ISSN: 2587-1218

CYBERPOLITIK JOURNAL
Siber Politikalar Dergisi

A Peer Review International E-Journal on Cyberpolitics, Cybersecurity and Human Rights

www.cyberpolitikjournal.org

Summer 2023

ISSN: 2587-1218

ABOUT THE JOURNAL

Owner/Sahibi

On behalf of Association for Human Rights Education / İnsan Hakları Eğitimi Derneği adına
Prof. Dr. Nezir Akyeşilmen

Peer Review

All articles in this journal have undergone meticulos peer review, based on refereeing by anonymous referees. All peer review is double blind and submission is online. All submitted papers (other than book and article reviews) are peer reviewed.

The Journal

The languages of the Journal are both Turkish and English.

ISSN 2587-1218

Cyberpolitik (CP) aims to publish peer-reviewed scholarly articles and reviews as well as significant developments regarding cyber world, cybersecurity, cyberpolitics and human rights.

Indexing/Endeksler

Cyberpolitik Journal is being indexed by;

* Academia Social Science Index (ASOS),
* Scientific Indexing Services (SIS),
* Eurasian Scientific Journal Index (ESJIndex),
* Index Copernicus International (ICI), (ICV 2017=64.65)
* Directory of Research Journal Indexing (DRJI).
* JournalITOCs.

* Open-Web.info.
* Google Scholars

Issue Referees / Sayı Hakemleri

Prof.Dr. Bilal Sambur
Prof. Dr. Nezir Akyeşilmen
Assoc. Prof. Dr. Fulya Köksoy
Assoc. Prof. Dr. Murat Tümay
Assist. Prof.Dr. Ayşegül Sili Kalem
Dr. Begüm Burak

Cyberpolitik consists of the following sections:

Research Articles: Each Volume would publish a selection of Articles covering aspects of cyber politics and human rights with a broad universal focus.

Comments: This section would cover recent developments in the field of cyber politics and human rights.

Book/Article Reviews: Each Volume aims to review books on cyber politics, cybersecurity and human rights.

Cyberpolitik Award: Each year one '*Cyberpolitik*' prize will be awarded, for the best article from material published in the previous year.

ISSN: 2587-1218

CONTENTS / İÇİNDEKİLER

EDITORIAL PREFACE: THE AGE OF DIGITAL EMPIRES: TRANSFORMATION OF INTERNATIONAL POLITICS ____ vi

Nezir AKYEŞİLMEN

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ ____ 1

CYBER SECURITY POLICIES OF TURKIYE AND ENGLAND DURING THE PANDEMIC PERIOD ____ 2

Gül Nazik ÜNVER

OPINIONS / YORUMLAR ____ 17

EMBRACING CYBERSPACE: MALAYSIA AND THE CYBER SECURITY INITIATIVES 18

Sonny ZULHUDA

DO ALIENS PERFORM CYBER- ATTACKS ON GLOBAL NETWORK? ____ 24

Nezir AKYEŞİLMEN

INTERVIEWS / RÖPORTAJLAR ____ 29

MALAYSIA'S EFFORT TO STRENGTHEN CYBERSECURITY ____ 30

Mahyuddin Bİn DAUB

Kamil TARHAN

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ ____ 40

CYBERSECURITY FOR BEGINNERS ____ 40

Gül Nazik ÜNVER

NOTES FOR AUTHORS / YAZARLAR İÇİN NOTLAR ____ 46

ISSN: 2587-1218

EDITORIAL PREFACE: THE AGE OF DIGITAL EMPIRES: TRANSFORMATION OF INTERNATIONAL POLITICS

Dear Readers,

We are proud to present to you the fifteenth issue of the *Cyberpolitik* Journal. It is a great honor for all of us to continue our journey that we started eight years ago without interruption. As the digital world grows every day and every second, new developments and new technologies emerge, we are trying to read and understand this area within our limitations. This issue has new researches and indept analysis.

This volume deals with a number of topics ranging from cybersecurity strategis, to cyber attacks by aliens, from malasian cybersecurity policies to cybersecurity measures at all levels.

To start with the age of empires

The age of digital empire is upon us. We are living in a time when technology has become so pervasive that it is shaping every aspect of our lives, from the way we communicate to the way we shop.

Digital empires are state actors that have amassed enormous power and influence through their control of digital technology, artificial intelligence, IoTs and big data. Today the USA, China, Russia and the EU are considered as digital empires. Some also use the same concepts for bigtech companies, such as Google, Amazon, Facebook, and Apple, have come to dominate our lives in ways that were unimaginable just a few decades ago. Yet, these companies also belong to the states mentioned or the EU.

Digital empires have the power to shape our thoughts, our behavior, and even our political beliefs. They can control what we see, what we hear, and what we buy. They can also use their data to target us with personalized advertising that is designed to influence our behavior. The rise of digital empires raises a number of important questions about the future of our society. How can we protect our societies from their interference? How can we protect our privacy and our personal data? And how can we ensure that everyone has access to the benefits of the digital age?

These are just some of the challenges that we will need to address in the age of digital empire. It is a time of great change and uncertainty, but it is also a time of great opportunity. We can use technology to make our lives better, but only if we are careful about how we use it.

Here are some of the key characteristics of the age of digital empire:

- The rise of data as a new form of currency. In the age of digital empire, data is more valuable than ever before. Some states and even companies are collecting vast amounts of data about our online activities, and they are using this data to target us with cyber attacks, with personalized advertising and to influence our behavior.
- The growing power of algorithms. Algorithms are now used to make decisions about everything from cyber armies to cyber weapons. From communication to trade. From entertainment to education. These algorithms are often opaque and biased, and they have the potential to create new forms of discrimination.
- The decline of trust in traditional institutions. As people become increasingly reliant on digital platforms, they are also becoming more skeptical of traditional institutions, such as governments and the media. This decline in trust has created an environment in which digital empires can thrive.

The age of digital empire is still in its early stages, but it is clear that it is already having a profound impact on our lives. As we move into the future, it is important to be aware of the challenges and opportunities that this new era presents.

The USA

The United States is often considered to be a digital empire, due to the dominance of American technology and its companies in the global market. The rise of American digital empires has been accompanied by concerns about the potential it to abuse its power. There have been allegations that the USA and its companies have engaged in anti-competitive practices, that they have harvested our personal data without our consent, and that they have used their platforms to spread misinformation and propaganda.

These concerns are valid, and they need to be addressed. However, it is also important to recognize the benefits that American digital empires have brought to the world. These companies have created jobs, they have driven innovation, and they have made it possible for people all over the world to connect and share information.

China

China is also considered to be a digital empire, due to the dominance of Chinese technology companies in the domestic market and their increasing presence in the global market. Some of the most well-known digital empires in China are:

- Alibaba: Alibaba is the world's largest e-commerce company, and it also owns a number of other popular digital platforms, such as Taobao and Alipay.
- Tencent: Tencent is the world's largest gaming company, and it also owns a number of other popular digital platforms, such as WeChat and QQ.
- Baidu: Baidu is the world's leading search engine in China, and it also owns a number of other popular digital platforms, such as iQIYI and Baidu Maps.
- Huawei: Huawei is the world's largest telecommunications equipment manufacturer, and it is also a major player in the smartphone market.
- ZTE: ZTE is another major telecommunications equipment manufacturer in China, and it is also a major player in the smartphone market.

These companies have amassed enormous power and influence through their control of digital platforms and data. They have the power to shape the Chinese economy and society, and they are increasingly playing a role in the global economy.

The rise of Chinese digital empires is a major development in the 21st century. It is a trend that is likely to continue in the years to come. As these companies become more powerful, it is important to ensure that they are held accountable and that they do not abuse their power.

Russia

Russia is not typically considered to be a digital empire in the same way that the United States and China are. The Russian government has been actively promoting the development of the country's digital economy. The government has invested heavily in research and development, and it has created a number of favorable policies for technology companies. As a result, Russia is home to a number of innovative technology companies that are making a significant impact on the global market.

However, the Russian government also has a history of using technology to control its citizens and to interfere in foreign affairs. This raises concerns about the potential for Russia

to use its digital power to achieve its own political and strategic goals. This reality is a fact for al the states, particularly for those considered as digital empires.

The rise of Russia as a digital power is a major development that is having a significant impact on the global economy and society. It is important to be aware of the potential benefits and risks of this trend, and to ensure that Russia's digital power is used responsibly.

The European Union

The European Union (EU) is set of states that try to have a common digital policies and regulations. As a Union it is a big market and significant player in the global digital sphere. The EU is home to a number of large technology companies, such as SAP, Amadeus, and Spotify. These companies are playing an increasingly important role in the global digital economy.

The EU is also a major force in the development of digital regulation. The EU has enacted a number of laws that are designed to protect consumers, promote competition, and ensure the responsible use of data. These laws are having a significant impact on the way that technology companies operate in the EU and around the world. The EU is also investing heavily in research and development in the field of digital technology. The EU is funding a number of projects that are aimed at developing new technologies, such as artificial intelligence and quantum computing. These projects are helping to position the EU as a leader in the development of new digital technologies.

Here are some of the key characteristics of the European Union's digital empire:

- A focus on regulation and competition: The EU is committed to regulating the digital economy in order to protect consumers, promote competition, and ensure the responsible use of data. This approach has been controversial, but it has also helped to make the EU a leader in digital regulation.
- A focus on research and development: The EU is investing heavily in research and development in the field of digital technology. This investment is helping to position the EU as a leader in the development of new digital technologies.
- A focus on open standards and interoperability: The EU is committed to open standards and interoperability in the digital economy. This approach is designed to

promote innovation and competition, and it is also helping to make the European digital market more accessible to businesses and consumers.

The European Union's digital empire is still in its early stages, but it is growing rapidly. The EU is well-positioned to become a major digital power in the future.

The Impacts on International Politics

Digital empires are transforming international politics in a number of ways. They are:

- Reshaping the balance of power: The rise of digital empires, such as the United States, China, and the European Union, is challenging the traditional balance of power in international politics. These digital empires are not only economic and military powers, but they are also wielding significant influence in the digital world.
- Changing the nature of warfare: Digital technologies are being used to wage new forms of warfare, such as cyberwarfare and information warfare. These new forms of warfare are blurring the lines between traditional military conflict and peacetime competition.
- Eroding national sovereignty: Digital empires are collecting vast amounts of data about individuals and organizations around the world. This data can be used to track people's movements, monitor their communications, and influence their behavior. This raises concerns about the erosion of national sovereignty and the protection of individual privacy.
- Challenging the international order: The rise of digital empires is challenging the existing international order, which is based on the principles of sovereignty, non-interference, and multilateralism. Digital empires are increasingly acting unilaterally and disregarding international norms. This is creating uncertainty and instability in the international system.

The transformation of international politics by digital empires is still in its early stages. It is unclear how this transformation will play out in the long run. However, it is clear that digital empires are having a significant impact on the way that countries interact with each other.

Here are some additional ways that digital empires are transforming international politics:

- They are creating new opportunities for cooperation and collaboration. For example, digital empires can work together to combat cybercrime and promote the free flow of information.
- They are also creating new challenges for cooperation. For example, digital empires may compete for control of key infrastructure, such as undersea cables and data centers.

