve uluslararası koordinasyonun sağlanması adına kurulmuştur. İnternet aktörleri, kolluk güçleri, uluslа-

USOM is established in order to ensure the national and the international coordination in interventions to cyber security incidents in our country. The communication and coordination between the internet agents, law enforcers, international organisations, research centers and the private sector is realised by USOM. USOM is doing the alarm, warning and notice activities regarding the cyber security incidents and also ensuring the national and the international coordination in the subject of preventing the cyber attacks made to critical sectors.[10]

5. Providing national cooperation and coordination

In the national platform, anyone and any institution who has a liability in the subject of cyber security shall be conducting a work. In this regard, it is important that people should also ensure their individual cyber security besides the measures taken by ensuring the security of the information in the private institutions and organisations and governmental agencies.

Taking into consideration that, all systems and infrastructures are related to each other, it is not possible to talk about the total security without ensuring seperately the security of each system. Because of that, success of efforts and works within this field can only be obtained through cooperation and coordination.

6. Development of the capacity

New technological threats should be combatted by technical as well as legal and administrative products and solutions. Empowering of the protection of critical infrastructures and the cyber security should be provided by the new and practical solutions and the regulations of the legislation. The technical staff, lawyers and legislators should be aware of the technology in order to develop their knowledge the changing types of cyber crimes.

7. Cyber security awareness

In order for the cyber security work to succeed, awareness augmentation work should be conducted throughout the country within the private and public institutions and organiations. Accordingly, all institutions should accept the cyber security as a part of their working process and they should be conscious enough to protect their employees against the current risks and to protect the valuable properties of the company. While

rarası kuruluşlar, araştırma merkezleri ve özel sektör arasındaki iletişim ve koordinasyon USOM vasıtasıyla gerçekleştirilmektedir. USOM siber güvenlik olaylarına yönelik alarm, uyarı, duyuru faaliyetleri yapmakta, kritik sektörlere yönelik siber saldırıların önlenmesinde ulusal ve uluslararası koordinasyonu sağlamaktadır.[10]

5. Ulusal İşbirliği ve Koordinasyonun Sağlanması

Ulusal platformda, siber güvenlik hususunda sorumluluğu bulunan her kişi ve kurumun çalışma yürütmesi gerekmektedir. Bu bağlamda, özel nitelikli kurum ve kuruluşlar ve devlet kurumlarında bulunan bilgi güvenliğinin sağlanması yolunda alınan tedbirlerin yanı sıra, kişilerin de bireysel anlamda kendilerine ait siber güvenliği sağlaması önem arz etmektedir.

Tüm sistemlerin ve altyapıların birbiriyle bağlantılı olduğu göz önünde bulundurulduğunda, her bir sistemde ayrı ayrı güvenlik sağlanmadan tam bir güvenlikten bahsedilemeyeceği unutulmamalıdır. Bu sebeple de işbirliği ve koordinasyon ile çalışmaların başarılı olması sağlanmalıdır.

6. Kapasitenin Geliştirilmesi

Teknolojik anlamda ortaya çıkan yeni tehditler ile teknik ve bunun yanı sıra hukuki, idari boyutta ürünler ve çözümler vasıtasıyla mücadele edilmelidir. Kritik altyapıların korumalarının güçlendirilmesi, bilişim alanında geliştirilecek yeni ve pratik yöntemlerle ve mevzuat düzenlemeleriyle siber güvenlik etkin şekilde sağlanmalıdır. Biçim değiştiren siber suçlar doğrultusunda teknik personel, hukukçular ve kanun koyucuların teknolojiyi yakından takip ederek bilgi birikimlerini geliştirmeleri gerekmektedir.

