İSTANBUL BEYKENT ÜNİVERSİTESİ

VIII. ULUSLARARASI TERÖRİZM VE GÜVENLİK KONFERANSI

VIII. INTERNATIONAL CONFERENCE ON TERRORISM AND SECURITY

BİLDİRİ KİTABI / PROCEEDING BOOK

Editörler/Editors
Kinem TOKDEMİR-Hakan DUMLU

İstanbul Beykent Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
VIII. Uluslararası Terörizm ve Güvenlik Konferansı
Bildiri Kitabı

Istanbul Beykent University
Faculty of Economics and Administrative Sciences
VIII. International Conference on Terrorism and Security
Proceedings Book

Editörler / *Editors*

Arş. Gör. Dr. / *R. Asst. Dr.* Kinem TOKDEMİR

Arş. Gör. / *R. Asst.* Hakan DUMLU

İnternet Sitesi / *Website*

http://beykentits.org

VIII. Uluslararası Terörizm ve Güvenlik Konferansı Bildiri Kitabı

VIII. International Conference on Terrorism and Security Proceedings Book

İSTANBUL BEYKENT ÜNİVERSİTESİ YAYINLARI:

Editörler / *Editors*

Arş. Gör. Dr. / *R. Asst. Dr.* Kinem TOKDEMİR

Arş. Gör. / *R. Asst.* Hakan DUMLU

e-ISBN : 978-625-5950-03-1

İstanbul Beykent Üniversitesi Yayınevi, Yayın No: 196

İSTANBUL BEYKENT ÜNİVERSİTESİ

8. ULUSLARARASI

TERÖRİZM VE GÜVENLİK KONFERANSI

TEMA

GÜVENLİĞİN DEĞİŞEN MİMARİSİ

KONULAR

- Siber Güvenlik
- Yapay Zekâ
- İstihbarat ve Bilgi Operasyonları
- Ekonomik Güvenlik

ÖNEMLİ TARİHLER

13 Ekim 2024 : Bildiri Özetlerinin Son Teslim Tarihi
13 Kasım 2024: Kabul Edilen Özetlerin İlanı
20 Kasım 2024: Konferans Programının İlanı
13 Aralık 2024: Konferans Tarihi
13 Ocak 2025: Genişletilmiş Özetlerin Son Teslim Tarihi

Konferans Yeri
İstanbul Beykent Üniversitesi Taksim Yerleşkesi Adem Çelik Konferans Salonu

Konferansı Düzenleyenler
İstanbul Beykent Üniversitesi İktisadi ve İdari Bilimler Fakültesi
Siyaset Bilimi ve Kamu Yönetimi Bölümü (İngilizce/Türkçe)

www.beykentits.org
beykentits@beykent.edu.tr

* Konferans dili Türkçe ve İngilizce'dir.
* Konferans uluslararası niteliktedir ve yeni doçentlik kriterlerini karşılamaktadır.
* Bildiri özetleri yukarıda verilen e-posta adresine gönderilecektir.

ISTANBUL BEYKENT UNIVERSITY

8TH INTERNATIONAL CONFERENCE ON TERRORISM AND SECURITY

THEME

THE CHANGING ARCHITECTURE OF SECURITY

TOPICS

- Cyber security
- Artificial intelligence
- Intelligence and Information Operations
- Economic Security

KEY DATES

13 October 2024 : Abstract Submission
13 November 2024: Announcement of Acceptance
20 November 2024: Announcement of the Conference Program
13 December 2024: Date of Conference
13 January 2025: Deadline for Extended Abstract Submission

Conference Venue
Istanbul Beykent University Taksim Campus Adem Çelik Conference Hall

Organizers
Istanbul Beykent University, Faculty of Economics and Administrative Sciences
Department of Political Science and Public Administration (English/Turkish)

www.beykentits.org
beykentits@beykent.edu.tr

* The conference will be held in Turkish and English.
* The conference is an international event, meeting the criteria for associate professorship applications.
* Abstracts should be sent to the above-mentioned e-mail address.

VIII. ULUSLARARASI TERÖRİZM VE GÜVENLİK KONFERANSI
VIII. INTERNATIONAL CONFERENCE on TERRORISM and SECURITY

DÜZENLEME KURULU / *ORGANIZING COMMITTEE*

Dr. Öğr. Üyesi / Asst. Prof. Mustafa KARAHÖYÜK (Başkan / *Chairman*)

Doç. Dr. / Assoc. Prof. Kemal OLÇAR

Arş. Gör. Dr. / R. Asst. Dr. Kinem TOKDEMİR

Arş. Gör. Dr. / R. Asst. Dr. Taylan Özgür ÜRESİN

Arş. Gör. / R. Asst. Hakan DUMLU

DESTEK GRUBU / *SUPPORTING GROUP* [1]

Alânur ATILGAN

Dilan NAR

Emirhan YÜKSEL

Feyza ÇOLAK

İsmail Cem GÜNEY

Mustafa Eren TALU

Nebahat SEVENBİGE İKİZGÜL

Sedef SARIÇELİK

[1] İstanbul Beykent Üniversitesi İktisadi ve İdari Bilimler Fakültesi Siyaset Bilimi ve Kamu Yönetimi TR ve EN Programlarının öğrencilerinden oluşmaktadır. Düzenleme Kurulu olarak, kendilerine özellikle teşekkür ederiz.

&

It consists of undergraduate students from the Political Science and Public Administration TR and EN Programs of the Faculty of Economics and Administrative Sciences at Istanbul Beykent University. As the Organizing Committee, we extend special thanks to them.

İÇİNDEKİLER /*CONTENTS*

KISALTMALAR / *ABBREVIATION LIST*

AB	: Avrupa Birliği
AI	: *Artificial Intelligence*
ABD	: Amerika Birleşik Devletleri
ANOVA	: *Analysis of Variance*
BM	: Birleşmiş Milletler
CARVER	: *Criticality, accessibility, recoverability, vulnerability, effect, recognisability*
CCDCOE	: *Cooperative Cyber Defence Centre of Excellence*
CIA	: *Central Intelligence Agency*
CIMIC	: *Civil Military Cooperation*
COE-DAT	: *Centre of Excellence Defense Against Terrorism*
COM-B	: *Capability, opportunity, motivation, and behaviour*
COVID-19	: Yeni Koronavirüs Hastalığı
ÇHC	: Çin Halk Cumhuriyeti
DDoS	: *Distrubuted Denial of Service*
DFA	: Doğrulayıcı Faktör Analizi
DSA	: *The Digital Services Act*
EU	: *European Union*
EUMS	: *European Union Military Staff*
EUROJUST	: *European Union Agency for Criminal Justice Cooperation*
EUROPOL	: *European Union Agency for Law Enforcement Cooperation*
EU INTCEN	: *EU Intelligence and Situation Centre*
F2F	: *Face-to-Face*
FBI	: *Federal Bureau of Investigation*
FET	: *Female Engagement Teams*
FONOPs	: *Freedom of Navigation Operations*
FRONTEX	: *The European Border and Coast Guard Agency*
GDPR	: *The General Data Protection Regulation*
GEOINT	: *Geospatial Intelligence*
HTŞ	: *Hey'etu Tahrîri'ş-Şâm* (Şam Kurtuluş Heyeti)

IEA : *Information Environment Assessment*

InfoOps : *Information Operations*

IoT : *Internet of Things*

IR : *International Relations*

IŞİD/DAEŞ : Irak ve Şam İslam Devleti

KLE : *Key Leader Engagement*

MEDCAPs : *Medical Civic Action Programs*

MilPA : *Military Public Affairs*

ML : *Machine Learning*

NATO : *The North Atlantic Treaty Organization* (Kuzey Atlantik Antlaşması Örgütü)

NCMSC : *NATO Crisis Management Strategic Concept*

NCRS : *NATO Crisis Response System*

OECD : *Organisation for Economic Co-operation and Development* (Ekonomik İş Birliği ve Kalkınma Örgütü)

OSINT : *Open Source Intelligence*

PMM : *Post Meeting Minutes*

PRC : *People's Republic of China*

PsyOps : *Psychological Operations*

RF : Rusya Federasyonu

SATCEN : *European Union Satellite Centre*

SCS : *The South China Sea*

SIAC : *Single Intelligence Analysis Capacity*

SLES : *Soldier-Level Engagements*

SMEs : *Subject Matter Experts*

SMO : *Special Military Operation*

SSCB : Sovyet Sosyalist Cumhuriyetler Birliği

STEMPLES : *Social, technological, environmental, military, political, legal, economic and security*

STO : *NATO Science and Technology Organization*

SOCMINT : *Social Media Intelligence*

StratCom : *The Strategic Communication*

UN : *United Nations*

UNCLOS : *The United Nations Convention on the Law of the Sea*

YBS : Yönetim Bilişim Sistemleri

YNS : Yeni Nesil Savaş

GİRİŞ / *INTRODUCTION*

13 Aralık 2024 tarihinde düzenlenen VIII. Uluslararası Terörizm ve Güvenlik Konferansı'nda araştırmacılar, akademisyenler ve alanın profesyonelleri bir araya gelerek güvenlik tehditlerinin güncel boyutlarını tartıştılar.