- Digital empires are also changing the way that people communicate and interact with each other. This is having a profound impact on the way that people form opinions and make decisions.

The rise of digital empires is a major development in international politics. It is important to understand the implications of this development for the future of the international system.

Conclusion

The rise of digital empires is a major development in the 21st century. The United States, China, Russia, and the European Union are all vying for dominance in the digital economy. These countries are investing heavily in research and development, and they are enacting laws and regulations that are designed to shape the future of the digital world.

The rise of digital empires has a number of implications for the global economy and society. These companies have the power to shape our thoughts, our behavior, and even our political beliefs. They can control what we see, what we hear, and what we buy. They can also use their data to target us with personalized advertising that is designed to influence our behavior.

The rise of digital empires also raises concerns about the potential for these companies to abuse their power. There have been allegations that these companies have engaged in anti-competitive practices, that they have harvested our personal data without our consent, and that they have used their platforms to spread misinformation and propaganda.

These concerns are valid, and they need to be addressed. However, it is also important to recognize the benefits that digital empires have brought to the world. These companies have created jobs, they have driven innovation, and they have made it possible for people all over the world to connect and share information.

The rise of digital empires is a complex issue with no easy answers. It is important to be aware of the potential benefits and risks of this trend, and to work together to ensure that digital empires are used responsibly.

Nezir Akyesilmen, Ph.D

Editor-in-Chief

RESEARCH ARTICLES / ARAŞTIRMA MAKALELERİ

CYBER SECURITY POLICIES OF TURKIYE AND ENGLAND DURING THE PANDEMIC PERIOD

Gül Nazik ÜNVER*

ORCID ID: 0009-0005-5003-1555.

Abstract

The World Health Organization (WHO), which officially announced global health emergency in January 2020, declared that the COVID-19 outbreak was a pandemic by 11 March. Since then, the pandemic has become global. The pandemic spread rapidly between countries and affected almost every community in many ways. This shows that it especially affects politics, economy, health, culture, education and technology.

This study claims that the policy and strategy, economic sector, health sector, education and training and technologies of Türkiye and England were adversely affected during the pandemic period and that countries developed cyber security policies for these elements. This study highlights that lockdowns, quarantines and other preventive measures have far-reaching effects on the political and economic well-being of countries around the world, including Türkiye and England. In addition, this study analyzes and provides an overview of the Turkish and British governments' response to COVID-19 in terms of cybersecurity policies, in order to demonstrate the far-reaching and potentially long-term consequences of the virus on the future of countries.

Keywords: Global Epidemic, Pandemic, Covid-19, Türkiye, England, Cyber Security Policies.

PANDEMİ DÖNEMİNDE TÜRKİYE VE İNGİLTERE'NİN SİBER GÜVENLİK POLİTİKALARI

Özet

2020 yılında ocak ayında resmi olarak küresel acil sağlık durumunu ilan eden Dünya Sağlık Örgütü (WHO), 11 Mart'a gelindiğinde COVID-19 salgınının bir pandemi olduğunu bildirmiştir. O zamandan beri, pandemi küresel bir hâl almıştır. Pandemi ülkeler arasında

* Dr., Selcuk University, IR, E-mail: gulunver@outlook.com This study was produced from the author's PhD thesis. For Detailed Information: Ünver, Gül Nazik (2023). *Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği*, PhD Thesis, Konya: Selcuk University.

hızla yayılmış ve neredeyse her topluluğu birçok açıdan etkilemiştir. Bu da özellikle siyasi, ekonomik, sağlık, kültür, eğitim-öğretim ve teknolojiyi etkilediğini göstermektedir.

Bu çalışma, pandemi döneminde hem Türkiye'nin hem de Birleşik Krallık'ın siyaset ve strateji, ekonomik sektör, sağlık sektörü, eğitim ve teknoloji açısından olumsuz etkilendiğini ileri sürüyor. Ayrıca bu ülkelerin bu sorunları çözmek için siber güvenlik politikaları geliştirdiklerini ileri sürüyor. Bu çalışma tecritler, karantinalar ve diğer önleyici tedbirlerin, Türkiye ve İngiltere'de dahil olmak üzere dünyanın dört bir yanındaki ülkelerin siyasi ve ekonomik refahı üzerinde geniş kapsamlı etkileri olduğunu vurgulamaktadır. Ayrıca bu çalışma, virüsün ülkelerin geleceği üzerindeki geniş kapsamlı ve potansiyel olarak uzun vadeli sonuçlarını sergilemek amacıyla Türk ve İngiliz hükümetlerinin COVID-19'a verdiği yanıtı siber güvenlik politikaları açısından analiz etmekte ve genel bir bakış sunmaktadır.

Anahtar Kelimeler: Pandemi, Covid-19, Türkiye, İngiltere, Siber Güvenlik Politikaları.

Giriş

An unknown type of disease has been detected in the city of Wuhan, China's Hubei province. This disease was officially reported by the World Health Organization (WHO) on 31 December 2019. In January, WHO named this disease COVID-19 and declared it a "Public Health Emergency of International Concern". While cases of COVID-19 are increasing rapidly, WHO announced on 11 March 2020 that this disease has become a pandemic (WHO, 2020).

Politicians who want to control the spread of the pandemic have taken some measures with various restrictions. On January 23, 2019, China imposed a lockdown in Hubei province and restricted the use of public transport. In the initial phase of the pandemic, such regulations have received widespread criticism from various international organizations for their negative consequences on human rights and freedoms in non-democratic countries. In March 2020, the focus of infections shifted from China to Europe, especially Italy. The infection spread rapidly, passed to Türkiye and England, and although it affected these countries to a large extent, the primary form of quarantine began to be widely used. To date, approximately 180 countries, at local or national level, have implemented some degree of mandatory lockdown. This has resulted in the closure of education systems and the restriction of most commercial activities (Ünver, 2023: 108-110).

In Türkiye and England, the pandemic has become a national security issue as a priority at the same level as national security concerns such as cyber attacks and the proliferation of weapons of mass destruction, thus increasing the importance of the national economy. In addition to the fiscal and monetary measures implemented to prevent the economic crisis and stimulate the economy, the disproportionate effects of isolation, quarantine and restrictions on private sector workers have increased income and wealth inequalities. In addition, economic fluctuation in these countries can widen racial and socio-economic divisions and increase social unrest (Unver, 2023: 109).

Individuals are said to be the weakest link in cybersecurity (Akyesilmen, 2018). Individuals are the target of two types of attacks during the pandemic. The first is social engineering. This reveals that individuals have insufficient knowledge in cyber security. The second is logical engineering. Logical engineering, on the other hand, targets a system or technology. It reveals outdated and defensively weak software. The "new normal" process of remote work is focused on cybersecurity, data protection, policy enforcement, and rule-compliance. The pandemic has made it possible for state institutions and organizations, private sectors to face their digital preparations in the direct fight against cyber threats and attacks.

While institutions and organizations offer secure virtual private network (VPN) access to their employees, the level of cyber security is insufficient in networks used in the home environment. The existence of Information and Communication Technologies (ICT) in situations where physical interactions are not possible makes it possible to continue education and training. However, both teachers and students need to be very familiar with these technologies and their uses in order to be effective in distance education.

After the COVID-19 based cyber attacks, cyber-network users in the home environment need to be informed about accounts, logins, remote maintenance, software updates, security of home network routers and integration of home-based printers, IoT devices. It is important for organizations to conduct exercises and work in this area to increase their ability to detect, respond and recover from cyber threats and attacks in a timely manner.

By examining the cyber security strategy documents of Türkiye and England, it is expected to ask and answer research questions that allow states to better understand different practices and procedures during the pandemic:

When did the global epidemic arise and how did it spread?

How does the pandemic relate to cybersecurity?

What will be the effects on Türkiye's domestic and foreign policy during the pandemic?

What will be the effects on England's domestic and foreign policy during the pandemic?

What kind of changes have occurred in physical education and cultural activities in Türkiye and England?

Why have institutions and organizations switched to individual online work environments?

Will the pandemic affect the steps to be taken by the Turkish and British governments, and if so, what path will the states follow?

This study will try to answer these and similar questions, and in the light of these questions, it will provide some explanations and predictions about these issues. This study aims to evaluate the attitudes of Türkiye and England in terms of cyber security policies during the periods when the effect of the pandemic reached its maximum. For this purpose, firstly, Türkiye's cyber security policies during the pandemic period, and secondly, Britain's cyber security policies during the pandemic period. In this study, it is claimed that the pandemic has affected countries in many ways.

The Relationship between Pandemic and Cyber Security: The Case of Türkiye

On March 11, 2020, then-Minister of Health Fahrettin Koca reported the country's first positive COVID-19 case. As the number of cases continues to rise in the country, the government has imposed lockdowns and restrictions. After the isolation and restrictions increased towards the end of March, many non-governmental organizations publicly expressed their concerns. Health Minister Fahrettin Koca announced 14 rules against the risk of the pandemic to the public (https://dhf.marmara.edu.tr/).

Epidemics leave lasting effects on the memories of societies. It can affect many aspects, such as political, psychological, social and economic, beyond catching a disease or resulting in death. The COVID-19 pandemic, which has shown its impact in the political, strategic, economic, education-training, technology and cultural fields in Türkiye, has revealed wide-ranging results in the country. The COVID-19 pandemic has been likened to the 1918 Spanish flu by many experts. The number of people who died due to the pandemic in Türkiye in 2020 and 2021 was 87 thousand 334 people (TUIK, 2023) according to the data of the Turkish

Statistical Institute (TUIK), and 101 thousand 492 people in 2022 according to the data of the Ministry of Health (Ministry of Health, "Covid-19 Information Platform").

Table 1: Cyber Security Policies of Türkiye and England During the Pandemic

	Türkiye	**England**
The number of cases infected with the disease according to the World Health Organization (WHO) data	17.004.677	20.470.658
The number of deaths from the disease according to the World Health Organization (WHO) data	101.419	227.272
Vaccination procedures for COVID-19 were given importance	Yes	Yes
Education was suspended and distance education system was started.	Yes	Yes
Students who received physical education at universities attended classes online from their homes and took exams.	Yes	No
The economy has been adversely affected and economic stagnation has emerged in the international arena.	Yes	Yes
Density in health institutions and organizations has increased	Yes	Yes
Compared to previous periods, an increase in cyber attacks has been observed	Yes	Yes
Cyber security policies have been made and tried to be implemented	Yes	Yes
Efforts and initiatives of governments for cyber security measures against cyber attacks in this process	Yes	Yes
Cyber security vulnerabilities have been experienced and security vulnerabilities have emerged	Yes	Yes
Isolation and quarantine measures were applied, various restrictions were made	Yes	Yes
An increase has been observed in Information and Communication Technologies	Yes	Yes
Use of masks and other personal protective equipment in daily life	Yes	Yes

Anxiety and concern have increased in most of the public during the pandemic	Yes	Yes
In the 2020 and beyond National Cyber Security Strategy Documents, the importance of acting quickly and cautiously in times of crisis such as pandemics is mentioned.	Yes	Yes
During the pandemic process, individuals have complied with the messages and rules given by the state.	Yes	Yes
Risk planning for future risks, threats and emergencies	Yes	Yes

Source: Produced from the author's PhD thesis.