7. Siber Güvenlik Farkındalığı

Siber güvenlik çalışmalarının başarıya ulaşabilmesi için ülke genelinde gerek özel, gerekse kamu kurum ve kuruluşları nezdinde farkındalık arttırılma çalışmaları yürütülmesi gerekmektedir. Bu doğrultuda, tüm kurumlar siber güvenliği iş süreçlerinin bir parçası olarak görebilmeli ve güncel risklere karşı çalışanlarını ve firmanın değerli varlıklarını koruyabilecek derecede bilinçli olmalıdırlar. Siber güvenliğin baş aktörleri kötü niyetli hackerlar iken, artık devletlerde siber orduları ile bu işin içinde ve dünya genelinde ciddi bir savaş halindedirler.

the chief actors of cyber security are malicious hackers, the states are now in a serious battle with cyber military forces in this business and worldwide. Especially, the document leaking activities which took place in the recent years and which created a big impact arund the world and the risks created by the world's giants reveal that the individuals and the companies are under serious risk. For this reason, collaborating with the IT Security, taking responsibility for cyber security, creating a cyber-secured environment, obliging the employees to act cyberly secured, sharing the values of cyber security and collaborating with people and institutions which have the IT knowledge for acting cyberly safe are important steps in order to increase the cyber security awareness.

8. Providing international cooperation

With the rapid development of the world, globalization and the influence of industrialization, remote control and access systems have started to be used for the management of geographically dispersed and large area infrastructures. In this respect, cooperation and integration studies of countries in international studies are facilitated and accelerated by computer systems. ENTSO- E (European Synchronous Region Network) that Turkey integrated its electrical critical infrastructure to Europe in 2010 can be given as an example. Under the roof of ENTSO-E, 41 Transmission System Operators from 34 European countries have been connected to each other by Supervisory Control and Data Acquisition (SCADA) Systems. Thus, the need to protect the information systems that control all the infrastructures of the countries has emerged.[11]

Cyber crime is an international problem that has no national boundaries and that will adversely affect many countries in the same global sense due to the nature of the cyber world. For this reason, as well as national measures, these crimes should also be avoided by international regulations. It is probable that any illegal cyber activities carried out abroad affect our country or that a person in our country conduct a cyber attack on a third country using the system of another country. Thus, cooperation between countries is essential in the search, detection and prevention of these attacks. For this reason, there are activities carried out by the European Union about cyber security as well as the United Nations and the International Telecommunication Union, Economic Cooperation and Development Organization and the Council of Europe, which our country is a member of.

Özellikle son dönemde yaşanan ve dünya genelinde büyük yankı uyandıran belge sızdırma eylemleri ve dünya devlerinin yaşattığı riskler bireylerin ve firmaların ciddi risk altında olduğunu açıkça ortaya koymaktadır. Bu sebeple, IT Güvenliği ile ekip çalışması yapmak Siber güvenlik için sorumluluk almak, siber güvenli bir ortam yaratmak, çalışanların siber güvenli davranışlarda bulunmasını mecbur kılmak, siber güvenlik değerlerini paylaşmak ve siber güvenli şekilde hareket etme yolunda IT bilgisine sahip kişi ve kurumlarla işbirliği yapmak söz konusu siber güvenlik farkındalığını arttırmak için önemli adımlardır.

8. Uluslararası İşbirliğinin Sağlanması

Dünyanın büyük bir hızla gelişmesi, küreselleşmesi ve sanayileşmenin etkisiyle birlikte, coğrafi olarak dağınık ve büyük bir alana yayılan altyapı tesislerinin yönetimi için uzaktan kontrol ve erişim sistemleri kullanılmaya başlanmıştır. Bu sayede uluslararası çalışmalarda ülkelerin işbirliği ve bütünleşme çalışmaları bilgisayar sistemleri sayesinde kolaylaşmış ve hızlanmıştır. Türkiye'nin elektrik kritik altyapısını 2010 yılında Avrupa'ya entegre ettiği ENTSO-E (Avrupa Kıtası Senkron Bölgesi Şebekesi)'yi buna örnek verebiliriz. ENTSO-E çatısı altında; 34 Avrupa ülkesinden 41 İletim Sistemi İşletmecisi Denetleme Kontrolü ve Veri Elde Etme (Supervisory Control and Data AcquisitionSCADA) sistemleri aracılığıyla birbirine bağlanmıştır. Böylece ülkelerin tüm altyapılarını kontrol eden bilgi sistemlerinin korunma ihtiyacı ortaya çıkmıştır.[11]