Konferans öncesi ve sonrasında desteklerini esirgemeyen rektörlüğümüze ve öğrencilerimize teşekkürü bir borç biliriz.

Konferansta tebliğlerini sunan akademisyenlerin hazırladıkları genişletilmiş özetleri içeren bu kitaptaki metinlerin sorumluluğu yazarlarına aittir.

&

The researchers, academics and professionals in the field came together and held discussions on current dimensions of security threats at the 8th International Conference on Terrorism and Security which was organized on the 13th of December, 2024.

We express our deep gratitude to the Rectorate and our students for their unwavering support before and after the conference.

The responsibility for the texts in this book, which contain the extended summaries prepared by the academics who presented their papers at the conference, rests with the authors.

1. KONFERANSIN HEDEFLERİ / *AIMS of the CONFERENCE*

İstanbul Beykent Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Siyaset Bilimi ve Kamu Yönetimi İngilizce ve Türkçe bölümleri tarafından ortaklaşa düzenlenen "VIII. Uluslararası Terörizm ve Güvenlik Konferansı" alandaki araştırmacı, akademisyen ve profesyonelleri bir araya getirerek, araştırmacıları siber güvenlik, yapay zekâ, istihbarat ve bilgi operasyonları ve ekonomik güvenlik çalışmalarına dair meseleleri ve güncel gelişmeleri konu edinerek bilgilendirmeyi hedeflemiştir.

&

"VIII. International Conference on Terrorism and Security", which was jointly organised by Istanbul Beykent University, Faculty of Economics and Administrative Sciences, Departments of Political Science and Public Administration (English and Turkish), aimed to bring together researchers, academics and professionals in the field and to inform researchers about cyber security, artificial intelligence, intelligence and information operations and economic security studies by addressing the current situation, agenda and discussions.

2. KONFERANSIN YÖNTEMİ/ *METHOD of the CONFERENCE*

Konferans, katılımcı akademisyenlerin hazırlamış oldukları sunumlar üzerinden yapılmıştır. Her araştırmacı, uluslararası terörizm ve güvenlik kapsamında farklı bir konuyu değerlendirmiş, gelen soruları yanıtlayarak katkıda bulunmuştur.

&

The conference was based on the presentations prepared by the participating academics. Each researcher evaluated a different topic within the scope of international terrorism and security and contributed by answering the questions.

3. KONFERANSIN PROGRAMI/ *PROGRAMME of the CONFERENCE*

İSTANBUL BEYKENT ÜNİVERSİTESİ

8.ULUSLARARASI TERÖRİZM VE GÜVENLİK KONFERANSI

AKIŞ

4.OTURUM

15.00-16.00

Oturum Başkanı:
Doç. Dr. **Kenan ORÇANLI**

Oturum Başlığı:
İstihbarat

13. Arş. Gör. **Aybars ÖZTUNA**
(Johns Hopkins Üniversitesi, ABD)
Evaluating Chinese Naval Infrastructure Developments in the South China Sea Through Geospatial Intelligence / 15.00-15.10

14. Doç. Dr. **İbrahim İRDEM**
Dr. **Murat UZUNPARMAK**
(Polis Akademisi Başkanlığı, Türkiye; İçişleri Bakanlığı, Türkiye)
Siber İstihbaratın Küresel Güvenlik Mimarisine Etkisi / 15.10-15.20

15. Dr. Öğr. Üyesi **Laçin AKYIL**
(İstanbul Arel Üniversitesi, Türkiye)
Avrupa Birliği'nin Yeni Bir İstihbarat Servisi Oluşturmasının Türkiye-Avrupa Birliği İlişkilerine Olası Etkileri/ 15.20-15.30

16.Dr. Öğr. Üyesi **Atahan Birol KARTAL**
(İstanbul Beykent Üniversitesi, Türkiye)
İstihbarat ve Teknoloji: Yeni Kaynakların Yönetimi / 15.30-15.40

Soru-Cevap
15.40-15.50

ARA
15.50-16.00

5. OTURUM

16.00-17.00

Oturum Başkanı:
Dr. Öğr. Üyesi **Bekir Aşık**

Oturum Başlığı:
Güvenlikte Jeopolitik Tartışmalar

17. Doç. Dr. **Stanislav MYŠIČKA**
(Hradec Králové Üniversitesi, Çek Cumhuriyeti)
The PRC Military Base in Djibouti and China's Growing Security Presence in Africa / 16.00-16.10

18. Dr. **Marina GLASER**
(Ulusal Araştırma Üniversitesi, Ekonomi Yüksek Okulu, Rusya Federasyonu)
Influence of the Political-Informational "Landscape of Betrayal" on the Intensity of Internal Terrorist Activity During an External Conflict (Case of Russia During the "Special Military Operation") / 16.10-16.20

19. **Sunday Jacob AJOSE**
(Bağımsız Araştırmacı, Nijerya) | Çevrim İçi
Corruption and Violence in Nigeria: A Critical Analysis / 16.20-16.30

20. **Zarina M. LAZAROVA**
(Öğrenci, Rakovski Millî Savunma Üniversitesi, Bulgaristan) | Çevrim İçi
The Changing Architecture of Security: Zangezur Corridor's Economic Importance / 16.30-16.40

Soru-Cevap
16.40-16.50

KAPANIŞ
17.00

ISTANBUL BEYKENT UNIVERSITY

8TH INTERNATIONAL CONFERENCE ON TERRORISM AND SECURITY

FLOW

OPENING REMARKS

09.00-09.10

Prof. Dr. **Volkan ÖNGEL**
(Rector, Istanbul Beykent University)

Dr. Öğr. Üyesi **Mustafa KARAHÖYÜK**
(Conference Organizing Committee Chairman, İstanbul Beykent University)

SPECIAL SESSION

09.10-10.30

Session Moderator:
Prof. Dr. **Ece BABAN**
(Dean, Faculty of Communication, İstanbul Beykent University)

Session Title:
The Changing Architecture of Security

1. Prof. **Christopher FARRANDS**
(Nottingham Trent University, the United Kingdom)/09.10-09.30

2. (Rt) Ambassador **Uluç ÖZÜLKER**
(Türkiye) / 09.30-09.50

3. Prof. Dr. **Nuray EKŞİ**
(Marmara University (Rt), Turkey) / 09.50-10.10

4. Asst. Prof. **Naim BABÜROĞLU**
(İstanbul Aydın University, Türkiye) / 10.10-10.30

Q & A
10.30-10.45

BREAK
10.45-11.00

1.SESSION

11.00-11.50

Session Moderator:
Assoc. Prof. **Ülke Evrim UYSAL**

Session Title:
Cyber Security

1. Assoc. Prof. **Izabela KAPSA**
(Kazimierz Wielki University, Poland)
Contemporary Dilemmas of the Digital State: Balancing Civic Inclusiveness with the Right to Refrain from Technology / 11.00-11.10

2. Dr. **Kamila SIERZPUTOWSKA**
(Kazimierz Wielki University, Poland)
Cybersecurity Threats as One of the Challenges for the Eastern Border of NATO in the Face of the Russian - Ukrainian Conflict / 11.10-11.20

3. Asst. Prof. **Şükran ORUÇ**
Res. Asst. **Özlem ÇILDIRIM KOCABIYIK**
(İstanbul Beykent University, Türkiye)
Dijital Dönüşümde Güvenlik Algısının Değişen Yüzü: Siber Güvenlik / 11.20-11.30

4. **Elfadil ORSAD**
(Independent Researcher, Egypt) | Online
The Changing Architecture of Security: The Role of Cyber Security and Artificial Intelligence / 11.30-11.40