In the light of the information given in Table 1, although there is a significant difference between TurkStat and the Ministry of Health, the World Health Organization (WHO) announced the number of people who died from the pandemic in Türkiye as 101 thousand 419 people (WHO, 2023). The human costs in terms of lives lost are lastingly affecting global economic growth, in addition to rising poverty levels, economic recession, unemployment, costs of healthcare facilities and rising social unrest. Approximately 17 million 4 thousand cases of global epidemics have been detected (WHO,2023).

According to policy makers, Türkiye was thought to have relatively coped with the pandemic, given the low number of confirmed cases in the early stages of the pandemic, the low number of patients (the adequacy of the infrastructure in the hospitals, especially the intensive care beds in terms of the number of patients), and timely isolation and follow-up measures. However, as the disease spread, some administrative and capacity problems emerged.

By 2021, the Turkish government has started many vaccination processes, which are known as CoronaVac, Sinovac, BioNTech, Turkovac, with a public announcement. It originally emerged as a vaccination campaign involving healthcare workers, the elderly, and people in nursing homes. As the pandemic spread, vaccination has become mandatory. People go to hospitals, their jobs, shopping malls, banks etc. In order to enter many institutions, they had to verify their information showing that they were vaccinated.

During the pandemic period in the international system, Türkiye has provided many assistance regarding COVID-19 outside its borders (sending medical aid support such as

masks and other personal protective equipment to many countries) and has taken a proactive approach to improve the country's global image.

During the pandemic period, Türkiye's health sector and economy have been adversely affected. Especially among those who manage small and medium-sized enterprises and those whose income is below a certain level, dependence on government support packages has increased. In this respect, it is clear that security (including food, health, economics, education and cybersecurity) is more important than freedom for most individuals. Stating that it was not unusual to resort to the intervention of state power in Türkiye until the pandemic process, Güder (Güder, 2020) reminded in his study that nation-states had been waiting for such an action for a long time. During the pandemic, globalists, supporters of nation-states and populist movements have been the main actors of new power struggles.

Health sector and economic forecasts in Türkiye reflected the continuing risks to a sustainable global recovery with potential inflationary pressures due to increased infectious cases and consumer demands. These risks are coupled with the highlights of the pandemic, which has challenged national efforts to emerge new epidemic variants and contain infections.

As the COVID-19 pandemic worsens in countries around the world, most governments have taken measures to close their schools to contain the spread of the virus. Some changes have been made in the education process in Türkiye. In Türkiye, excluding the non-compulsory part of the curriculum, schools were closed for approximately 23 to 30 hours of face-to-face compulsory education (every week when schools are closed, primary-secondary education in general) and the education-teaching process was switched to the online system. Schools have been forced to replace this time with online learning and homeschooling, which in many cases is facilitated by teachers and parents. After the school closures that lasted for weeks, a complex process has begun in Türkiye, such as the gradual reopening of schools, as in some countries (Unver, 2023: 110-111). In addition to professional standards in universities in Türkiye, academic and educational standards are based on the Bologna process. The Bologna process is the reference frame of the European Union's higher education agenda (Toprak et al. 2020: 183).

The pandemic has increased concerns about cybersecurity. In particular, the uncertainty experienced in the structure of the international system has revealed some discontents such as disorder and unprincipled and caused them to be questioned. It has been important to conclude the current situation somehow and to structure the discourse of the new world order.

The pandemic has accelerated this process. Adil Karaismailoğlu, Minister of Transport and Infrastructure, announced that during the pandemic process, cyber attacks against Türkiye decreased from 118 thousand 470 to 84 thousand 113 in 2020 (Daily Sabah, 27.02.2022). In addition, the Minister stated that the "cyber shield" was strengthened against cyber attacks. He added that the National Cybersecurity Response Center (USOM) teams are working in coordination to detect malware and cut off hackers' access to critical infrastructure. Apart from these, he emphasized that he used the infrastructures of software components called "Kasırga, Avcı and Azad" to provide cyber security and prevent attacks (Daily Sabah, 27.02.2022). These programs use artificial intelligence to provide cyber security and stay up-to-date against cyber attacks and threats (Unver, 2019).

The Relationship between Pandemic and Cyber Security: The Case of England

In England, the pandemic has given rise to what has been called the "new normal" in terms of societal norms, the way of living and working. The pandemic has brought with it a unique series of cyber attacks and threats affecting society, institutions and organizations. The increase in the concerns that caused the epidemic in England has also revealed the increase of cyber attacks and threats. The increase in remote working and education due to the pandemic has also increased the number of malware and threats.

In 2020, the COVID-19 pandemic has disrupted lives in all countries and communities globally. The pandemic has started a process where the future is uncertain and the "new normal" life is revealed. It has left global economic growth beyond what has been experienced in nearly a century. It has had maximum effects on global politics and economic growth. In June 2020, many states could not achieve economic development and progress. By September, the British economy recovered quickly and has made positive progress in economy-based charts since then.

England is one of the countries negatively affected by the pandemic. In the context of England's response to the COVID-19 outbreak in March 2020, the repeated and consistent message "stay at home, protect the NHS and save lives" stated that the pandemic is an important process in this country (Mott, 2023: 165). In September 2021, the emergence of the COVID-19 Delta variant showed that the virus spread rapidly on a global scale and the virus mutated. In this period, England brought travel restrictions to the agenda and began to demand additional health measures (Unver, 2023: 108-109).

In the light of the information given in Table 1, the World Health Organization (WHO) announced the number of deaths from the pandemic in England as 227 thousand 272 people (WHO, 2023). Approximately 24 million 470 thousand cases of global epidemics have been identified (WHO, 2023). In England, the pandemic has led to changes in the risky discourse mediating between government officials, academia, IT professionals and individuals. By June 2020, many states had imposed extensive restrictions on behavioral patterns, including political, strategic, educational, economic and social activities, and tried to limit the spread of the epidemic. The British people also experienced these restrictions. The British government has renounced far-reaching behavior to the extent that it is criminalized through the 2020 Coronavirus Act in its effort to limit infections, hospitalizations and deaths (Mott, 2023: 161). Such widespread and relatively short-term restrictions and lockdown policies have been implemented to increase the lifespan of the population and protect critical systems and services that rely on them (BBC News, 2020).

The message given by the government in the first stage of the pandemic in England was important for individuals to comply with the rules. According to the information given in Table 1, individuals complied with these rules at a high rate and this showed that it is important in ensuring that the British people obey the rules. Such messages fit within the framework of securing the relationship between vital systems. Three recommendations are given on cybersecurity preparedness in England. The first recommendation is to take expertise from a broader discipline and develop plans backed by international best practice. The British government should ensure that England is "a world leader for coordinating international risk planning", with comprehensive and up-to-date plans for "future risks and emergencies" (UK Parliament, 2021: 30). The second recommendation is for the British government to develop cybersecurity policies for "future threats". The third recommendation is to ensure that arrangements are made and tested that will "allow instantaneous data flow between institutions involved in emergencies". These recommendations are important for the implementation of England's cyber security policies. In the first days of the crisis, data and information may be insufficient and time may be required for analysis. In such a situation, it may be important to act quickly and cautiously rather than waiting for greater scientific certainty (UK Parliament, 2021: 59; see. Table 1). Providing these recommendations in the future The development of various cybersecurity strategy documents in England appears to reflect risk planning for future emergencies in this area.

England has taken a series of steps to ensure economic development and progress. The Bank of England (BOE), which predicts that the British economy will shrink by 30% in May 2020, has predicted that the British economy will enter a "V" shaped recovery process towards the end of May (Jackhson, 2021: 91).

England National Cyber Security Center (NCSC) issued a joint cyber alert with the US Cyber Security and Infrastructure Agency (CISA) on May 5, 2020, to both health and medical research organizations. There is a comprehensive risk assessment process in England. The cybersecurity triad of protecting the confidentiality, integrity and availability of data is more evident in the health and economic sectors. Still, there are some projections to improve the British government's security risk planning (Hilton; Baylon, 11.2020: iv):

- Institutions and organizations should have a mechanism that provides full expertise or oversight to ensure adequate cybersecurity risk plans.
- Although England is one of the countries affected by COVID-19, it has not made any long-term "isolation or quarantine plans".
- It is known that England has good risk management processes in the international system. But according to the National Security Risk Assessment (NSRA), the problems are so great that the risks to England are not identified.
- The British government should give importance to planning processes related to cyber security policies, making risk assessments and improving risk plans.

In its cybersecurity policies, England has defined critical infrastructure as the networks and other systems required to keep it operational and to provide essential services (e.g. energy, finance, health, communications, education and water services) for which a significant portion of the National Critical Infrastructure (CNI) is privately owned (Cabinet Office, 2017: 5).

It has been discussed during the pandemic that cyber security policies have been transformed into high-level government strategies, but that these policies will be necessary for England to provide cyber security. For example; Mandatory reporting of cyber incidents in key sectors is a consideration for the British government (Mott, 2023: 163).

England government strategy covering 2022-2030 states: "It is necessary to ensure that government functions and services are resilient to the cyber threats and attacks it faces" … "England as a cyber power is an authority that attaches importance to acting together with

institutions and organizations that protect and advance the British economy, culture and society" (Cabinet Office, 2022b: 7-8).

Conclusion

In the light of the information given in this study, how the pandemic ended and what its consequences mean for the governments of Türkiye and England were examined. In addition, this study addressed government actions and the changes caused by the pandemic. These actions and changes have brought about the transition to online working, which has been seen to bring cyber security vulnerabilities. The study discussed that the pandemic, including the national and international organizations of Türkiye and England, brought about the search for a "new normal" and inevitably changed the hierarchy of priorities. The impact of COVID-19 on the international system has been examined within the framework of globalization, health, economy, global cooperation, political and strategic priorities. This article will be a guide for future studies and evaluations. It is important to distinguish before and after the pandemic (COVID-19, coronavirus, global epidemic, etc.) in the studies to be carried out.

The pandemic has caused cyber security experts to reconsider their security measures, and they have focused on implementing new processes and technologies to strengthen cyber security policies in the post-pandemic world.

The restrictions imposed by the Turkish and British governments during the pandemic have encouraged individuals to work from home and "stay at home". Thus, technology has become more important in both business and private life. Still, if we look at the international system, within the framework of England-EU Trade and Cooperation Agreement signed on January 1, 2021, a Free Trade Agreement was signed between Türkiye and England. According to this agreement signed between Türkiye and England on 29 December 2020, continuity, clarity and predictability in economic and commercial relations have been ensured (https://www.mfa.gov.tr/).