Siber suçlar ülkesel sınırı bulunmayan ve siber dünyanın niteliği gereği global anlamda aynı anda birçok ülkeyi olumsuz etkileyecek uluslararası bir problemdir. Bu sebeple, ulusal tedbirlerin yanı sıra uluslararası düzenlemelerle de bu suçların önüne geçilmelidir. Yurtdışında yürütülecek ve olan yasadışı siber faaliyetlerin ülkemizi etkilemesi veyahut ülkemizdeki bir kişinin başka bir ülkenin sistemini kullanarak üçüncü bir ülkeye siber saldırı gerçekleştirmesi her daim ihtimal dahilindedir. Hal böyleyken, bu saldırıların araştırılması, tespiti ve önlenmesi kapsamında ülkeler arası bir işbirliği elzemdir. Bu sebeple, ülkemizin de üyesi olduğu Birleşmiş Milletler ve bünyesinde yer alan Uluslararası Telekomünikasyon Birliği, Ekonomik İşbirliği ve Kalkınma Teşkilatı ve Avrupa Konseyi'nin yanı sıra Avrupa Birliği tarafından siber güvenlik konusunda yürütülmekte olan faaliyetler bulunmaktadır.

C. Applicable law

The resolution for the implementation, administration and coordination of the national cyber security workshop from 11.06.2012 with the was published in the Official Gazette numbered 28447 and dated 20.10.2012 and came into force at the date of publicatin. With this Resolution the cyber security council was constituted, the minister of transportation, maritime affairs and communication was accepted as a competent authority with some duties in the field of cyber security. Another point given place in the Resolution is that different working groups and commissions can be established to work in the field of cyber security.[12]

Other staturory provisions, which were regulated in Turkey are; the cyber security strategy and the acceptance

C. İlgili Mevzuat

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 20/10/2012 tarihli ve 28447 sayılı Resmi Gazete-de yayımlanarak yürürlüğe girmiştir. Bu karar gereğince Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği karara bağlanmıştır.[12]

Türkiye'de siber güvenlik alanında düzenlenen diğer mevzuatlar; 20.06.2013 tarihli 28683 numaralı Resmi Gazete'de yayınlanan Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planının Kabulü Hakkında Karar;

PART 8

of the course of action were published in the newspaper numbered 28683 on 20.06.2013; The cyber intervention team, duty and about were adviced about the procedures and principles of their work in the newspaper numbered 28818 on 11.11.2013; in the electronic communication sector the official gazette numbered 29059 on 13.07.2014 published the network and information assurance regulations; the Bülent Ecevit Univerity Karaelmas cyber security implementation and the research center regulations were published in the official gazette numbered 29059 on 13.07.2014; the provision about the information safety in the energy sector, which is used in the industrial control system published in the official gazette numbered 30123 on 13.07.2017; cyber security infrastructure protection and the research center regulations at the Kadir Has Univerity were published in the official gazette numbered 30209 on 13.10.2017; cyber security implementation and research center regulations published in the official gazette 30295 on 8.01.2018.