Q & A
11.40-11.50

BREAK
11.50-12.00

ISTANBUL BEYKENT UNIVERSITY

8TH INTERNATIONAL

CONFERENCE ON TERRORISM AND SECURITY

FLOW

2. SESSION

12.00-12.50

Session Moderator:
Doç. Dr. **Asuman KUTLU**

Session Title:
Artificial Intelligence

5. Dr. **Chenghao SUN**
Asst. Flw. **Xueyu ZHANG**
(Tsinghua University, the People's Republic of China) | Online
From Risk to Opportunities: Addressing National Security Challenges of Open-Source AI / 12.00-12.10

6. Dr. **Sumanta BHATTACHARYA**
Bhavneet KAUR
(The International Union for Conservation of Nature, India; Suresh Gyan Vihar University, India) | Çevrim İçi
Regulatory Framework and Policy Implications for Implementation of AI and ML for Upgrading Economic Sector in Banking and Trade Sectors/ 12.10-12.20

7. Atty. **Orçun OLTULU**
(PhD Student, Hacettepe University, Türkiye)
Askerî Tam Otonom Silahlarda Orantılılık ve Ayrım Gözetme Sorunu: Silahlı Çatışma Hukuku Bağlamında Bir İnceleme / 12.20-12.30

8. Dr. **Giovanni ERCOLANI**
(University of Murcia, Spain)
The Emergence of Paranoid Security / 12.30-12.40

Q & A
12.40-12.50

LUNCH BREAK
12.50-13.45

3. SESSION

14.00-15.00

Session Moderator:
Doç. Dr. **Kemal OLÇAR**

Session Title:
Information Operations

9. **Can DEMİR**
(PhD Student, Turkish National Defence University, Türkiye)
NATO Doctrine of Information Operations and Key Takeaways for the Modus Operandi / 14.00-14.10

10. Dr. **Federico PRIZZI**
(Independent Researcher, Italy)
Key Leader Engagement, The Most Challenging Way in Warfighting to Influence Adversaries / 14.10-14.20

11. Assoc. Prof. **Greg SIMONS**
(Turiba University, Latvia; Daffodil International University, Bangladesh)
Security Versus Insecurity in a Transforming Global Order: The Role of the Fifth Dimension of Strategy / 14.20-14.30

12. Prof. Dr. **Erdal ARSLAN**
(Selçuk University, Türkiye)
Uluslararası Terörizm ile Mücadelede NATO'nun Rolü / 14.30-14.40

Q & A
14.40-14.50

BREAK
14.50-15.00

ISTANBUL BEYKENT UNIVERSITY

8TH INTERNATIONAL

CONFERENCE ON TERRORISM AND SECURITY

FLOW

4. SESSION

15.00-16.00

Session Moderator:
Assoc. Prof. **Kenan ORÇANLI**

Session Title:
Intelligence

13. Res. Asst. **Aybars ÖZTUNA**
(Johns Hopkins University, the United States of America)
Evaluating Chinese Naval Infrastructure Developments in the South China Sea Through Geospatial Intelligence / 15.00-15.10

14. Assoc. Prof. **İbrahim İRDEM**
Dr. **Murat UZUNPARMAK**
(Turkish National Police Academy, Türkiye; Ministry of Interior, Türkiye)
Siber İstihbaratın Küresel Güvenlik Mimarisine Etkisi / 15.10-15.20

15. Asst. Prof. **Laçin AKYIL**
(İstanbul Arel University, Türkiye)
Avrupa Birliği'nin Yeni Bir İstihbarat Servisi Oluşturmasının Türkiye-Avrupa Birliği İlişkilerine Olası Etkileri/ 15.20-15.30

16. Asst. Prof. **Atahan Birol KARTAL**
(İstanbul Beykent University, Türkiye)
İstihbarat ve Teknoloji: Yeni Kaynakların Yönetimi / 15.30-15.40

Q & A
15.40-15.50

BREAK
15.50-16.00

5. SESSION

16.00-17.00

Session Moderator:
Dr. Öğr. Üyesi **Bekir Aşık**

Session Title:
Geopolitical Arguments in Security

17. Assoc. Prof. **Stanislav MYŠIČKA**
(University of Hradec Králové, the Czech Republic)
The PRC Military Base in Djibouti and China's Growing Security Presence in Africa / 16.00-16.10

18. Dr. **Marina GLASER**
(HSE University, , the Russian Federation)
Influence of the Political-Informational "Landscape of Betrayal" on the Intensity of Internal Terrorist Activity During an External Conflict (Case of Russia During the "Special Military Operation") / 16.10-16.20

19. **Sunday Jacob AJOSE**
(Independent Researcher, Nigeria) | Online
Corruption and Violence in Nigeria: A Critical Analysis / 16.20-16.30

20. **Zarina M. LAZAROVA**
(Student, Rakovski National Defence College, Bulgaria) | Online
The Changing Architecture of Security: Zangezur Corridor's Economic Importance / 16.30-16.40

Q & A
16.40-16.50

CLOSING REMARKS
17.00

4. KONUŞMALAR VE SUNUMLAR / *SPEECHES AND PRESENTATIONS*

Konferans 13 Aralık 2024 günü Açış Konuşması, Özel Oturum ve farklı konularda 5 oturum hâlinde gerçekleştirilmiştir. Konferansın açış konuşmalarını yapan Düzenleme Kurulu Başkanı Dr. Öğr. Üyesi Mustafa KARAHÖYÜK (İstanbul Beykent Üniversitesi İktisadi ve İdari Bilimler Fakültesi Öğretim Üyesi) konferansın amacına ve geçmiş konferanslara değinmiştir. İstanbul Beykent Üniversitesi Rektör Yardımcısı Prof. Dr. Kazım SARI ise, siber güvenlik, ekonomik güvenlik, istihbarat ve bilgi operasyonlarına dair konuşmasını yapmıştır.

Konferansın "Güvenliğin Değişen Mimarisi" konulu özel oturumunda İstanbul Beykent Üniversitesi İletişim Fakültesi Dekanı Prof. Dr. Ece BABAN başkanlığında Prof. Christopher FARRANDS (Nottingham Trent University), Emekli Büyükelçi Uluç ÖZÜLKER ve Prof. Dr. Nuray EKŞİ (Marmara Üniversitesi) güncel güvenlik tartışmalarına ilişkin sunumlarını gerçekleştirmişlerdir.

Oturum başlıkları ve moderatörler aşağıdaki gibidir:

1- Siber Güvenlik – Doç. Dr. Ülke Evrim UYSAL

2- Yapay Zekâ – Doç. Dr. Asuman KUTLU

3- Bilgi Operasyonları – Doç. Dr. Kemal OLÇAR

4- İstihbarat – Doç. Dr. Kenan ORÇANLI

5- Güvenlikte Jeopolitik Tartışmalar – Dr. Öğr. Üyesi Bekir AŞIK

&

The conference was held on December 13, 2024 with an Opening Speech, a Special Session and 5 sessions on different topics. The opening speech of the conference was made by the Head of the Organizing Committee, Asst. Prof. Mustafa KARAHÖYÜK (Istanbul Beykent University, Faculty of Economics and Administrative Sciences), who touched upon the purpose of the conference and previous conferences. Istanbul Beykent University Vice Rector Prof. Dr. Kazım SARI made a speech on cyber security, economic security, intelligence and information operations.

In the special session of the conference on the Changing Architecture of Security, Dean of Istanbul Beykent University Faculty of Communication, Prof. Dr. Ece BABAN, Prof. Christopher Farrands (Nottingham Trent University), retired Ambassador Uluç ÖZÜLKER and Prof. Dr. Nuray EKŞİ (Marmara University) made presentations on current security discussions.

The session titles and moderators were as follows:

***1- Cyber Security** – Assoc. Prof. Dr. Ülke Evrim UYSAL*

***2- Artificial Intelligence** – Assoc. Prof. Dr. Asuman KUTLU*

***3- Information Operations** – Assoc. Prof. Dr. Kemal OLÇAR*

***4- Intelligence** – Assoc. Prof. Dr. Kenan ORÇANLI*

***5- Geopolitical Arguments in Security** – Asst. Prof. Bekir AŞIK*

4.1. DAVETLİLERİN SUNUMLARI/ *PRESENTATIONS of the INVITEES*

Konferansımızın açılışında yapılan özel oturumda, dünya gündemini değerlendirmeleri için davet edilen konuşmacılarımız, Türkiye'yi uluslararası alanda temsil etmekten ve Türkiye'nin güvenlik bürokrasisi için personel ve öğrenci yetiştiren kurumlarda yöneticilik yapmaktan kaynaklanan deneyimlerini aktardılar. Bu bölümdeki metinler konuşmacıların sözlerinin metne aktarılması yöntemiyle hazırlanmıştır.