It has been observed that the increase in online work from home in both Türkiye and England causes individuals to be more exposed to cyber risks and threats. During the pandemic, cyber attackers have exploited the vulnerability of individuals working online from home. Cyber attackers have increased their criminal activities by taking advantage of individuals' interest in news about the COVID-19 pandemic. Hackers also used credential filling techniques to

gain access to individuals' credentials and then sold the stolen data to other cybersecurity criminals. For example; The use of credential filling, username and password combinations for businesses that rely on video conferencing platforms is a form of cyber attack by hackers. This is possible because it is common for individuals to use the same username, same password, and information across multiple accounts.

There are ways to reduce the likelihood and impact of cyber risk, threats or attacks. But these pathways require focused strategy, action and planning. It is important for Türkiye and England to develop and implement remote working practices to ensure cyber security against future cyber risks, threats or attacks.

The pandemic has individually led to some critical questioning. The pandemic has also revealed an opportunity to reevaluate state administration and world politics. In terms of global governance and cooperation, the existence and functions of international and regional organizations continued to be questioned in the post-process. It has also been observed that there is a lack of governance in terms of cyber security policies. However, some institutions and organizations in Türkiye and England have adapted to working remotely at the end of the pandemic process. This situation is an indication that institutions and organizations are strengthened instead of weakening them. The pandemic has also revealed the fact that no country can be managed alone with a global epidemic.

Considering the fact that cyber security vulnerabilities can be social and technical, communication strategies applied before and after the event should be multi-layered. Although national strategy documents are promising in this regard, it will be important to create a national policy and participate in international negotiations in order to achieve the goals. It is vital that states learn from the pandemic process to avoid possible next disasters. This study is not just for the pandemic process. It aims to benefit from retrospective views to identify weak systems that need to be improved before future security risks and possible disasters and to actively implement cyber security policies.

REFERENCES

- ___ITU (2020). *Tech v COVID-19: Managing the Crisis", ITU News 03,* Access Date. 25.06.2023, [https://www.itu.int/en/myitu/Publications/2020/09/09/13/13/ITU-News-Magazine-No3-2020].

- ___ “Koronavirüs Riskine Karşı 14 Kural”, Access Date. 25.06.2023,
- [https://dhf.marmara.edu.tr/notice/koronavirus-pandemisi-riskine-karsi-14-kural].
- AKYESILMEN, Nezir (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber*
- *Güvenlik*, Istanbul: Orion.
- BBC News (2020). “In full: Johnson orders UK to ‘Stay Home’ to Protect NHS from
- Coronavirus”, 23 March 2020, Access Date. 25.06.2023, [https://www.bbc.co.uk/news/av/uk-52012583].
- CABINET OFFICE (2017). “Public Summary of Sector Security and Resilience Plans”,
- London: Cabinet Office.
- CABINET OFFICE (2021a). “Global Britain in a Competitive Age: The Integrated Review of
- Security, Defence, Development and Foreign Policy”, London: Stationary Office.
- CABINET OFFICE (2021b). “National Resilience Strategy: Call for Evidence.” Gov.uk, 13
- July 2021, Access Date. 25.06.2023,
- [https://www.gov.uk/government/consultations/national-resiliencestrategy-call-for-evidence].
- CABINET OFFICE (2021c). “Public Response to Resilience Strategy: Call for Evidence”, 15
- December 2021, Access Date. 25.06.2023 [https://www.gov.uk/government/consultations/national-resilience-strategy-call-for-evidence/outcome/public-response-to-resilience-strategycall-for-evidence].
- CABINET OFFICE (2022a). “National Cyber Strategy 2022: Pioneering a Cyber Future with
- The Whole of the UK”, London: Stationary Office.
- CABINET OFFICE (2022b). “Government Cyber Security Strategy: Building a Cyber
- Resilient Public Sector. London: Stationary Office”.
- Daily Sabah (27.02.2022). “Cyberattacks targeting Turkey dropped in 2021”, Access Date.
- 25.06.2023, [https://www.dailysabah.com/turkey/cyberattacks-targeting-turkey-dropped-in-2021/news].

- Ministry of Foreign Affairs. “Türkiye-Birleşik Krallık İlişkileri”, *Girişimci ve İnsani Dış*
- *Politika*, Access Date. 26. 06. 2023, [https://www.mfa.gov.tr/turkiye-ingiltere-siyasi-iliskileri.tr.mfa].
- GUDER, Süleyman (2020). “The Effects of COVID-19 on the International System and Turkish
- Politics”, *The COVID-19 Pandemic and its Economic, Social, and Political Impacts*, (ed. Dilek DEMIRBAS et al.) Istanbul: Istanbul University, pp. 151-165.
- HILTON, Samuel and Caroline Baylon (11.2020). “Risk management in the UK: What can we
- Learn from COVID-19 and are we Prepared for the next Disaster?”, *The Centre for the Study of Existential Risk (CSER)*.
- JACKHSON, James (et al.) (10.11.2021). “Global Economic Effects of COVID-19”, *CRS*
- *Report*.
- Ministry of Health, “Covid-19 Information Platform”, Access Date. 24.06.2023
- [https://covid19.saglik.gov.tr/TR-66935/genel-koronavirus-tablosu.html].
- MOTT, Gareth, Jason R. C. Nurse & Christopher Baker-Beall (2023). “Preparing for future
- Cyber crises: Lessons from Governance of the Coronavirus Pandemic”, *Policy Design and Practice*, 6/2, pp. 160-181.
- TOPRAK, Metin (vd.) (2020). “The Covid-19 Pandemic and the Digital Transformation in
- Turkish Higher Education: an Evaluation From the Perspective of Industry 4.0 And Society 5.0”, *The COVID-19 Pandemic and its Economic, Social, and Political Impacts,* (ed. Dilek DEMIRBAS et al.) Istanbul: Istanbul University, pp. 167-185.
- TUIK (23.02.2023). “Ölüm ve Ölüm Nedeni İstatistikleri, 2021”, Access Date. 23.06.2023
- [https://data.tuik.gov.tr/].
- TURKIYE (2016-2019). *Ulusal Siber Güvenlik Strateji Belgesi.*
- TURKIYE (2020-2023). *Ulusal Siber Güvenlik Eylem Planı.*
- UK Parliament (2021). “House of Commons Health and Social Care, and Science and

- Technology Committees. Coronavirus: lessons Learned to Date. Sixth Report of the Health and Social Care Committee and Third Report of the Science and Technology. Committee of".
- UNVER, Gül N. (2017). "Ulusal Siber Güvenlik Strateji Belgelerinde İnsan Hakları",
- *Cyberpolitik Journal*, 2/4, pp. 104-129.
- UNVER, Gül N. (2018). "Siber Çatışmaların Tanımlama Sorunu", *Cyberpolitik Journal*, 3/5,
- pp. 23-44.
- UNVER, Gül N. (2019). "Siber Uzay ve Gözetim Toplumu", *3rd Istanbul Bosphorus*
- *International Conference On Cyberpolitics and Cybersecurity (27-30 June 2019),* Istanbul: Dragos.
- UNVER, Gül Nazik (2023). *Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye*
- *ve İngiltere Örneği*, PhD Thesis, Konya: Selcuk University.
- WHO (12.03.2020). "WHO Announce COVID-19 Outbreak as a Pandemic", Access Date.
- 22.06.2023, [http://www.euro.who.int/en/health-topics/health-emergencies/coronavirus-covid-19/news/news/2020/3/who-announces-covid-19-outbreak-a-pandemic].
- WHO (21.06.2023). Türkiye, [https://www.who.int/countries/tur].
- WHO (21.06.2023). United Kingdom, [https://covid19.who.int/region/euro/country/gb].

OPINIONS / YORUMLAR

EMBRACING CYBERSPACE: MALAYSIA AND THE CYBER SECURITY INITIATIVES

Sonny ZULHUDA*

ORCID ID: https://orcid.org/0000-0003-0192-1971

Introduction

With the proliferation of digital technology and the adoption of digital innovation in the realm of social and political lives, governments worldwide must be ready to embrace the digital challenges. Malaysia, refusing to be left behind, aims to restart and rejuvenate its socioeconomic development for long-term sustainability and prosperity by restructuring the economy as the foundation in improving the wellbeing of the people. Central to the agenda of the economy is the strengthening of the country's digital economy. With an accelerated digital technology adoption both at public and private sectors, extending the effect of digitalization to organizational and individual lives.

Meanwhile, it is axiomatic that enhancing national security and unity is a game-changer for nation-building. The need for these national objectives cannot be over-emphasised in the context of digital economy, because the nation will ultimately face those challenges and we shall come prepared. It is important to remind that in the context of digital economy, cyber security stands out as a prerequisite for Malaysia to enjoy a secured, trusted and resilient cyberspace for everyone. A comprehensive national effort for enhancing our cyber security is crucial, so that we can make the best of the digital economy and eliminate all those risks that will threaten our digital sustainability. This paper stands to remind that for the nations and governments to sustain this digital realm, having a nationally-coordinated effort towards the security of its critical information infrastructure is a necessity instead of luxury.

Beyond the Buzz Word of 'Critical Information Infrastructure'

At the gist of this paper is the term critical information infrastructure. The word information infrastructure is a category of information and digital assets that include both the information technology and operational technology. The adjective 'critical' is added to indicate those

* Associate Professor at Ahmad Ibrahim Kulliyyah of Laws, International Islamic University, Malaysia, e-mail: sonny@iium.edu.my

assets that are so crucial, that we rely on them to ensure a variety of essential services that involve public interests.

In the context of Malaysia, the National Security Council defined critical national information infrastructure as those critical systems that include electronic or information assets, network, functions, processes, facilities and services within the environment of information and communications technology that are very critical to the nation, the interruption or destruction of which would severely impact the national defense and security, national economic stability, national image, government's ability to function, public health and safety as well as individual's right to privacy.

From this proposition and similar terminologies in other countries, we can see that the security and sustainability of a national critical information infrastructure determines the safety and sustainability of a nation. Take, for example, the airport communications system or hospital medical databases. These digital assets are not like any ordinary electronic system. They are critical assets that have to remain secure and resilient to ensure the safety of public transport passengers and patients' health and well-being. Beyond that, any disruption to those systems will detriment public trust and further disturb the agility of economic activities in the country. Therefore, critical information infrastructure is not merely a technical buzz-word, but a significant element of social, economic and political stature of a country and therefore requires a serious political will.

Reality Check: The Risks to Critical Information Infrastructure

Given the criticality of the digital assets, countries worldwide have therefore stepped up to renew their cyber security strategy, taking into account the ever-growing cyber risks and their detrimental effect on digital security and social well-being. But to reach this objective, we need to understand the threats and challenges before us. What is so scary about this cyber security breach?

The effect of cyber security breach in the context of national economy cannot be underestimated. The judicial notice made by Mohamad Shariff Abu Samah, a learned Malaysian High Court judge in his judgment in *Rose Hanida bt Long lwn Pendakwa Raya* [2017] MLJU 1212, confirms that abuse of computer system in a financial institution, considered a national critical information infrastructure by the country, does challenge

national dignity and integrity. An attack to this institution will ultimately affect the future of this industry by compromising the reputation of such essential service and eroding public confidence. An attack at this juncture shall, according to the court, be looked at seriously and be condemned strongly by the community.