The law numbered 6518 dated 06.02.2014 and the law electronic communication numbered 5809 dated

11.11.2013 tarihli 28818 numaralı Resmi Gazete'de yayınlanan Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ; 13.07.2014 tarihli 29059 numaralı Resmi Gazete'de yayınlanan Elektronik Haberleşme Sektöründe Şebeke ve Bilgi Güvenliği Yönetmeliği; 13.07.2014 tarihli 29059 numaralı Resmi Gazete'de yayınlanan Bülent Ecevit Üniversitesi Karaelmas Siber Güvenlik Uygulama ve Araştırma Merkezi Yönetmeliği; 13.07.2017 tarihli 30123 numaralı Resmi Gazete'de yayınlanan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemlerinde Bilişim Güvenliği Yönetmeliği; 13.10.2017 tarihli 30209 numaralı Resmi Gazete'de yayınlanan Kadir Has Üniversitesi Siber Güvenlik ve Kritik Altyapı Koruma Uygulama ve Araştırma Merkezi Yönetmeliği; 08.01.2018 tarihli 30295 numaralı Resmi Gazete'de yayınlanan Bahçeşehir Üniversitesi Siber Güvenlik Uygulama ve Araştırma Merkezi Yönetmeliği'dir.

06.02.2014 tarihinde yayımlanan 6518 saylı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na bazı maddeler eklenerek ilgili Bakanlar Ku-

05.11.2008, have become some new articles, which were updated with the decision of the council of ministers. Moreover some new assignments about cyber security were given to the information technology and communication institution.

Furthermore, there are different international studies about the cyber security. The studies, which were attended by Turkey, were; the crime agreement, which is openend in the council of europe's virtual environment on 01.07.2014 and the council of europe cyber crime agreement and the cyber war from 23.11.2001 from the companion Tallinn.

III. Cyber Security Insurance

A. Cyber Threat and its Types

Cyber attack is a type of an electronic attack which is executed by harmful users or groups for damaging the computer systems of the government, police, banks and individuals.

The cyber attacks made by spywares used for providing information and enquiry, the attacks made for hindering or blocking the portal and the internet service, the attacks named "phishing" made with the aim of illegal deception, the attacks made by sending harmful documents by involuntary e-mail named "spam", the attacks made by listening to the network traffic, the attacks made by using the social media, social engineering, search engines, providing Free Web Service can be given as example for the mentioned cyber attacks.[13]

Cyber threats can be divided into two as software origined threats and man made threats. Software origined threats are; zombi/ghost softwares, phishing softwares, involuntary e-mail softwares, softwares with a malevolant/spy purpose while the man made threats are; organized crime syndicates, foreign intelligence services, hackers, employees who have access to the BIS and cyber terroristes.

Cyber attacks may be realised for many reasons increasing everyday such as; service hindering, critical infrastructure loss, data/information theft, fraud, data corruption, exploitation from inside, political data (information) combat, cyber terrorism, cyber crimes, malevolant hackers, vandalism, blackmail and ransom, experimental and entertainment.

rulu kararı güncellenmiş, Bilgi Teknolojileri ve İletişim Kurumu'na siber güvenlik ile ilgili yeni görevler verilmiştir.

Ayrıca siber güvenlik kapsamında çeşitli uluslararası çalışmalar da mevcuttur. Türkiye'nin de yer aldığı bu çalışmaların başlıcaları; 1 Temmuz 2014 tarihli Avrupa Konseyi Sanal Ortamda İşlenen Suçlar Sözleşmesi, 23.11.2001 tarihli Avrupa Konseyi Siber Suçlar Sözleşmesi ve Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı'dır.

III. SİBER GÜVENLİK SİGORTALARI

A. Siber Tehdit ve Türleri

Siber saldırı; zararlı kullanıcılar veya kullanıcı grupları tarafından devlet, polis, jandarma, banka veya şahısların bilgisayar sistemlerine, hesaplarına zarar vermek amacıyla gerçekleştirilen bir çeşit elektronik saldırı biçimidir.