&

In the special session held at the opening of our conference, our invited speakers, who were asked to evaluate the world agenda, shared their experiences stemming from representing Türkiye internationally and managing institutions that train personnel and students for Türkiye's security bureaucracy. The texts in this section have been prepared by transcribing the words of the speakers.

4.1.1. Christopher FARRANDS[2]

Recent discussion by Kruck and Weiss, Mügge and others has deployed the idea of the 'regulatory security state' to try to make sense of the behaviour of governments and government regulatory bodies faced with highly complex technologies and difficult relationships with very powerful technology corporations. This paper begins by accepting that scholars need a new language to describe the adaptation of the state to sophisticated technologies and the corporations which produce and manage them, and finds some value in the concept of a 'regulatory security state'. However, the paper also identifies some important ways in which that concept is inadequate, including both a failure to recognise the scope of change required by innovations (including but not limited to Artificial Intelligence), and a failure to recognise the forms of both power and authority now increasingly exercised by leading corporations. Most of those firms, but not all, are based in the US. How other state authorities manage their relationships with big tech and with the speed of technological innovation may perhaps help to identify questions that need to be examined more closely. Some work already exists on the US and on the EU (which has some extensive legislation partly in place). Other cases may now be useful alongside that work. This paper looks at three brief case studies: Canada, the United Kingdom and Australia, all of which have made different government responses to these issues, and which have different regulatory frameworks to build on. The paper concludes that while none of these might pass for a 'model', there are useful policy lessons to take from the cases, as well as theoretical academic approaches which refine the concept of the state in addressing complex technological change.

[2] Professor, FRSA, FRAI, Nothingam Trent University, United Kingdom.

4.1.2. Uluç ÖZÜLKER[3]

Sevgi ve saygıyla hepinizi selamlıyorum. Hoş geldiniz! Bu arada, bu konuyla ilgili olarak birkaç söz edebilme fırsatı vermiş olduğunuz için teşekkür etmekteyim. Şimdi, şöyle diyelim. Evvela size basit bir şey anlatarak yola çıkmak istiyorum. 8 yıl evvel bana bir ricada bulundular, "bir kitap yaz", dediler. Ben de "Küresel Düzende Oyun Devam Ediyor" isimli bir kitap yazdım. Aslında bu kitap 300-350 sayfa... O da tam sınırda. Neden? Çünkü yaz yaz bitmiyor. O kadar çok şey var ki söyleyecek. Bugün burada anlatacaklarımı, baktım ki 8 yıl evvel zaten bütün haşmetiyle yazmışım. Şimdi, bugün, dolayısıyla bunu paylaşmak istiyorum her şeyden önemlisi. Ama kitapta yazılmış olan şeyler, bugün hepsi gerçek olmuştur. Ben 8 yıl evvel, 14 değişik alanda, dünyanın farklı bir boyuta erişmiş sorunlarla karşı karşıya yaşamakta olduğunu, orada deliller vererek vesaire yazmışım. Şimdi kendi kendime, "Bugün acaba buna ilave ne olabilir, ne olmayabilir?" diye düşünürken; bunların zaten olduğunu ve olmasının dünyada yakın gelecekte beklendiğine dair gelişmeleri her geçen gün biraz daha fazla yaşadığımızı görmekteyim. Üzüleyim mi, sevineyim mi? Onun ikilemi içine girdim.

Evvela çok basit şekliyle bir tarif yapmak lazım. Şimdi biz oturuyoruz ve güvenlik diyoruz. Evde yangın çıkmasın diye neler yapılabileceği hususunda düşündüğümüzde, o da bir güvenliktir. Bugün Suriye meselesi mesela, Türkiye'miz için başlı başına bir güvenliktir. Ama dünya çapında bakıldığı zaman, özetleyerek sizinle paylaşacağım. Bütün bu konularla, hepsi, birer güvenlik sorunu hâline gelip önümüze konulmuş durumdadır. Buradaki en önemli faktör, oradan başlayayım… Bir. Dilerseniz şöyle yapalım. Ben, bu kitabı yazarken de aynı şeylerle karşılaştım. Normal şartlarda, biz kimiz? Homo sapiens(iz). Biz insanların, aşağı yukarı 70 bin ila 150 bin yıl arasında bu dünyada bir varlığımız var. Şimdi, geçenlerde bir yabancı toplantıda tartışılıyor. Keşifler yapılıyor ve bu keşifler, bir tanesi 12 bin yıl, öbürü 5 bin vesaire, böyle gidiyor. Soru şuydu: Eğer biz 70 bin yıldan beri var olan Homo sapiens isek, peki o 70 bin yıl ile bugün arasında, 12 bin yıla kadar iniyoruz. O zaman nasıl oldu? Bir şey oldu herhâlde orada. Oldu da bizim hiçbir şeyden haberimiz yok. Çünkü Atlantis diyoruz, o diyoruz, bu diyoruz. Şimdi, sonuç itibarıyla burada çok önemli bir faktör var. Zannediyorum dünya, her hâlükârda bu krizlerle karşı karşıya kaldı. Başından beri insanoğlu, evvela bir şeyler yapıyor, gelişiyor, en üst düzeye çıkıyor. Daha sonra doğa ya bizi yok ediyor ya da biz kendi kendimizi yok ediyoruz.

Bugün güvenlik dediğiniz zaman hâlihazırda karşı karşıya bulunduğumuz en önemli sorunlardan bir tanesi, nükleer başlık sahibi başat güçlerin bu dünyada birbirini tehdit ederek neyin sonunu getirecekler hususunu, sabahtan akşama kadar işlemekte oluşlarıdır. E peki, ben size yaşanmış bir olay olarak bahsedeyim. Ondan sonra da sırasıyla hemen söyleyeceğim. Çok basit bir şey daha var. Normal koşullarda, insanoğlu öyle veya böyle, zannediyorum kendi kendini aldatmakla zamanını geçiren ve egoizmi dolayısıyla da yok olma noktasına gelmiş olabilecek kadar da acımasız bir yapıda. Hani, bana

[3] Büyükelçi (E) / *Ambassador (Ret)*, Türkiye.

dediler ki çok büyük bir ihtimalle geçmişte de evvela çok büyük bir şey oluyor. Ya deprem oluyor, ya bir afetle karşılaşıyoruz. Ve ondan sonra afet olmasa da kendi kendimizi başka şekilde, bir hegemonya kavgası içinde kendi kendimizi yok ediyoruz. Ve dünya, neticede ayakta kalabilenlerin devam edebileceği bir ortam içinde devam ediyor. 21. yüzyıl, normal şartlarda, eğer bu ortaya konmuş teori gerçek ise, bugün 21. yüzyıl, insanoğlunun gerçek anlamda kendi kendini yok etmeye veya yok etmese bile doğa koşullarını yok etmesi suretiyle, en basit şekliyle hepimizi yok edebilecek bir konuma gelmesi şeklinde gelişen bir suret içine girmiş bulunuyor.