This strong judicial notice does not come out of the blue as our digital cyberspace has not been remembered as a peaceful realm. From time to time, cyber threats and cybercrimes have come top within the raking of global risks in the past few years. The World Economic Forum reported in 2022 that cyber threats were perceived as the top global risks bypassing other prominent global concerns such as pandemic, economic gap, as well as environmental hazards. At the private sectors, the PWC has also reported in 2022 that cyber risks including attack to critical information infrastructure and infringement of privacy were among the top risks perceived by global CEOs.

From the various reports on cyber security risks, there is a myriad of cyber risks that arise from the convergence of critical information infrastructures ranging from the threat to the confidentiality of data asset and threat to the integrity of the convergent information systems to the threat to the availability and smooth-running of the system. In the discourse of cyber security, this is known as the CIA-triangle of information security objectives.

Firstly, the confidentiality of digital assets. This aspect of security focuses on the need to ensure only relevant person would have access to the digital assets. Measures must be taken to prevent unauthorised hands or eyes from entering the restricted space or accessing the confidential information. There are incidents we heard from many parts of the globe where confidentiality of digital assets was compromised, such as leak of military and official secrets, massive breach of personal data that impacts public at large, or an illegal interception of confidential communications system.

Secondly, the integrity of the information system. This second aspect of the CIA-triangle aims at preventing malicious or negligent disruption to the accuracy, completeness or truth of the information system. Threats such as illegal intrusion ('hacking') of digital system, unauthorised modification to the digital system, data theft as well as disinformation and misinformation are incidents that compromise with the integrity of a cyber security system. When threats such as these happen, the owner of the critical information system must be prepared to embrace the worst scenario of cyber security attacks. Therefore, access restriction

and data preservation mechanism must take place and must be enforced by law to ensure abuses can be effectively prevented or prosecuted.

Thirdly, the availability of system's security. This third objective of cyber security perceives that any interruption to the smooth-working of digital system of a country or an organisation must be prevented, quickly detected or otherwise responded to. This is because such interruption will not only stop or slow down the system's function, but certainly when it comes to the critical information infrastructure, this may cause disturbance to public service delivery and may therefore create massive disturbance to public safety or economic chaos. Thus, threats such as sabotage and shutting-down of the system, malicious down-time, and the denial of services (DOS) should be perceived as serious disturbance to national security.

The Problems and the Responses

It is important for any policymakers to consider cyber breach as a national concern which requires nation-wide responses. However, this effort may encounter problems as we see the current situations are not a perfect time just yet. Despite the rise of cybercrime and cyber threats, the number of incidents investigation and successful prosecution is low. In addition to that, the owners or stakeholders of the critical information infrastructure in Malaysia still tend to work on separate legal and regulatory framework, creating a disharmony of governance of national public services.

Meanwhile, there are still gap and loopholes in the law. There are several laws applicable for different types of cybercrimes and cyber threats with different agencies being in charge. The sets of cybercrimes in Malaysia have not changed for more than 25 years. There is seemingly an absence of law that coordinates the national oversight and management of critical information infrastructure in Malaysia.

Having said that, cyber security has always been a policy issue for the Government of Malaysia since late nineties. The efforts taken have never been short of excellent visions and policies. On the issue of effective cyber governance, initiatives have been taken including the Multimedia Super Corridor Vision (1996), Communications and Multimedia Industry Objectives (1998), National Cyber Security Policy (2006), the Malaysia Cyber Security Strategy (2020), and the National Cyber Security Management NSC Directive (2021).

The latest evidence came from the current Prime Minister after his first chairing of the National Cyber Security Committee Meeting in June 2023 (*Business Today*, 15th June 2023). Prime Minister Anwar Ibrahim reiterates that the role of the Committee is crucial in navigating the challenges of the digital era and ensuring that Malaysia remains vigilant in the face of cyber security threats. He stressed the national vision that cyber security is a priority not only at the domestic level but also in the global arena, as cyberspace and digital communication permeate every aspect of our lives. This, according to Anwar, has to come from several policy directions including an efficient and effective governance. And this is exactly what people wish to hear from the Government, namely a governance that instils confidence among people and investors in the government's ability to manage cyber security challenges. Anwar further emphasises that national security, including one in the digital domain and cyber ecosystem must never be compromised. It is crucial to ensure "strengthened framework aims to establish more efficient and effective governance to safeguard national security, preserve the integrity of the digital economy, and ensure the social sustainability of Malaysia *MADANI*" – referring to his government's national vision of multi-dimensional development goals.

The present government has reiterated the need to speed up the enactment of Cyber Security Act to ensure an enforceable governance and implementation of cyber security management at the national level, especially that coordinate the national critical information infrastructure at both public and private sectors. This initiative, alongside with the proposed amendments of other cyber security-related laws, is an ultimate phase that is badly needed to reshape the cyber security landscape in Malaysia.

Conclusion

Seemingly backed by a strong digital leadership, the new law aimed by Malaysia shall become a national and conclusive rule for an effective governance, public-private partnership, and enforcement mechanism. To achieve this secured, trusted and resilient digital and legal ecosystem, the country needs to have a strong management and oversight leading agency equipped with the necessary skill sets of their people. To ensure its sustainability, the policy initiatives in this legislation are prepared in an open dialectical environment involving all the stakeholders from the government, industries as well as academia and civil society. At the end, we need to reiterate a very important lesson in cyber security. Cyber security is more than just a policy product; it is a national journey worth-traveling. It requires a long-term plan

that visions the whole aspects of the nation's sustainability and its people's welfare. To achieve this, the cyber security law and policy shall be firmly rooted in our commonly shared values and tradition as well as being driven by civility and innovation.

DO ALIENS PERFORM CYBER- ATTACKS ON GLOBAL NETWORK?

Nezir AKYEŞİLMEN*

ORDIC ID: https://orcid.org/0000-0001-8184-5280

Introduction

The possibility of aliens organizing cyberattacks on our global network is a complex one. There is no evidence that Aliens have ever launched a cyber-attack against us, but there is also no way to know for sure whether they have launched any or not, at least for now? We have also no idea about their technological capacity and capability. Indeed, we are also even not sure about their existence, except for some allegations (Turchin, 2009).

Do They Exist or Not?

In social constructivism we construct everything including politics, ideas, social entities and even aliens or UFOs. Thus, if there is a widespread perception of the existence of aliens, that means they exist. And therefore, we construct our arguments on this assumption.[1]

If UFOs do have the ability to hack into our computer systems, they could potentially cause a great deal of damage. They could disrupt our power grids, financial systems, transportation, water supply and communications networks. They could also steal sensitive data or even launch a full-scale cyber-attack.

However, it is also possible that UFOs do not have the ability to hack into our computer systems. If this is the case, then they would not be able to launch cyberattacks against us.

Can Aliens Launch Cyber-Attacks?

Ultimately, the question of whether or not UFOs can organize cyberattacks on our global network is one that we cannot answer definitively. There is not enough evidence to say for sure either way. However, it is a possibility that we should take seriously and be prepared for.

* Prof. D., Department of International Relations, Selçuk University- Konya – Türkiye. E-mail: nezir.akyesilmen@gmail.com

[1] Concepts of both UFO and aliens are used interchangeably in this paper.

If they have the technology to travel to Earth, they likely have the technology to hack into our computer's networks and other cyber infrastructures. There is abundance of claims on the There are more than enough claims and rumors that many people and even institutions have seen UFOs at different times and in different geographies around the globe. Beyond these claims, the vast majority of people have the perception that UFOs exist and are visiting our planet. This widespread perception is in itself strong evidence that UFOs exist. Secondly, even if UFOs do not really exist, if there is such a widespread perception among people, we need to act as if there are UFOs and take precautions. Because perceptions often either determine the truth or they are even stronger than the truth in the society.

Another significant feature here is about the nature of the network that makes it difficult to figure out the source of cyber-attacks. The source of many cyber-attacks is unknown. Even those effective and well-known attacks such as Stuxnet on Iranian nuclear facilities (2010) and attacks on Ukrainian power grid (2013).[2] There are some assumptions about who launched these attacks but no concrete evidence. Thus, many claims that since they are enormously complicated and a new type of attacks on industrial infrastructures particularly the Stuxnet, then it might be launched by Aliens. Technically both claims can be equally true or false.

It is also worth noting that cyber-attacks are not always harmful and destructive. Sometimes, they are used for cyber surveillance, espionage or to steal data. Attacks such as backdoors or trojan horse are of these kinds (Li and Liu, 2021). So even if aliens did launch such cyber-attack against us, it is possible that we have not realized or unaware of them yet or maybe never. Thus, again we cannot prove both possibility of the existence of cyber-attacks or non-existence.

What Sort of Attack?

Aliens could assault global networks over the internet in a number of ways. Here are some potential examples:

[2] Stuxnet is assumed to be organized by a US-Israeli consortium and attack on Ukraine power grid by Russia, yet these are just claims. They cannot be and have not proved so far, and these countries have not accepted responsibility. Thus some claims that they might be launched by UFOs.

They might gain access to our computer networks. They probably have the means to break into our computers if they have the means to reach Earth. They might interfere with our financial systems, communication networks, and power grids.

They might infect our PCs with malware. Software that is intended to damage a computer system is known as malware. Once installed, it has the ability to manipulate the computer, steal data, and deactivate crucial features.

They might carry out denial-of-service or/and distributed denial of service (DOS or/and DDOS) assaults. A denial-of-service attack aims to prevent users from accessing a website or online service. This is accomplished by pouring a ton of traffic onto the target. “With respect to DDoS attacks covering other breaches, Verizon made a humorous comparison to the government covering up evidence of alien visitation: it is often heard but not so easy to prove.”(Koch and Golling, 2019).

They might launch attacks on satellites. Since satellites are in outer space, comparatively far from human control and physically close to aliens, they are easier target for them. There are no evidence so far that they have attacked satellites yet it might take place in the future (Eriksson and Giacomello, 2022).

Overall, the possibility of alien cyber-attacks is a serious one. But we should not panic. There is no evidence that aliens are planning to attack us, and hopefully we have the technology to defend ourselves.

Defending Against Their Cyber attacks

So, how can we defend ourselves against cyberattacks by aliens?

Improving cyber security procedures. To increase our capacity to recognize and respond to cyberattacks, we must spend money on research and development. At the national and international levels we need to make legal and administrative regulations. New treaties, laws, and other regulations to keep our networks safe. We also need to set up national and international institutions dealing with cybersecurity. The citizens need to be trained for cybersecurity awareness. Our computer networks are protected. This involves creating secure

passwords, maintaining the most recent version of our software, and being selective about the websites we visit.

Cooperate with other nations and with all other stakeholders. Since the networks are generally run by private companies. NGOs are also active in maintaining global network. Collaboration between states, states and companies, states and international organizations and among all stake holders is vital for the global network security. On issues related to cybersecurity, we must collaborate and exchange information. This will enable us to better defend against threats from around the world.

To Conclude

Even if the existence of UFOs and the possibility of cyber-attacks by them are debatable, the world has to take all precautions. It has to develop simulations and scenarios and institutionalize necessary measures accordingly. The future of the world today depends on global computer networks. All our life, including economy, health, environment, development, management, security and even survival, is laden with new technologies, connected to networks and adding comfort to our lives. The collapse of the global web will afflict humanity for at least 50 years, perhaps even a century. Ignoring such a major threat can cause irreparable problems and enormous costs in the future.