Söz konusu siber saldırılara; bilgi ve istihbarat sağlama amacıyla kullanılan casus yazılımlar aracılığıyla yapılan saldırılar, portal ve internet hizmetinin aksatılması veya engellenmesine yönelik yapılan saldırılar, Yemleme (phishing) olarak adlandırılan ve illegal yollardan yanıltma amacıyla yapılan saldırılar, istem dışı elektronik posta olarak adlandırılan spam yöntemiyle zararlı dosyalar göndererek yapılan saldırılar, ağ trafiğini dinleyerek yapılan saldırılar, sosyal medya kullanarak yapılan saldırılar, sosyal Mühendislik, arama motorları, Ücretsiz Web Hizmeti Sunma örnek gösterilebilir.[13]

Siber tehditler yazılım kaynaklı tehditler insan kaynaklı tehditler olarak ikiye ayrılabilir. Yazılım kaynaklı tehditler; zombi/hayalet sistem yazılımları, yemleme yazılımları, istem dışı e-posta yazılımları, casus/kötü amaçlı yazılımlar iken, insan kaynaklı tehditler; organize suç grupları, yabancı istihbarat örgütleri, Hacker'lar, BİS'lere erişebilen çalışanlar ve siber teröristlerdir.

Siber saldırılar; hizmet engelleme, kritik altyapı kaybı, veri/bilgi hırsızlığı, dolandırıcılık, veri yolsuzluğu, içeriden istismar, politik, veri (bilgi) savaşı, siber terörizm, siber suçlar, kötü niyetli hacker (bilgisayar korsanlığı), vandalizm, şantaj ve fidye, deneysel veya eğlence gibi ve her geçen gün artış gösteren çeşitli amaçlarla gerçekleştirilebilmektedir.

PART 8

B. Cyber Security Insurance

Cyber security insurance also named '"data protection insurance" is a new insurance sector in our country. This sector comprises protection and consultancy for the stages of "data protection", "support in cases of crisis" and "legal proceedings" and compensation for the loss in case the incident happens.

According to the survey made by ABI Research, it is predicted that the global market for the cyber risk assurance will reach 10 milliard dolars until 2020. The main factor for the growth is stated as the increase of expenditures related to violations and attacks, risk managements strategies inclining to transfer the risk to the assurance providers.

1. Cyber Risk Assurance Warranty

The risks of cyber security are increasing every year. The loss affecting the world's economy, created by the mentioned incidents require the people and the institutions to apply for compensation methods after the loss. If the systems are affected by the attacks despite all the meaures taken, the assurance takes action and prevents that the institutions get any permanent damage.

The cyber risk insurance warrants the cost of data loss and replacement of the lost data. The loss of profit in case of work intermission and/or deceleration due to cyber attacks or malevolant softwares and additional expenditures are the subject of the cyber risks insurance policy.

B. Siber Güvenlik Sigortaları

Siber güvenlik sigortası diğer adı "veri koruma sigortası" olan bu hizmet ülkemizde yeni rastlamaya başladığımız sigorta alanlarından biridir. Bu alanda kişisel veya kurumsal müşterilerin yararlanabileceği sigorta hizmetinde başlıca "veri koruma" "kriz anında destek" ve sonrasındaki "yasal takip" aşamaları için koruma ve danışmanlık ve olayın gerçekleşmesi halinde zararın sigorta tarafından karşılanması unsurları yer almaktadır.

ABI Research'ın araştırmasına göre, küresel siber risk sigortası pazarının 2020 yılında 10 milyar dolarlık hacme ulaşacağı tahmin edilmektedir. Bu büyümenin ana etmeni olarak, siber ihlallerle ve saldırılarla bağlantılı maliyetlerin yükselmesi, risk yönetimi stratejilerinin giderek riski sigorta sağlayıcılarına devretmeye doğru itmesi gösterilmektedir.

1. Siber Risk Sigortası Teminatları

Siber güvenlik ile ilgili riskler her geçen yıl bir öncekine oranla artış göstermektedir. Bahse konu olayların dünya ekonomisine verdiği büyük ölçülü zararlar kişi ve kurumların bilgi güvenliği hususunda çeşitli zarar sonrası telafi yöntemlerine de başvurmasını gerektirmektedir. Alınan tüm önlemlere rağmen sistemler saldırıdan etkilendiği zaman ise sigorta devreye girerek kurumların kalıcı hasarlar almasının önüne geçmektedir.