İkinci bir tartışma konusu da yine yurt dışında bir toplantıda dile getirildi. Hristiyan âleminin %40'ı, artık inanmadığını ifade etmeye başlamış. Müslüman dünyasında ise bu oran %19 şu sıralar. Yani, sizin din ve inanç dediğiniz şeyler, bütün bu gelişmelerle birlikte risk altına giriyor veya en azından darbe yiyor. Peki, burada birkaç sual sordular mesela. Cevabını kimse bilmiyor. Sizlerle paylaşarak nerelerde sıkıntımız var, niçin bir felakete doğru biraz da kendimiz isteyerek kendimizi mahvetme noktasına gidiyoruz, devam edeyim. Mesela ortaya atılan iki tane sorun vardı. Çok ilginç… Din faktörünün dünyadaki yeri. Çünkü bu özellikle terörle mücadele dediğimiz şey, dünyayı mahvediyoruz. Burada da uzatmayayım, hepimiz biliyoruz ne olduğunu. Ama burada söylenen bir şey var. Tevrat tek bir tanedir, 3 bin yıllık bir geçmişi var. Eğer 70 bin geriden gelen Homo sapiense, o zaman demek ki geri kalanların hepsi cehennemde mi yanıyor diye sordular. Kendimizi cehenneme atmak için hazır olarak o kapının önünde bekliyoruz demek ki. İkincisi, yani Rusya sabahtan akşama kadar tehdit ediyor. Ben nükleer silahı kullanırsam eğer… Böyle bir şey olabilir mi? Dünyada 9 ülkede hâlihazırda nükleer başlık var. Bunlardan beşi Güvenlik Konseyi üyeleri. Dünyaya hâkimler… İsrail var. 1974'te Fransızlara verdirtti… E şimdi bunlara ilave olarak bir de Kuzey Kore ile 9 tane var. Şu veya bu şekilde nükleer bir çatışma çıkacak olursa, 15 bin 500 civarında dünyada başlık var. Bunlardan %90'ına yakını ABD ve Rusya'nın elindedir. Şimdi, şu sual soruldu toplantıda. Farzımuhal kullandı. E sen de yok olacaksın. Yani netice itibarıyla dünyada, bir başkasına zarar verirken kendini de bu zarardan kurtarmıyorsun ki. Ya blöf yapıyorsun… Efendim, hâlihazırda başat güçlerin dünyasıdır bu. Diğer hepsinin elinde böyle imkânları olmadığı için böyle tehditler karşısında uyum sağlamaya mecbur kalıyorlar. Yani böyle bir zihniyet... Dolayısıyla 21. yüzyıl güvenliğimiz açısından altından kalkamayacağımız olaylar zinciri içerisinde negatif bir sona doğru gidiyor. Dolayısıyla ben size satır başı hâlinde söyleyeceğim. Sorunuz olursa tabii ayrıntılarına da girerim.

1. Küresel Isınma. Peki, küresel ısınmanın sebebi nedir? Çok basit… Biz. Netice itibarıyla evvela ozon tabakasını perişan ettik. Arkasından da genişleme ve gelişme perspektifi hedefiyle, hani, medeniyetimizi daha iyi yere taşıyoruz diye, dünyayı da yaşanamaz bir yer hâline getiriverdik. Bugün de çölleşme kuzeye doğru doludizgin gidiyor. Küreselleşmenin üç boyutu var. Birincisi, biz kendi özkaynaklarımızı yok ederek burada ciddi bir güvenlik sorunu yaratıyoruz. Yapılan bir araştırma var. Macar bir profesör, ilk defa bunu bir rapor hâlinde yazdı ve AB'ye sundu. 2030 yılından itibaren dünya, pek çok yerde ciddi

bir su sorunuyla karşı karşıya kalacak. Bu arada Orta Doğu'da bundan istisnai değildir. 2030 yılından itibaren, hani, bugün hep beraber işte perişan olduk, Suriye vesaire diyoruz, 2030 yılından itibaren Orta Doğu'da Türkiye'mizin de dışında kalamayacağı bir çatışma ortamının su yüzünden yaşanacağını savunuyorlar. Yani dünya toplumu, bir anlamda, susuzluğa itilecek. Bu kapsamda, küresel ısınmayı da bunun tabiiyetiyle bir parçası olarak düşünmek lazım.

2. Hem bölge, hem gelir düzeyi açısından dünyada dengesizliğin çok üst düzeylere çıkmış olması. Yani bir tarafta kişi başına 50 bin dolar gelirle kendisini zararda ve fakirleşme sürecinde gören bir ABD, diğer tarafta günde 1 doları bile bulamadan yaşamaya çalışan ülkeler… Etiyopya'da da yine bu var. Dehşet verici bir şey… Yani, oradaki insanlar yaşıyor mu, yaşamıyor mu? Bu dünyadan mı, değil mi? Belli değil. Bir tek rakam vereyim size: 850 milyon çocuk, genç vesaire şu sırada açlık sınırında. Ölümle baş başa bulunuyorlar dünyada. BM çok basit bir hesaplama yapmıştı. Bundan 10 yıl evvel yayımlandı. Bunun sonradan başımıza geleceğini de görerek… Diyor ki her yıl 27 milyar dolar sayesinde dünyada açlıktan ölüm vesaire, falan, bunlar müstesna hâle gelecektir. ABD Savunma Bakanlığının bu yılki bütçesi, eski bütçesi, 868 milyar dolardır. Bunun ötesinde de bu kaynak, İsrail vesaire bunlara verilen paralarla birlikte 1 trilyon 250 milyar dolar… Yani Türkiye Cumhuriyeti'mizin gayrisafi yurt içi hasılası itibarıyla, bu yıl ulaştığını -parantez içerisinde söylüyorum- ileri sürmüş olduğumuz gayrisafi yurt içi hasılamızın bütünü, ABD'nin 2024 savunma bütçesine denktir. Şimdi burada, 850 milyon insan ölürken biz insanları belki daha kolay öldürüp de sayıyı azaltalım falan diye herhâlde bir felsefeyi takip ederek dünyada inanılmaz bir güvenlik sorununu hep beraber işlemekteyiz. Dolayısıyla bunun en büyük faktörlerinden biri de ekonomidir. Buradaki dengesizlikler, dünya çapında hepimiz için son derece vahimdir.

3. Toplumlar arasında gelişmişlik ve gelişmelerden yararlanma farkının artması. Biraz önce yapay zekâ anlatıldı. Sizin o yapay zekâ dediğiniz şey, aslında dünya çapında kendisini muhteşem, çok zeki, başka türlü gören Amerika'da yaşayan birtakım insanların hiç umursamaz bir şekilde dünyayı bir felâkete sürükleme kararı almalarından ibarettir. Yapay zekâ, sonuç itibarıyla sizin yarattığınız ama sonuçta da dönüp dolaşıp sizin aklınızın yerine geçerek sizi yönlendirecek bir felâketin habercisidir. O zaman ne oluyor? İşte, filmlerde devamlı işlendi. Bambaşka bir dünyaya gideceğiz, en güzel tarifini de bunun biliyorsunuz Orwell yapmıştır; 1984 diye bir kitabı var. Doludizgin, hep beraber oraya gidiyoruz ve bundan da fevkalade müstefitiz: Oh! Ne güzel, ne güzel… Ama şunu da ben söylüyorum buradan; dünyada hâlihazırda çok ciddi biçimde bir değişim var. O da şu, çok satır başı hâline geldi, söyleyeceğim zaman dolayısıyla. Normal olarak Batı dünyası, ABD özellikle, 80 yıldır başat güç olarak bu dünyada hüküm sürdü. Her şey onun üzerine bina edilmiştir. Hâlen bizim yaşam standartlarımız, onların İkinci Dünya Savaşı'ndan sonra empoze edilmiş Bretton Woods Sistemi'ne dayanır. Bu, altından kalkamadığımız, çok ağır sonuçları olan gelişmenin adıdır. Peki, ne değişiyor? Değişen bir şey var. Bu dünyada, sömürge çağı bitti. 19. yüzyılda sömürge çağına girdik ve şu anda sömürge çağı bitti. Ama

bununla birlikte, aynı zamanda dünyaya bugüne kadar topyekûn hâkim olan bu ülkeler de zayıflamaya başladılar. Burada ikiye bölünüyor esas itibarıyla bu zayıflama. Bir tanesi, Avrasya boyutu ortaya çıkıyor. Avrasya boyutu, Varşova Paktı'nın yerini almıştır ve hâlihazırda biliyorsunuz, Rusya, Çin ve Kuzey Kore de bir üçlü ittifak kurdular ayrıca. Hindistan ve İran'ı da aldılar buradaki sistemin içine. Bugün dünya, Batı ile Doğu arasındaki bir çatışmadan geçiyor ve bu çatışmada da Batı dünyası, bugüne kadar alışılageldiği "üstün ırk" yaklaşımını sürdürüyor. Türkiye'yi de onun için sevmezler belki dışarıda. Çünkü biat etmeyi pek beceremeyen bir ülkeyiz, her ne hikmetse. Bu koşullar altında dünya, yeni bir güvenlik sorunuyla karşı karşıya. Kıtalararası bir çatışma var. Bu kıtalarda da bir tanesi diktatörlükler dünyası, Avrasya; diğeri de sözüm ona demokrasilerden oluşuyor ama o demokrasi dostlar başına! Hâlihazırda Fransa'da neler olduğunu biliyorsunuz, Almanya'da ırkçılık nereye gitti. İtalya perişan… Amerika da Trump'la birlikte yakında herhâlde yeni çatışmalarla ilgilenecek. İç sisteminde de birtakım çatlaklar falan olacağı da bekleniyor. Onun için Batı, geriliyor. O zaman ne oluyor? Batı, gerileme politikasını yenebilmek için, ayakta kalabilmek için savaş çıkartmaya yöneliyor efendim. İşte size, buyrun, bir olay daha: Savaş. Biden'ın bütün politikaları, Amerikan hegemonyasında bir savaş çıkararak Çin gibi kendisine rakip olabilecek ülkelere diz çöktürme politikasıdır. Şimdi Trump gelince farklı mı olacak? Olmayacağından da ben size her türlü garantiyi veririm.