References

- Eriksson, J. and Giacomello, G.(2022*). Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*.Publisher: Routledge. https://www.researchgate.net/publication/357934889_Cyberspace_in_Space_Fragmentation_Vulnerability_and_Uncertainty[Access date: 15.08.20223].
- Koch, R. and Golling, M.(2019). 2019 11th International Conference on Cyber Conflict: Silent Battle: Towards Unmasking Hidden Cyber Attack. in T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga, G. Visky (Eds.) 2019 © NATO CCD COE Publications, Tallinn. https://ccdcoe.org/uploads/2019/06/Art_29_Silent-Battle.pdf [Access date: 15.08.20223].
- Li, Y anf Liu, Q.(2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments.*Energy reports.* Volume 7, November 2021, Pages 8176-8186.

https://www.sciencedirect.com/science/article/pii/S2352484721007289 [Access date: 17.08.20223].

- Turchin, A.(2009). *UFO as Global Risk.* https://www.scribd.com/doc/18221425/UFO-as-Global-Risk [Access date: 13.08.20223].

INTERVIEWS / RÖPORTAJLAR

MALAYSIA'S EFFORT TO STRENGTHEN CYBERSECURITY
INTERVIEW WITH ASST. PROF. DR. MAHYUDDIN BIN DAUD

Mahyuddin Bin DAUB*

Kamil TARHAN*

ORDIC ID: https://orcid.org/0000-0003-4668-7920

In the ever-evolving landscape of the digital age, Malaysia has been at the forefront of fortifying its cybersecurity measures to safeguard its citizens, businesses, and critical infrastructure from the ever-increasing threats in cyberspace. This situation causes Malaysia to rank first in international cyber security indexes. In this exclusive interview with Dr Mahyuddin bin Daud, a prominent cybersecurity expert and cyber law academician, we delve into the nation's resolute efforts and strategic initiatives to enhance its cyber resilience. It shows invaluable insights into the challenges faced, the progress made, and the vision that propels Malaysia's commitment to securing its digital future. This interview, conducted by Kamil Tarhan, promises to shed light on the crucial role played by Malaysia in the global cybersecurity arena.

1-) How do you evaluate the approach to Malaysia's Cybersecurity policies?

If you create the right cybersecurity policy and legislation, it can improve many areas of the country's development, including infrastructure development, and human talent. Cybersecurity is essential in creating a secure, trusted and resilient network essential for creating trust and confidence in an economic environment based on the Internet and digital network without undermining the country's sovereignty and strategic interests. Cybersecurity is also instrumental to the digital economy. For digital economic activities to flourish, the country's ability to create the right policies, legislation, infrastructure development and human talents is imperative.

* Assistant Professor Mahyuddin Bin Daud, Ahmad Ibrahim Kulliyyah of Laws - IIUM, mahyuddin@iium.edu.my . Area of Specialisation: ICT Policy and Social Impact ~ ICT Law - Internet Content Regulation Dr. Mahyuddin Daud obtained his PhD on Cyber Law (Internet Content Regulation) from IIUM, LL.M from UiTM and LL.B from IIUM. Started his academic career in 2010, he actively writes for academic journals and teaches contracts, torts and information technology laws at the Department of Civil Law, Ahmad Ibrahim Kulliyyah of Laws, International Islamic University Malaysia.

* Ph.D. candidate at Dept. Of Political Science – International Islamic University of Malaysia (IIUM) kmltrhn.kt@gmail.com

As Malaysia pursues digital economic agenda, upgrading national security is imperative to ensure its well-being and long-term viability. Through the 12th Malaysia Plan, it is anticipated that the nation's digital economic plan will be strengthened and achieved through advanced technology and digitalisation. The 12th Malaysia Plan further makes it apparent that a comprehensive national cyber security governance and legal framework would continue to be strengthened corresponding with the pace of change in the technology.

2-) Do you think Malaysia attaches enough importance to cybersecurity policies and cyber technologies?

Malaysia has shown growing awareness and recognition of the importance of cybersecurity policies and cyber technologies in the early period. The government has taken steps to address cybersecurity challenges and promote the use of technology for various sectors. There are some indicators of Malaysia's commitment to cybersecurity include:

- National Cyber Security Policy (NCSP) 2006: Malaysia formulated its NCSP to address the increasing cyber threats and ensure a secure cyberspace for the nation. The policy outlines strategies and initiatives to enhance cybersecurity across various sectors at the same time at the national level.
- National Cyber Security Agency (NACSA): The establishment of the NACSA in 2017 demonstrates the government's commitment to coordinate and centralize efforts in securing Malaysia's cyberspace. NACSA plays a crucial role in implementing cybersecurity strategies and ensuring collaboration between different stakeholders.
- Cybersecurity Education and Awareness: The Malaysian government has shown efforts to promote cybersecurity education and awareness among its citizens. Various campaigns and initiatives have been launched to inform the public and businesses about cyber threats and best practices for protection.
- Cybersecurity Industry Development: Malaysia has been actively working to develop its cybersecurity industry. The country aims to be a regional hub for cybersecurity services, and this ambition indicates the importance attached to cyber technologies.

While there have been positive developments, the evolving nature of cyber threats demands continued focus and investment in cybersecurity policies and technologies. Regular updates and adjustments to policies are necessary to keep up with the changing threat landscape and emerging technologies.

3-) How do you evaluate Malaysia's cybersecurity policies in general?

The efforts to strengthen cybersecurity in Malaysia has begun since the early days of the Multimedia Super Corridor (MSC) in 1996. Amongst others, committees, policies and strategies were introduced and implemented, including the National Information Technology Council of Malaysia (NITC) and the National IT Agenda.

On the other hand, the National Security Policy highlights the importance of a safe cybersecurity framework, specifically under the 17th strategy which is to ensure a secured cyber environment through comprehensive risk management involving the consolidation of the security and defence infrastructure, especially the Critical National Information Infrastructure (CNII) of the country.

With specific focus on cybersecurity, the NCSP 2006 was introduced with the following objectives: -

1) to address the risks to CNII;
2) to ensure that CNIIs are protected to a level that commensurate with the risks; and
3) to develop and establish a comprehensive program and a series of frameworks.

The Cabinet through its meeting on 24 February 2010 agreed to execute key recommendations from NCSP: -

1) to implement MS ISO/IEC 27001 Information Security Management System (ISMS) Certification for the CNII;
2) the implementation of the ISMS certification is coordinated by the ministries and regulatory agencies responsible for the national CNII sectors; and
3) that CNII organisations obtain ISMS certification within 3 years.

In a much more recent development, Malaysia Cyber Security Strategy 2020–2024 (MCSS) was developed to instil confidence in cyber environment, not only for the sake of national security, but also to support the government agenda in the digital economy, Industry 4.0, and the adoption of other disruptive technologies for the economic growth of Malaysia.

MCSS replaces the NCSP since it is more inclusive and comprehensive in terms of protecting the CNII, enterprises, and persons. The MCSS was developed with an allocation of RM1.8 billion to step up national cyber security preparedness and upgrade the country's cyber security measures.

It comprises five pillars that represent the main areas of focus and the strategies required for each.

- 1st Pillar: Effective governance and management
- 2nd Pillar: Strengthening legislative framework and enforcement
- 3rd Pillar: Catalysing world class innovation, technology, R&D and industry
- 4th Pillar: Enhancing capacity and capacity building and Awareness and education
- 5th Pillar: Strengthening global collaboration

Therefore, the current proposal for the enactment of the Cyber Security Bill is a timely measure that expands from the 2nd Pillar of the MCSS - and at the same time, supports other pillars. It combines several elements including laws, policies, technologies, and training, including effective governance, legislative and regulatory, cybersecurity technology, culture of security and capacity building, research and development toward self-reliance, compliance and enforcement, cyber security emergency preparedness, and international cooperation.

4-) What measures does Malaysia take for the security of cyberspace?

The Malaysia cybersecurity strategy 2020 -2024 is a master plan. The first focus is on effective governance and management of cybersecurity. So, this means that the government is working to ensure that all stakeholders both government and private.

The NACSA play a role to coordinate between government agencies as well as the private sector. It can manage the cybersecurity threats together to reduce the threats and improve security in the long run. For example, I was involved in this cybersecurity project under the government with other participants from different sectors. There are 11 critical sectors in Malaysia such as defence, banking, health, education and finance identified by the National Security Council.

Secondly, the government is also working on strengthening the legislative framework as well as enforcement, both for cybersecurity and cybercrime. This has already been on the agenda for recent cybersecurity policy. The government is in the process of drafting cybersecurity legislation. Also, the government is planning to revise and amend the existing cyber laws such as the Computer Crimes Act.

The government can't be just complacent with doing awareness and campaigns. Therefore, the new cybersecurity laws need to be strengthened as well. So, with the coming of this cybersecurity legislation, the critical sectors would be more prepared to ensure that layers of protection in systems are upgraded.

5-) Do you think Malaysia's policies are sufficient according to international approaches?

Technology is very fast changing every day. So, I think, it's never enough and sufficient. Malaysian government need to continue the effort so that policies are always up to date with international approaches.

6-) Do you think Malaysians are ready to face cyber threats?

Malaysia, like many other countries, faces cyber threats on various fronts. The readiness of a nation to face cyber threats depends on several factors, including government initiatives, cybersecurity awareness among citizens, and the overall level of preparedness within the public and private sectors.

The readiness of individual Malaysians to face cyber threats might vary. While some individuals and businesses may have strong cybersecurity practices in place, others might lack awareness or technical knowledge to protect themselves adequately. Cybersecurity education and awareness campaigns are crucial in enhancing the overall readiness of the population to face cyber threats.

It's worth noting that cyber threats are continuously evolving, and countries, including Malaysia, need to remain vigilant and adapt their cybersecurity strategies accordingly. Collaboration between the government, private sector, and individuals is essential to create a resilient and prepared cyber ecosystem. Regular updates and assessments of cybersecurity

policies and practices are necessary to ensure that the country is well-equipped to face the ever-changing landscape of cyber threats.

7-) Do you think that the legal regulations created are sufficient?

The effective implementation of the cybersecurity law requires a combination of strategies that must be tailored according to the needs of the nation's cybersecurity landscape. However, the most basic way forward would be communicating the law's purpose, requirements, and consequences to the governed subjects and the general public. Such could be done through public education campaigns and training for the relevant law enforcement and government officials.

Next, it is also necessary to allocate adequate resources to support the cybersecurity law implementation efforts. With NACSA being expected to experience an increase in resources and manpower if the Cyber Security Bill is passed, issues with lack of resources and competent personnel may need to be resolved or at the very least mitigated. NACSA should also increase collaboration with relevant agencies such as government agencies, industry players, and advocacy organisations to ensure that implementation efforts are coordinated, efficient, and responsive to contemporary cyber security needs, especially when it comes to developing the appropriate liability regime for cyber security service providers in Malaysia.