Siber risk sigortaları, sigortalının veri kaybı ve kaybolan verinin yerine konma masraflarını teminat altına alır. Yine siber saldırı ve ya kötü niyetli yazılım yayılması ya-

FOOTNOTE

1 Especially in military strategies, the increase and development of information and intelligence based technologies, which are used both for defense and attack purposes, have led to the concept of "information war". This term, which was first used in 1991 during the Gulf War, is related to military strategists and international relations specialists because of the use of information technology and the use of war technology in the context of information technology.
2 **Onur Yılmaz,** "Transformational Security Perception and Cyber Safety in the Globalization Process" (Globalization and Cyber Safety), DERGIPARK, December 2017, C.II, Issue.4, p. 26
3 **Zeynep Nur Iman,** "Cyber Security and Search Engines", http://ab.org.tr/ab16/bildiri/103.pdf , Last Access Date: 25.06.2018
4 **Yılmaz,** *Globalization and Cyber Security,* p. 31
5 https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, Last Access Date; 24.06.2018
6 **Mustafa Unver, Cafer Canbay,** "Cyber Security at National and International Dimensions" (National/International Cyber Security), Electric Engineering, İssue: 438, March 2010, p. 32
7 **Unver, Canbay,** National/International Cyber Security, p.100
8 https://www.btk.gov.tr/siber-guvenlik-kurulu, Last Access Date: 25.06.2018
9 https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Last Access Date: 24.06.2018
10 https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Last Access Date: 24.06.2018
11 **Ercan Nurcan Yilmaz, Halil Ibrahim Ulus, Serkan Gonen**, "Transition to Information Society and Cyber Security", Journal of Information Technologies, Volume: 8, Issue: 3 September 2015, p. 141
12 https://www.btk.gov.tr/siber-guvenlik-kurulu, Last Access Date: 25.06.2018
13 **Yılmaz,** Globalization and Cyber Security, p. 29
14 https://www.americanbar.org/publications/gp_solo/2016/may-june/cyber_insurance_law_firms.html, Last Access Date: 24.06.2018

It is not possible to protect all the systems despite all the measures taken. Not only the small or middle scale companies but the world's giants may also be influenced by the attacks and they may be forced into terminating partially their operations.

So, the cyber security assurance assists for providing the continuity of the institution by compensating the loss occured and also helping the crisis management by giving the necessary consultancy during the process.

2. Extent of the Cyber Insurance

Cyber security insurance consists of prevention, protection and regulation. Therefore, expenses of crisis management, expenses of informing, data protection loss, data and network structuring expenditures, dignity damage, workintermission, blackmail and ransom expenditures and outsourcing liability, additional payments, cyber blackmail and multimedia costs are covered by cyber insurances so that victimization resulting from attacks can be avoided.

The first steps of cyber security insurances appear to have taken place in the United States at the beginning of the 2000s. In addition to this, in recent years, the European Union and the United Kingdom have developed this issue. In relation to this issue in the UK, lawyers included cyber security insurances within the scope of occupational risk insurances because they retain important information about their clients in the cyber environment in the context of proxy relations.[14] In our country, however, this is still one of the areas that continue to develop.

şanabilecek iş durması ve/ve ya yavaşlamasına bağlı kâr kaybı ve ek masrafları da siber riskler poliçesinin konusudur.

Bütün önlemlere rağmen tüm sistemlerin tamamen korunması söz konusu değildir. Sadece bireyler, küçük ve orta ölçekli firmalar değil, aynı zamanda dünya devleri de zaman zaman bu saldırılardan etkilenerek operasyonlarını kısmen durdurmak zorunda kalabilmektedir.