4. Ezilmişlik ve mağduriyet duygusunun güçlenerek tepkiselleşmesi. Şimdi, bütün bu anlattıklarımın bir parçası zaten bu. Birtakım insanlar orada kendi zenginliklerini kaybetmemek için, sözüm ona kaybetmemek için, hep başkalarını yok ediyorlar. Bir Fransız dostumla bir gün konuşuyoruz Paris'te. "Yahu bu kadar çırpınıyorsunuz, bir şeyler yapmak için, aslında bizim zihniyetimiz nedir, bilir misin?" dedi. Anlat bakalım, öğrenelim. "İki metre derinliğinde bir havuz düşün," dedi. "Biz, iki kişiyi alıp suya batırıyoruz havuzda, otuz saniyede bir de dışarıya çıkarıyoruz, nefes aldırıyoruz ve tekrar batırıyoruz. Ama biz hep dışarıda yaşıyoruz. Biz bu alışkanlık içinde bugüne kadar geldik. Ama şimdi birileri başka taraftan, bu yanlış yahu, olmaz, deyip ayağımıza basmaya başladılar. Nasıl kurtulacağımızı da bilmiyoruz, biz içeride birbirimizi yemeye başladık," dedi. Bunlar aslında doğrudan doğruya güvenlikle alakalıdır; ezilmişlik ve mağduriyet duygusunun güçlenerek tepkiselleşmesi.

5. Çevresel ve sosyal sorunlar. Kirlenme, göç ve terör, tabiatıyla buna bağlı olarak… Hani göç diyoruz ya, Nostradamus, biliyorsunuz o büyük kâhin, onun 1914 yılında bitiyor kehâneti. Ondan sonrasını kitap olarak herhâlde yazamamış. Orada çok net söylediği bir şey var; dünyayı yok edecek olan Doğu-Batı ekseninde, özellikle sarı ırkın gerçekleştireceği göçtür, diyor. Bugün Türkiye'miz de jeopolitik konumu itibarıyla bunun dışında kalamayacak kadar hassas bir noktada oturmaktadır. Yani, bir de bu tabiatıyla kimse önleyemez. Merkel kitabında yazıyor, "Gittim, kandırdım Türkleri; 6 milyar avrolarını da vermedim". Yarısı geldi, yarısı gelmedi. Sen de batıyorsun. Dolayısıyla beni batırdığın zaman benle birlikte sen de gidiyorsun.

6. Küreselleşme. Ekonomik krizler ve başat ülkelerin sadece kendi menfaatlerini ve bekalarını düşünerek aldıkları önlemlerle dünyayı olumsuz etkilemeleri… Anlatmaya bile gerek yok. Amerika, ya Rab bana, hep bana! Politika bu. Öbür tarafta AB ayaktaydı, şimdi AB gitti. Hiç endişe etmeyin. Şimdi AB çözüldü. Macar başbakan da gelecek. O da Rusya'ya gidiyor mesela, bu arada. İlginç… AB, bizi almadı ama şimdi, hâlihazırda bizden de vazgeçemiyorlar. Çünkü bizden vazgeçti mi burada, hudutlarımızı açtığımız gün, Avrupa bitti! Ama AB, bugünkü koşulları itibarıyla bir ticaret ortaklığıdır. Bunun ötesi de "Avrupa Birliği" yönünden bir hayaldir ve bitmiştir. Netice itibarıyla hiçbir şey de yapamazlar buna karşı. Teferruatına girmeyeyim ama AB; 16 milyar avro, o noktalara kadar gelen ve Amerika ile eş değer bir zenginliği olan bir grup olarak siyaseten ABD'nin yerine geçemedi. Hak ettiği ya da düşündüğü noktayı yakalayamadı, o yok. Ama bunun ötesine, bir ekonomik birliğin ötesine de gidemiyor. Orada ciddi sıkıntıları var. Devamlı krizler içerisine giriyorlar.

7. İletişim araçlarının kontrol edilemezliği. Mesela, en basit şekliyle şu telefon, değil mi? Burada otururken birisi ısrarla aramaya devam ediyor. Ama bunun ötesinde başka bir şey daha var: Bizi esir almış vaziyettedir bütün bu iletişim vasıtaları. Oturup da bu doğru mudur, yanlış mıdır; bunları hiç düşündüğümüz yok. Bendeniz o kadar meraklı değilim telefona. Ama benim torunlar dahi beni otuza, kırka katladılar, ben ne yapsam bükemiyorum. Burada yapay zekâ falan işte, bu konular, teferruatına bırakalım.

8. Fosil yakıtların kirleticiliği, nükleer enerjinin yayılması, kontrol dışına çıkması öyküsünde teröristlerce de kullanılabilmesi dâhil yarattığı büyük risk. Pakistan'ın elinde nükleer başlık var. Pakistan, kendi güvenliği itibarıyla kayıtta, her şeyi kontrol altında tutabilen bir ülke midir? Haşa! Yok. Orada ikide bir ayaklanıyorlar, çarpışıyorlar vesaire. Ezkaza oradaki nükleer silahları ele geçirmiş olsalar, onu da Hindistan'ı vurmak için diyelim ki kullanmaya başladılar. Dünya savaşı çıkar. Yani, oturup da bir Pakistan için dünyanın birbirine girmesi… Pakistan, benim tabii can ciğerim ama oradaki koşullarla birlikte mütalaa ettiğimde çok dikkatli ve aynı zamanda çok kontrol altında tutularak yürünmesi gereken bir ortamı var.

9. Uluslararası örgütlenmenin, hukukun yaptırım gücüne sahip olmaması. Güçlünün kendi çıkar ve kurallarına göre meşruiyet oluşturma kavgası… Amerika, hep başat güç olarak haklı. İsrail'i o destekler. Yapma yahu… Yani İsrail, orada bir soykırım oluşturmuş, Amerika diyor ki yapabilir, haklıdır. Peki, ey Amerika, sen kimsin yahu? Geçmişin de senin hiç tertemiz bir sayfa değil. Oturup da beni "yapmadığım" bir şeyle suçlarken Ermeni vesaire diye; sen git, evvela Kızılderililerden başlamak üzere yedi sülale yok ettin. Ama ben oturup da bunu söylediğim zaman benim karşıma çıkıyorsun. Şimdi dolayısıyla dünyada "Ben güçlüyüm, dolayısıyla haklıyım," zihniyetiyle gittiğin zaman, geçmiş olsun 21. yüzyıl. Hukuk falan da yok hiç, bakmayın. Uluslararası hukuk dediğiniz şey… O konuda benim ihtisasım var. Bir büyükelçi olarak da mecbursunuz zaten. Ama uluslararası hukukta bakıyorum, mesela, efendim,

Netanyahu yakalanırsa ne olurmuş. Türkiye Cumhuriyeti olarak biz, Sudan'daki Sayın Başkan'ı, Türkiye'de alay-ı vâlâ ile çağırıp ağırladık. Hatırlıyorsunuz, değil mi? O da neydi? Şu ünlü ceza mahkemesi var ya Roma'da, onun, tutuklanması ve yargılanması için karar almış olduğu kişiydi. O da öyleydi. Biz Türkiye olarak dahi "Ben o mahkemenin üyesi de değilim," dedik ve onu buraya davet ettik. Netanyahu'yu hiç kimse yakalayamaz, merak etmeyin. Ama orada, göstermelik olarak yapmış gözüküyor.