Moreover, efforts for regular monitoring and evaluation of the effectiveness of the law can help identify challenges and areas for improvement in implementation, as well as opportunities for scaling up successful efforts. Enforcement mechanisms, such as penalties or fines for non-compliance, must be clarified and updated to ensure that the law strikes the balance between deterring potential violators and becoming a tool of unnecessary oppression.

Lastly, the Parliament must have the political will in adapting the law to changing circumstances and new information, especially in the face of emerging cyber threats. There might be a point where new cyber threats necessitates a review of the law, or the policies created under the law. When that time comes, change would be necessary.

8-) Should the policies created by the government be evaluated only in terms of national security or does it include individuals as well?

Government policies should be evaluated not only in terms of national security but also with consideration for individuals' rights, privacy, and overall well-being. Striking the right balance between national security and individual rights is a critical aspect of any well-rounded and democratic policy framework.

While ensuring national security is an essential responsibility of the government, it should not come at the expense of violating individual rights and privacy. Policies that focus solely on national security without adequate consideration for individual freedoms may lead to issues like excessive surveillance, data breaches, and potential abuse of power.

Effective policies should aim to protect both the country and its citizens. They should address national security concerns while upholding fundamental human rights, privacy, and civil liberties. Here are some key considerations for evaluating government policies:
Privacy Protection: Policies should safeguard individuals' privacy and personal data, ensuring that data collection, storage, and usage adhere to appropriate legal and ethical standards.
Transparency and Accountability: Policies should be transparent, with clear objectives and measures. There should be mechanisms in place to hold government agencies accountable for their actions related to national security.

Rule of Law: Policies must adhere to the rule of law, respecting constitutional rights and established legal principles. Any infringement on individual rights must be justified, proportional, and necessary in the context of national security.

Cybersecurity and Data Protection: Policies should address cybersecurity threats and promote measures to protect individuals and organizations from cyber-attacks.
Public Participation and Consultation: In a democratic society, involving the public in policy development through consultations and feedback is crucial to ensure policies are well-rounded and representative of diverse viewpoints.

Human Rights Considerations: Policymakers should conduct human rights impact assessments to evaluate the potential impact of security measures on individual rights and freedoms.

International Obligations: Government policies should align with international human rights standards and conventions to which the country is a signatory.

Balancing national security with individual rights is a complex task, but it is essential to maintain a fair and just society. Governments should continuously evaluate their policies, taking into account feedback from citizens, civil society organizations, and international partners, to ensure they strike the right balance and effectively address both national security concerns and individual well-being.

9-) What do you think about Malaysia's latest national strategy document of 2020 and the recent new understanding of cybersecurity?

The Malaysia National Cyber Security Strategy 2020-2024 is a comprehensive plan that outlines the country's approach to address cybersecurity challenges and enhance its cyber resilience over a specific period. The strategy covers a range of key areas and initiatives to strengthen Malaysia's cybersecurity capabilities and protect its cyberspace. Some notable aspects of the strategy include:

Comprehensive Approach: The strategy takes a holistic and multi-faceted approach to cybersecurity, encompassing various sectors, stakeholders, and potential threats. It seeks to address not only technical aspects but also policy, legal, and capacity-building components.
Protection of Critical Infrastructure: The strategy likely emphasizes the protection of critical infrastructure, recognizing the significance of these assets and their vulnerability to cyber threats.

Capacity Building and Awareness: Efforts to build cybersecurity capabilities among government agencies, businesses, and individuals are likely a crucial part of the strategy. This may include cybersecurity training, workshops, and awareness campaigns.

International Cooperation: International collaboration and information sharing to counter global cyber threats are likely integral to the strategy. Engaging with regional and international partners can enhance Malaysia's cybersecurity posture.

Public-Private Partnerships: Collaboration between the public and private sectors is often essential to ensure a coordinated and effective response to cyber threats. The strategy likely encourages partnerships with industry stakeholders.

Incident Response and Recovery: The strategy likely addresses the establishment and improvement of cybersecurity incident response mechanisms to mitigate and recover from cyber incidents effectively.
Legal and Regulatory Framework: A robust legal and regulatory framework is essential for effective cybersecurity. The strategy may involve efforts to enact or amend laws related to cybercrime, data protection, and cybersecurity.

Research and Development: Emphasizing research and development in cybersecurity can lead to innovative solutions and technologies to stay ahead of evolving threats.

10-) Is there cooperation with non-governmental organizations in the creation of cybersecurity policies?

In the vast majority of countries around the world, the private sector owns and operates the ICT infrastructure. In many nations, the private sector is often the first to adopt new technologies and evaluate their vulnerabilities. The creation of cybersecurity policies will not be possible if there were no involvement from the NGO as well as the private sector. Therefore, the participation of the business sector is essential to any national cybersecurity endeavour.

A cybersecurity service provider plays a crucial role in protecting individuals, organisations, and systems from cyber threats. They offer a range of services aimed at identifying vulnerabilities, mitigating risks, and defending against various cyberattacks, which may be classified such as Threat Detection and Prevention, Incident Response, Vulnerability Assessment and Penetration Testing, Security Consulting and Risk Management, Security Awareness Training and Managed Security Services. In summary, a cybersecurity service provider helps organisations build resilient defences and minimise the impact of potential cyberattacks.

ARTICLE AND BOOK REVIEWS / MAKALE VE KİTAP İNCELEMELERİ

CYBERSECURITY FOR BEGINNERS

Gül Nazik ÜNVER*

ORCID ID: 0009-0005-5003-1555.

The Heimdal.(2023). ***Cybersecurity for Beginners, e-book, 317 pages.***

2011 yılından bu yana yüzbinlerce kullanıcıyı siber suç saldırılarına ve veri güvenliği ihlallerine karşı korumak için yeni teknolojiler geliştiren ve istihbarat sağlayan The Heimdal Security ekibi, gizli bilgileri güvende tutarak kullanıcıları ve şirketleri siber suç eylemlerinden korumak ve gerçek dünyada çözüm ihtiyacını karşılamak için kurulan çevrimiçi bir platformdur. Bu platformda eğitim programları yapılmakta, anket ve test teknikleri uygulanmakta ve siber güvenliğe dair çeşitli çalışmalar yürütülmektedir. Danimarka'da merkezi bir kuruluş olarak ortaya çıkan, ancak uygulamalarını çevrimiçi sitesinde sürdüren The Heimdal Security, kendisini aşağıdaki şekilde açıklamaktadır:

H- Tüm kuruluşların ve bireylerin güvende kalmasına yardımcı olun.

E- Eğitim her şeyden önce gelir.

I- Yenilik asla durmamalı.

M-Kuruluşları daha güvenli hale getirmek aşağıdan yukarıya doğru başlar.

D- Kendinizi ve diğerlerini ileriye taşıyın.

A- Her şeye insan faktörünün dahil olmasına izin verin.

L- Önce dinleyin sonra teşhis koyun.

İncelemeye konu olan kitap, yıllar boyunca siber güvenlik alanında edinmiş olduğu bilgi birikimini ve tecrübesini yansıtan bir eserdir. Kullanıcıların siber güvenlik bilincini ve farkındalığını artıran eğitimlerin sürekli olarak planlanıp hayata geçirilmesi gerekmektedir. The Heimdal Security ekibinden Andra Zaharia, Haziran 2015'ten itibaren yeni başlayanlar için siber güvenlik kursunun verildiğini ve kursun ders kitabı olarak ilgili eserin olduğunu vurgulamaktadır (https://heimdalsecurity.com/blog/announcing-the-free-cyber-security-for-beginners-course/). Dolayısıyla The Heimdal Security ekibinin alana ve literatüre hakimiyeti gerek eserin içerisinde gerek üslubunda görülmektedir.

* Dr., Selcuk University, IR, E-mail: gulunver@outlook.com This study was produced from the author's PhD thesis. For Detailed Information: Ünver, Gül Nazik (2023). *Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği*, PhD Thesis, Konya: Selcuk University.

The Heimdal Security Ekibi tarafından kaleme alınan bu eser siber güvenliğe yeni başlayanlar için önemli bir kılavuz olmaktadır. İlgili eser, internette bu konuya dair bilgi kirliliğinden uzak tutarak bir kılavuz olarak yayınlanmıştır. Kurs için yapılmış bir ders kitabı olarak yayınlanan bu kaynak; bireylerin temel güvenlik önlemlerini nasıl uygulamaları gerektiğini, siber saldırıları nasıl önlemeleri gerektiğini, uzaktan çalışmayla birlikte siber tehditlere karşı nasıl durulması gerektiği ve bilgilerin güvenliğinin nasıl sağlanması gerektiği konusunda adım adım rehberlik sağlamaktadır.

İlgili eserde giriş, sonuç ve kaynakça bölümleri yoktur. The Heimdal Security Ekibi tarafından kurs için sağlanan bu e-kitap 19 farklı bölümden oluşmakta ve her bir bölümde kursta verilecek derslerin neleri kapsadığına dair genel bir bakış sunmaktadır. Her bölüm içerisinde konu ile ilgili uygulama ve örneklere ilaveten, kitabın içeriğinde video bağlantı linklerine, testlere, birçok görsele yer verilerek konuların gerçek dünya ile ilişkisi kurulmuş ve bunu okuyucuya akıcı bir şekilde basitçe açıklayarak konuyu temellendirmiştir. Bu kitap teknik olmayan bir geçmişe sahip olunsa bile, siber güvenliğin temelleri hakkında kolay bir fikir sağlamaktadır. Yazarın konuyu anlatış şekli oldukça başarılıdır. Bu kitap ayrıntılara girmemekte ve teknik tarafa çok az girmektedir. Yeni başlayanlar için siber güvenliğin nasıl çalıştığına dair iyi bir genel bakış sunmaktadır.

Kitabın birinci bölümünde güvenliği artırmak için on bir adımda uygulanabilecek bilgiler verilmektedir. E-posta ve/ya sosyal medya hesaplarında güçlü şifreler kullanılması, özel bir güvenlik çözümüyle casus yazılım tehditlerine karşı güvende kalınması, windows işletim sistemi ve güvenlik açığı bulunan uygulamaların güncel tutulması, çevrimiçi olmak için windows işletim sisteminde standart bir kullanıcı hesabının kullanılması, kullanıcı hesabının denetlenmesi, güvenli tarayıcının kullanılması, herkese açık ve ücretsiz wi-fi bağlantılarına güvenilmemesi, bir bağlantıyı tıklamadan önce kontrol edilmesi, kişisel bilgileri güvende tutmak için girilen sitelerden çıkış yapılması, özel bilgilerin sosyal medya aracılığıyla paylaşılmaması, şüpheli web konumlarına erişilmemesi gerektiği üzerinde durulmaktadır. Yazar, on bir adımı kısa ve öz olarak okuyucunun faydasına sunmuştur.