Bu durumda siber güvenlik sigortası, mevcut koruma önlemlerinin yetersiz kaldığı ve sistemin etkilendiği durumlarda hem yaşanan kayıpları telafi ederek kurumların hayatlarına devam etmesine, hem de süreç içinde gerekli danışmanlık hizmetlerini vererek kriz yönetimine yardımcı olmaktadır.

2. Siber Sigortaların Kapsamı

Siber güvenlik sigortaları; önleme, koruma ve tanzim etme şeklinde üç aşamayı kapsamaktadır. Dolayısıyla, kriz yönetimi masrafları, bilgilendirme masrafları, veri ihlali zararları, data ve networkun yeniden yapılandırılması masrafları, itibar hasarları, iş durması hasarları, şantaj ve fidye ödeme maliyetleri, dış kaynak kullanımı sorumluluğu hasarları, ek ödemelerle siber şantaj ve multimedya gibi masraflar siber sigortalar tarafından karşılanarak, saldırılar sonucu ortaya çıkan mağduriyetler önlenebilmektedir.

Siber güvenlik sigortalarının ilk adımlarının 2000'li yılların başında Amerika Birleşik Devletleri'nde atıldığı görülmektedir. Bunun yanı sıra, son yıllarda Avrupa Bir-

DİPNOT

1 Özellikle askerî stratejilerde gerek savunma gerekse saldırı amaçlı kullanılan bilgi ve istihbarat tabanlı teknolojilerin artması ve gelişmesi, "bilgi savaşı" kavramının doğmasına neden olmuştur. 1991 yılında ilk defa Körfez Savaşı esnasında kullanılan bu terim, günümüzde genelde bilgi teknolojisi ağırlıklı olmasından ötürü bilgi bilimcileri ve içeriğinde bir savaş teknolojisinin kullanılması sebebiyle de askerî stratejistleri ve uluslararası ilişkiler uzmanlarını ilgilendirmektedir.
2 **Onur Yılmaz,** "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik" (Küreselleşme ve Siber Güvenlik), DERGİPARK, Aralık 2017, C.II, S.4, s. 26.
3 **Zeynep Nur İman,** "Siber Güvenlik ve Arama Motorları", http://ab.org.tr/ab16/bildiri/103.pdf , Son Erişim Tarihi: 25.06.2018
4 **Yılmaz,** *Küreselleşme ve Siber Güvenlik,* s. 31.
5 https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, Son Erişim Tarihi; 24.06.2018
6 **Mustafa Ünver, Cafer Canbay,** "Ulusal ve Uluslararası Boyutta Siber Güvenlik" (Ulusal/Uluslararası Siber Güvenlik), Elektrik Mühendisliği, Sayı: 438, Mart 2010, s. 32
7 **Ünver, Canbay,** Ulusal/Uluslararası Siber Güvenlik, Sayfa: 100
8 https://www.btk.gov.tr/siber-guvenlik-kurulu, Son Erişim Tarihi: 25.06.2018
9 https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Son Erişim Tarihi: 24.06.2018
10 https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Son Erişim Tarihi: 24.06.2018
11 **Ercan Nurcan Yılmaz, Halil İbrahim Ulus, Serkan Gönen,** "Bilgi Toplumuna Geçiş ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, Cilt: 8, Sayı: 3 Eylül 2015, Sayfa: 141
12 https://www.btk.gov.tr/siber-guvenlik-kurulu, Son Erişim Tarihi: 25.06.2018
13 **Yılmaz,** Küreselleşme ve Siber Güvenlik, s. 29.
14 https://www.americanbar.org/publications/gp_solo/2016/may-june/cyber_insurance_law_firms.html, Son Erişim Tarihi: 24.06.2018