10. Dinî ve etnik faktörlerin yayılması. Hem kendi içlerinde hem dünya çapında çekişme ve çatışmalara yol açması…

11. Vekâlet savaşı yoluyla taşarenolara havale edilmek suretiyle bölgesel ihtilafların yaygınlaşması. Bunun adına da vekâlet savaşı diyoruz biz. Şimdi Amerika ile Rusya kapışsalar, dünya savaşı başlar. Ama ne yapar, Amerika da Rusya da kendi vekâlet vereceği kimlerse, bunları eğitir. Bugün Suriye falan diyoruz veya orada işte PKK imiş, yok şuymuş, buymuş… ABD, "Ben DAEŞ ile -ki IŞİD aslında o da- mücadele etmek üzere bunu eğittim". Yalan… Baştan aşağıya yalan… Kendileri de IŞİD'den beter. Dünyada hangi ülkeye el atsanız, dünya çapında bakıyorum, bir ateş topu hâlinde savaş var. Dünya savaşıyor bugün. Ama Amerika ile Rusya, Ukrayna'yı günah keçisi olarak kullanıp onlar üzerinden savaşıyor, karşı karşıya gelmiyor. Öbür tarafta Çin, Tayvan'a, bilmem neye gidiyor, olmuyor. Vekâlet savaşları yoluyla aslında Üçüncü Dünya Savaşı'nı, ne zamandan beri, 1990-1991'den beri başlatmış bulunmaktadırlar. 90-91'den kasıt nedir? Gorbaçov orada Perestroyka ve Glasnost ortaya attı. Arkasından kendileri çöktü ve dünya bir yere gitti. Fukuyama diye bir yazar vardır, biliyorsunuz. O bir kitap yazdı. O kitapta; küreselleşen dünyada bir tek güç vardır, o da Amerika'dır ve liberal kapitalizm de bunun temelidir, dedi. 15 yıl sonra da "Çok büyük hata yapmışım, özür diliyorum herkesten," diye bir ikinci kitap daha yazmak mecburiyetinde kaldı. Cümleye bakar mısınız? Yahu bunun adı, bütün dünyayı kendi hegemonyası altında sömürmektir. Bir sömürü düzenidir.

12. Mikro milliyetçiliğin teşviki, yerleşik ulus devlet ve hudut kavramlarının idamesinin giderek zorlaşması. Bugün bunu, bütün haşmetiyle Suriye'de yaşamaktayız. Suriye'de, ABD üçte birine hâkim pozisyondadır ve Türkiye diyor ki toprak bütünlüğünü esas alan bir çözüm peşindeyiz.

13. Kişinin mahremiyetinin kalmaması. Bilgi ve belgelere, resmî ve gayriresmî yollardan kolaylıkla müdahalede bulunulabilmesi.

14. Teknoloji. 21. yüzyılda bir teknoloji dünyasına girdik biz artık. Yani bugüne kadar, 19. yüzyıl bir sömürge çağıydı. Birinci Dünya Savaşı'nda dünya üzerinde 1 milyar nüfus vardı. Hâlihazırda 7,5 milyar nüfusumuz var.

4.1.3. Nuray EKŞİ[4]

Sayın Rektör Yardımcım, Sayın Büyükelçim, kıymetli katılımcılar… Benim size bugün sunacağım konu; göç, hibrit savaş ve güvenlik. Özellikle de Türkiye'nin bizzat kendisini güvenlik riskinin içine atmak için nasıl çabaladığını, yani güvenlik önemlerini alıp kendisini koruması gerekirken nasıl bizzat bu riskin içerisine kendisini attığını ve bu konuda yaptığı hukuki hataları açıklamaya çalışacağım.

Şimdi, hem Avrupa Birliği'nin (AB) hem de NATO'nun stratejik raporlarında göçün, hem hibrit bir savaş olduğu hem de ulusal, bölgesel ve uluslararası bir güvenlik meselesi olduğu açık ve net bir şekilde ifade ediliyor. Üstelik 1970'te UNDP yani Uluslararası Kalkınma Programı, Birleşmiş Milletler'e (BM) bağlı bir organ olan bu birimin yapmış olduğu özel bir çalışma var. Türkiye'de, henüz daha bu konular konuşulmazken; çevresel faktörler sebebiyle iklim göçünün, bir iklim mültecisi yaratacağını ve bu iklim mültecilerinin de aynı şekilde ulusal, bölgesel ve uluslararası güvenlik riski yaratacağını ifade etmiş bulunuyor.

Şimdi, bizim içinde bulunduğumuz coğrafi alana baktığınız zaman, bir yandan Irak'ta, İran'da, Suriye'de olan gelişmeler… Biraz daha eskiye gidin. Eski Yugoslavya İç Savaşı sırasındaki gelişmeler… Biraz daha eskiye gittiğiniz zaman İran'daki devrimden dolayı Türkiye'ye gelen 1-2 milyon insan olduğunu, arkasından 1991'de Belarus'ta imzalanan Sovyet Sosyalist Cumhuriyetler Birliği'nin (SSCB) dağılmasına ilişkin anlaşma çerçevesinde Türkiye, zaten hep bir göçün hedefi hâline gelmiştir.

Yine İkinci Dünya Savaşı sırasında Hitlerden kaçanlar, Museviler de, yine Türkiye'ye gelmiştir. Bunlardan bin tanesi Atatürk'ün özel bir mektubu ile kabul edilmiş, bu bin akademisyen Türkiye'nin çeşitli üniversitelerinde çalışmıştır. Özellikle de 1956 Türk Ticaret Kanunun yapıcısı da Prof. Dr. Hirsch'dir, Almanya'dan kaçan ve Türkiye'ye sığınan bir Yahudiydi.

Şimdi, Türkiye'nin coğrafi alanında, yani bakıyorsunuz. Bulgaristan'da baskıdan kaçan 350 bin kişi 1989 yılında Türkiye'ye geliyor. Arkasından eski Yugoslavya savaşı ve iç savaşı sırasında yaklaşık 60 bin kişi Türkiye'ye gelmiştir. Şimdi her zaman Türkiye bir göç çekim merkezi olarak karşımıza çıkıyor. Şu anda Türkiye, Afrika ülkelerinden başlayan bir iklim göçünün hedefi hâline gelmiştir. Peki, Türkiye bu kadar göçü kaldırabilecek mi? Kaldıramayacağını zaten hepimiz görüyoruz ve hepimiz de biliyoruz.

Türkiye'nin içinde bulunduğu konumunun göçte hedef olmak zorunluluğunu içerde tetikleyen son derece yanlış, hukuka aykırı uygulamalar var. Bir örnekle başlayalım. O zaman Türkiye'nin ne kadar ulusal güvenliğini ön planda tuttuğuna, arkasından da ne kadar yanlış politikalar uyguladığına geçelim.

[4] Prof. Dr., Marmara Üniversitesi (E) / *Professor, Marmara University (Ret)*, Türkiye.

Yıl 1991… Saddam rejiminden kaçmak üzere 500 bin Peşmerge, Türkiye'ye doğru yönelmişti. Türkiye ise BM'yi de harekete geçirerek sınırlarını kapattı. Bu gelen dalgayı Türkiye sınırları içerisine almayacağını ama Irak sınırında bunları tutacağını BM'ye bildirdi.

Fransa ve İran'ın da desteğiyle beraber Türkiye sınırından içeri girmeden ama Irak topraklarında bir tampon bölge, bir güvenlik bölgesi yani bir uçuşa yasak bölge ilan edildi. Gelenler o kesimde tutuldular. Bir kısmı da zamanla Türkiye içine girmeyi başardı. Bir kısmı ise Avrupa ülkelerine gitmeyi başardı ama çoğu 2 yıllık sürecin sonunda biraz da zor şartlarda yaşadıkları için ülkelerine, yani kendi ayrıldıkları daha doğrusu Irak'ın iç kısımlarına doğru gitmek durumunda kaldılar.

Ama 2011'e gelindiği zaman Türkiye'nin çok farklı bir politika uyguladığını, en başta yine bizim bir ya kırmızıçizgimiz var. Biz en fazla Suriye'den 100 bin kişi alırız, diyen dış işlerinin ve iktidarın birden bire bir açık politika denilen ve aslında açık sınır politikası denilen politika uyguladığını görüyoruz. Ama aslında bu bir politikasızlıktır. Çünkü bir ülkenin egemenliğinin ve gücünün başarısı, sınırlanırının korunmasından geçer. Biz sınırlarımızı koruyabiliyor muyuz? Özellikle doğu sınırlarımızı koruyabiliyor muyuz? Hayır. Peki, Türkiye, bir bakıyorsunuz ki yani İdlib'deki El Kaide, Irak ve Şam İslam Devleti (IŞİD/DAEŞ), Heyet Tahrir eş-Şam (HTŞ)… Bunların hepsi zaten uluslararası raporlarda, BM Güvenlik Konseyi kararlarında terörist örgütler ve kişiler olarak yer alıyorlar. HTŞ, BM Güvenlik Konseyinin kararında; Amerika Birleşik Devletleri'nin (ABD) aldığı ayrı kararda; Kanada, Avusturalya ve AB'nin aldığı kararlarda bir terörist örgüt olarak anılıyor ve Colani de terörist kişiler listesinde yer alıyor.