İkinci bölümde çevrimiçi ortamda bilgi ve verilerin giderek değiştiği ve yeni ilgi alanlarının ortaya çıktığından bahsedilmektedir. Bu nedenle güvenlik perspektifi de buna ayak uydurmalı ve geri kalan internet güvenliği efsaneleri unutulmalıdır. Üçüncü bölümde kısa sürede temel bilgi güvenliği teriminin öğrenilebileceğinden ve siber suçluların nasıl düşündüğünü ve nasıl davrandığını anlayabilecek seviyede bir ders olacağından bahsetmektedir.

Dördüncü bölümde birden fazla hesapta aynı şifrenin kullanılmaması ve güçlü bir şifreye sahip olmanın ne kadar önemli olduğu konusunda bazı yararlı bilgiler ve çözümler oluşturulması gerektiğinden bahsedilmektedir. Doğum tarihi, sıralı sayı ya da bulunduğunuz şehir, tuttuğunuz takım gibi şifreler kullanılması, siber suçluların o hesaplara daha basit ve kolay yollarda erişebilmesini olası kılmaktadır.

Beşinci bölümde en iyi antivirüs yazılımı nasıl seçilmesi gerektiği üzerinde durulmaktadır. İlgili eser bunu kullanıcı görüşleri, uzman değerlendirmeleri ve bağımsız testlerle ihtiyaç olabilecek bilgilerin bulunabileceğinden bahsetmektedir.

Altıncı bölümde geleneksel antivirüs yazılımları, siber suçluların başlattığı kötü amaçlı yazılımlardan koruyup koruyamadığını tartışmaktadır. İyi bir antivirüs ürünü sistemin güvenliğini sağlamada önemli bir etkendir. Ancak mevcut tehditler ve siber suç saldırıları, antivirüsü tespit sisteminin üstesinden gelme yeteneğine sahiptir. Bu nedenle, bilgisayar korsanları tarafından gönderilen gelişmiş kötü amaçlı kod parçalarına karşı mücadele ederken sadece antivirüs ürünü yeterli gelmeyebilir ve alternatif koruma araçları (güvenlik duvarı, önemli dosyaları şifrelemek vb.) kullanılması gerektiğinden bahsetmektedir.

Yedinci bölümde sistemdeki güvenlik açıklarının nasıl yönetilmesi gerektiğinden bahsetmektedir. Güvenlik açıklarında bireyler çoğunlukla kişisel veriler hakkında endişelenmektedir. Ama bireylerin çoğu verilerin yedeklenmesini unutmak ya da ertelemektedir. Bu nedenle sekizinci bölüm, ertelemek yerine verilerin güvenliğinin sağlanmasına odaklanmaktadır.

Dokuzuncu bölümde temel verileri şifreleme çevrimiçi tehditlerden ve gizlilik ihlallerinden koruyan şifreleme mekanizmasını kullanmak gerekmektedir. Şifrelemenin amacı hassas bilgileri siber suçlulardan veya diğer çevrimiçi tehlikelerden korumaktır.

Onuncu bölümde kullanıcıların tarayıcılarında (Internet Explorer, Mozilla Firefox ve Google Chrome vb.) güvenlik ayarlarını düzenleyerek çevrimiçi güvenliği artırmak, çerezler, uzantılar veya eklentilerden kaynaklanabilecek sorunlara karşı çözüm bulmak ve bu sorunlara karşı güvenlik önlemleri almaktan bahsetmektedir. On birinci bölümde güvenli olmayan genel wi-fi ağlarındaki kişisel verilerin nasıl korunacağından bahsetmektedir.

On ikinci bölümde çevrimiçi e-posta hesaplarını (Yahoo!, Gmail, Aol ve Outlook) güvende tutmak için izlenmesi gereken genel yönergelerden oluşmaktadır. On üçüncü bölümde sosyal medya kullanımı ile bilgilerin gizli tutulması arasındaki dengenin nasıl sağlanması gerektiği

üzerinde durmaktadır. On dördüncü bölümde onedrive, drivebox, icloud gibi bulut sistemlerinde yer alan dosyaların daha güvenilir bir altyapısı olduğundan bahsetmektedir. On beşinci bölümde kimlik hırsızlığına karşı alınması gereken önlemler üzerinde durulmaktadır. On altıncı bölümde riski doğru bir şekilde değerlendirebilmek ve etkili bir savunma stratejisi oluşturabilmek için kötü amaçlı yazılım bulaşmasının nasıl ortaya çıktığını öğrenmenin önemini vurgulamaktadır. On yedinci bölümde çocukların ve ebeveyinlerin siber güvenlik hakkında temel öğrenmesi gereken noktalardan bahsetmektedir. On sekizinci bölümde siber güvenliğin sağlanması için on şeyden bahsetmektedir. Bunlar; Telif hakkı, bilinmeyen e-postalarla uğraşırken dikkatli olmak, kaynaklar, bağlantıya veya çevrimiçi reklama tıklamamak, ücretsiz bir programın güvenli olup olmadığını bilmeden yüklememek, hassas bilgileri çevrimiçi ortamda ifşa etmemek, kimlik bilgilerini saklamak, çevrimiçi platformda yayınlanan her şeyin çevrimiçi kaldığını unutmamak, antivirüs koruması kullanmak, önemli öğeler için yedek kopyalar oluşturmaktır.

"Cyber Security Ninja level achieved!" başlıklı son bölümde, on sekiz ders boyunca verilen bilgiler ışığında meraklı bir kullanıcı olmaktan öte *Siber Ninja* olarak siber güvenliğin temelde nasıl sağlanacağını okuyucuların öğrendiğinden ve dersi alan okuyucuları teste tabi tutarak kendilerini denemelerinden bahsetmektedir. Kendi başınıza bir hacker saldırısı savuşturma becerilerini öğrenmek çok zaman alıcı olduğunu, bu nedenle ilgili eserin sıfırdan uzman hacker'a taşımak için gerçek dünyadan örneklerle siber güvenlik bilincini adım adım "Cyber Security For Beginners" e-kitabında hazırlandığını belirtmektedir. Son bölümde gelecek vaat eden her siber güvenlik uzmanının bilmesi gereken temel bilgilerin ne kadarını öğrendiğinizi test etmekte ve bu testi geçenler için siber güvenliğin temel argümanlarını başarıyla uygulayabileceklerini göstermektedir. Bu kapsamda kılavuzda, bu alanda çok az deneyim olsa veya hiç deneyimi olmasa bile, etkili bir siber güvenlik stratejisinin nasıl geliştirileceğini ve uygulanacağını öğretmektedir. "Cyber Security For Beginners", siber güvenliğe kariyer geçişi yapmayı düşünen ve hassas bilgilerin güvenliğini sağlamak isteyen herkes için ideal bir e-kitaptır.

Siber güvenlik, siber güvenliğe yönelik temel argümanlar, başlangıç için siber güvenlik gibi yıllardır internette birçok kaynak ortaya çıkmıştır. Hemen her kitap siber güvenliğin tüm konularına değindiğini iddia etmektedir. Birçoğu siber güvenlikle ilgili bilgi hazinelerinin anahtarlarını içeren en iyi kitap olduğunu belirtmektedir. Ancak birçoğu gerçek hayattan örnekler vermeden, kitaplarını dolambaçlı ve gereksiz konularla doldurmakta veya yüzeysel şeylerle geçiştirmektedirler. Yeni başlayanlar için siber güvenlik alanında iyi bir kitap,

bireylerin sadece ihtiyacı olan bilgileri edinmesi konusunda fayda sağlamalı, farklı konuları gerçek hayatla bağdaştırmalı, pratik olması gereken karşı önlemler ve olaylar gibi bazı gerçek hayattan örneklerle dolu olmalıdır. Arama motorunda "Cyber Security For Beginners" adlı ve buna benzer isimlerle birçok çalışma yapılmış olmasına rağmen, bu kitap eğitici bir biçimde yazılmış olması ve bir siber güvenlik uzmanının kütüphanesinde bulunması gereken konuları içermesi nedeniyle siber güvenlikle ilgili diğer kitaplardan farklıdır. Ayrıca bu kitap çerçevesinde ekstra bilgiye ihtiyaç duyulursa, The Heimdal Security ekibi aza@heimdalsecurity.com adresinden iletişime geçilmesini önermekte ve kısa zaman içerisinde dönüş sağlanacağını belirtmektedir.

Sonuç itibariyle incelemeye konu olan bu kitap, alana önemli katkı sunmaktadır. İlgili eser sistematiği, kurgusu, güncelliği ve anlaşılabilir anlatımıyla öne çıkan bir eserdir. Bu nedenle kitabın başta bu alanda çalışan ya da bu alana ilgi duyan bireylere bir referans kitabı olmak üzere, lisans ve lisansüstü öğrencilerine de tavsiye olarak önerilebilir nitelikte olduğu görülmektedir.

NOTES FOR AUTHORS / YAZARLAR İÇİN NOTLAR

We would like to thank you for choosing to submit your paper to *Cyberpolitik*. In order to fasten the process of reviewing and publishing please take try to read and follow these notes in depth, as doing so will ensure your work matches the journal's requirements.

All works including research articles, comments and book reviews submitted to *Cyberpolitik* need to be original contributions and should not be under consideration for any other journal before and/or at the same time.

All submissions are to be made online via the Journal's e-mail address: cyberpolitik@gmail.com

The authors of a paper should include their full names, affiliations, postal addresses, telephone numbers and email addresses on the cover page of the manuscript. The email address of the author will be displayed in the article.

Articles should be **1.5-spaced** and with standard margins. All pages should be numbered consecutively. Please avoid breaking words at the end of lines.

The articles need to be between 5000 - 7000 words (including footnotes and references); comments between 2000-4000 words (including footnotes and references); and book - article reviews between 500 - 1500 words.

An abstract of up to 150 words should be added during the submission process, along with an average of five keywords.

Authors should make a final check of their article for content, style, proper names, quotations and references.

All images, pictures, maps, charts and graphs should be referred to as figures and numbered. Sources should be given in full for images, pictures, maps, tables and figures.

Comments in Cyberpolitic

A comment is a short evaluation of an expert regarding new issues and/or development in cyberpolitics.

Comments require journal's full reference style.

Book / article Reviews in Cyberpolitic

A book review should provide a fair but critical assessment of a recent (not older than 5 years) contribution to the scholarly literature on the themes and topics relevant to the journal.

A book review for Cyberpolitik:

- provides complete bibliographical references of the book(s) and articles to be reviewed.
- summarizes the content and purpose of the book, focusing on its main argument(s) and the theory, methodology and empirical evidence employed to make and support these arguments
- Critically assesses the author(s)' arguments, their persuasiveness and presentation, identifying the book's strengths and weaknesses
- presents a concluding statement that summarizes the review and indicates who might benefit most from reading the book

Book / article reviews should be preceded by full publication information, in the following form:

Education for Peace: Politics of Adopting and Mainstreaming Peace Education Programs in Post-Conflict Settings by Vanessa Tinker, Academica Press, 2015, $81.62 (Hardcover), ISBN 978-1680530070.

The reviewer's name, affiliation and email address should appear, on separate lines, at the top of the review, right after the bibliography of the book/article.

Journal style

Authors are responsible for ensuring that their manuscripts conform to *cyberpolitik*'s reference style.

Reference style of *Cyberpolitik* is based on APA 6th Edition.