PART 8

IV. Conclusion

It is very significant to ensure that the cyber attacks and the security of the cyber world, where all systems with vital preservation together with globalization are inextricably linked, are inevitably harmful. Especially when the inevitable development of technology and cyber threats evolve in the same direction, it is necessary to periodically update the technical, administrative and legal measures to be taken in national and international scope. In our country, this area will also enable the necessary awareness to be increased in an institutional and individual way, and that the use of cyber insurance will take significant steps towards ensuring the protection of harmful cyber activities. ■

liği ve İngiltere'de bu konunun gelişme göstermektedir. İngiltere'de bu hususla alakalı olarak, avukatların vekalet ilişkisi kapsamında müvekkillerine ait önemli bilgileri siber ortamda muhafaza etmeleri sebebiyle mesleki risk sigortalarının kapsamı içerisine siber güvenlik sigortaları da dahil edilmiştir.[14]

Ülkemizde ise, bu husus henüz gelişme göstermeye devam eden alanlar arasında yer almaktadır.

IV. SONUÇ

Siber saldırıların ve küreselleşmeyle birlikte tüm hayati öneme sahip sistemlerin birbiriyle bağlantılı, kaçınılmaz olarak zarar görmeye elverişli olduğu siber evrende güvenliğin sağlanması oldukça önemlidir. Özellikle teknolojinin önlenemez gelişimi ve siber tehditlerin de aynı doğrultuda evrimleştiği göz önünde bulundurulduğunda, gerek ulusal gerek uluslararası kapsamda alınacak teknik, idari, hukuki tedbirlerin periyodik olarak güncellenmeleri gerekmektedir. Ülkemizde de, bu alanda gerekli farkındalığın kurumsal ve bireysel anlamda arttırılması ve siber sigorta kullanımının gelişim göstermesi zararlı siber faaliyetlerden korunmanın sağlanması yolunda önemli adımlar atılmasını sağlayacaktır. ■

BIBLIOGRAPHY

Ercan Nurcan Yılmaz, Halil Ibrahim Ulus, Serkan Gonen, "Transition to Information Society and Cyber Security", Journal of Information Technologies, Volume: 8, Issue: 3 September 2015

Mustafa Unver, Cafer Canbay, "Cyber Security at National and International Dimensions" (National/International Cyber Security), Electric Engineering, Issue: 438, March 2010

Onur Yılmaz, "Transformational Security Perception and Cyber Safety in the Globalization Process" (Globalization and Cyber Security), DERGIPARK December 2017

Zeynep Nur Iman, "Cyber Security and Search Engines", http://ab.org.tr/ab16/bildiri/103.pdf Last Access Date: 25.06.2018

https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, Last Access Date; 24.06.2018

https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Last Access Date: 24.06.2018

https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Last Access Date: 24.06.2018

KAYNAKÇA

Ercan Nurcan Yılmaz, Halil İbrahim Ulus, Serkan Gönen, "Bilgi Toplumuna Geçiş ve Siber Güvenlik", Bilişim Teknolojileri Dergisi, Cilt: 8, Sayı: 3, Eylül 2015

Mustafa Ünver, Cafer Canbay, "Ulusal ve Uluslararası Boyutta Siber Güvenlik" (Ulusal/Uluslararası Siber Güvenlik), Elektrik Mühendisliği, Sayı: 438, Mart 2010

Onur Yılmaz, "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik" (Küreselleşme ve Siber Güvenlik), DERGİPARK, Aralık 2017

Zeynep Nur İman, "Siber Güvenlik ve Arama Motorları", http://ab.org.tr/ab16/bildiri/103.pdf , Son Erişim Tarihi: 25.06.2018

https://www.btk.gov.tr/siber-guvenlik-stratejisi-ve-eylem-plani, Son Erişim Tarihi; 24.06.2018

https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Son Erişim Tarihi: 24.06.2018

https://www.btk.gov.tr/usom-ve-kurumsal-siber-olaylara-mudahale-ekibi, Son Erişim Tarihi: 24.06.2018