Türkiye, BM'nin üyesi olduğu için BM Güvenlik Konseyinin aldığı karar, Türkiye'yi de bağlıyor. O yüzden Türkiye de bunları terörist örgüt ve kişiler olarak kabul ediyor. Ama bakın, dünyadaki menfaat dengesi değişince… Dün G7 Zirvesi'nde, G7 ülkeleri dediler ki, "biz Suriye'deki bütün farklı etnik kökenden olanları, farklı dinden olanları kucaklayan; insan haklarına ve özellikle de kadın haklarına riayet eden; Suriye'nin üniter yapısına, toprak bütünlüğüne, bağımsızlığına ve kendi halkının kendi kaderini tercih etmesine inanan ve bunun için adım atan bir yönetim olursa bunun yanındayız". Yani ne oldu? Dünün teröristi olarak kabul edilen grup ya da kişiler, diğer ülkelerin başına ödül koyduğu kişiler, bugün farklı bir çehreye sahip olmuş durumdalar.

Günümüzde, artık böyle iki devletin düzenli ordusu arasında yürütülen savaşlar çok nadir... Biz Rusya-Ukrayna örneğinde de gördük ki farklı savaş yöntemleri kullanılıyor. Özellikle de bizim yabancı terörist savaşçı olarak adlandırdığımız veya vekâlet savaşı yürüten gruplar, gerillalar olarak adlandırılan çok farklı grupların farklı çıkarlar doğrultusunda bu ülkelerde kullanıldığına şahit olduk. Suriye, bunun yine en tipik örneklerinden bir tanesi olarak karşımıza çıkıyor. Hibrit savaşta göç nasıl bir araç olarak kullanılıyor? Göç, belirli bir politika doğrultusunda zayıf olan ülkeye yönlendiriliyor. Bu ülke de bu yönlendirilen göç sayısını kaldıracak durumda olmadığı için kendi içinde etnik birtakım gruplar arasında

çatışmalar olduğundan, ekonomik sorunları olduğundan, rüşvet ve yolsuzluk had safhada olduğundan, kamu kurumları çökmüş veya işlevsiz hâle getirilmiş olduğundan, zaten ülke hasass, bir de kaldıramayacağı bir göç dalgası ile yok edilebiliyor.

Şimdi, Suriye İç Savaşı'yla ilgili Amerikalı bir yazarın hazırladığı rapora göre, 1500 civarında farklı terör örgütünün kendi menfaatleri doğrultusunda hareket ettiği belirtilmiştir. Suriye güçlü bir devlet olsaydı, bu kadar terör örgütünün yuvalandığı bir ülke olabilir miydi? Kendi içinde bu dış güçler ile iş birliği yapan iş birlikçileri olmasaydı, elbette bu aktörlerin orda olması mümkün değildi. Aynı zamanda Suriye içerisindeki bu farklı mezhep ve farklı etnik kökene yönelik kaşımalar da bu dağılmanın ve bu ulusal bütünlüğün olmamasının yarattığı sorunlarla toprak bütünlüğünün ortadan kalkmasına sebebiyet vermiştir.

Şimdi, aslında uluslararası hukuk bize yasa dışı göç ile başa çıkabilmemiz için birçok araç vermiş. Nedir bu araçlar? Hiçbir devlet, kendi sınırlarını yabancılara açmak zorunda değil. Örneğin, Türkiye'den bir profesör Amerika'ya gidiyor. İktisat profesörü, 10 yıllık vizesi var ve Amerika onu içeri almıyor. Her şeyi düzgün olmasına rağmen ve geri çeviriyor. Şimdi, bundan dolayı o devleti sorumlu tutamıyorsunuz. Çünkü bir devlet, kimlerin kendi ülkesine gireceğini kendisi belirler. Şunu devlet yapamaz; kendi vatandaşı devlet sınırına giriyorsa, ben sizi içeri almıyorum, diyemez. Kendi vatandaşı terörist olsa bile… Şimdi bizim hiçbir şekilde sınırımızı açmak ya da yabancı uyruklu Suriyelileri Türkiye'ye almak gibi bir yükümlülüğümüz söz konusu olmamasına rağmen, üzülerek belirtirim ki bazı hukukçular da bunun içerisinde, Türkiye'nin böyle bir yükümlülüğünün olduğunu söylüyorlar. Böyle bir yükümlülüğünün olmadığını bütün yabancı literatür ve uluslararası anlaşmalar zaten gösteriyor.

İkincisi, Türkiye, vize konusunda özellikle de 2011 yılından beri inanılmaz bir esneklik içerisinde. Bakıyorsunuz ki kabileler arasında savaşın olduğu Afrika ülkelerinden ve yine Orta Doğu ülkelerinden Türkiye'ye vize muafiyeti ile gelinmesine, 30 günlük, 60 günlük, 90 günlük vize muafiyeti ile gelinmesine izin veriliyor. Zaten vize muafiyeti gelen bir daha Türkiye'den de ayrılmıyor. Çok enteresan bir şey daha var. Türkiye 12-15 yaştan küçük olanlarla 55 yaş ve üzeri olan Irak, Cezayir ve Libya vatandaşlarını Türkiye'ye vizesiz alıyor. Nedir bunun amacı? Bunu defalarca gündeme getirmiş olmamıza rağmen ki 12 yaş ve 15 yaştan küçük demek bakıma muhtaç ve kamuya ciddi yük getirecek bunlar… 55 yaş üstünde olan kişi de muhtemelen çalışma gücü daha zayıf olanlar. Peki, nedir bunun amacı? Bu Resmî Gazete'de yayımlandığı zaman da anlaşılması mümkün olmayan, neyin hedeflendiği bilinmeyen bir durum olarak karşımıza çıkıyor.

Şimdi, demek ki vize konusunda, vizelerin Türk Konsolosluğundan alınması konusunda bir esneklik söz konusu. Bu esnekliğin getirilmesi ve bazı ülkelerin vatandaşına yani iç savaş olan, paralı askerlerin olduğu, çocuk askerlerin kullanıldığı birçok Afrika ülkesinden Türkiye'ye yönelik bu göç dalgalarına

müsaade ediliyor. Buna karşı Türkiye'ye giriş yasağı konulabilir. Koyuluyor da. Şimdi, giriş yasağı olan bu kişinin bir bakıyorsunuz ki Cumhurbaşkanı ile randevusu çıkıyor. Ancak Türkiye'ye girişi yasak. Bunun ulusal güvenlik ve kamu düzenine aykırı bir durumu var, diye ulusal güvenlik açısından Türkiye'ye girişi yasak ama siyasilerle randavusu olabiliyor. Bir başka husus, Türkiye'ye giriş yasağı koyuyor bizim yetkili bakanlar ama idare mahkemesi diyor ki bu raporlarla konulan ülkeye giriş yasaklarını ben dikkate almam. Almak zorunda çünkü anayasamızın 125'inci maddesinde der ki "İdarenin yerine geçerek idare mahkemesi karar veremez." Türkiye'nin ulusal güvenliğini dikkate almak açısından bu kuralı da yine dikkate alması gerekiyor idare mahkemesinin.

Türkiye'de sınır kontolü var mı? Gerçekten de hepimiz görüyoruz ki batıda hem deniz hem de kara yoluyla Bulgaristan'a, Yunanistan'a geçişte inanılmaz bir kontrol var. Ama Türkiye, Doğu ve Güneydoğu Anadolu sınırlarında önemli ölçüde, özellikle de Suriye ve İran sınırına duvar örmesine rağmen, duvarların üstüne dikenli tel çekilmesine rağmen, birtakım manyetik ekipmanlarla donatmasına rağmen, şu anda ilk 10 ay içerisinde Türkiye'ye giren yasa dışı göçmen sayısı 216 bindir. Arkadaşlar, 216 kişi demiyorum. 216 bin, resmî kayıtlara göre ama bu yasa dışı göçte yakalanamayan sayısını zaten bilmiyoruz. 216 bin kişi Türkiye'ye yasa dışı giriyorsa ve bunların ne olduğu bilinmiyorsa… Yani nereden, hangi kimlikle, bir suç örgütü mensubu mu? Bu kadar terör örgütünün kol gezdiği ülkelerden, özellikle de Afganistan'dan yönelen bu yasa dışı göç, nasıl oluyor da durdurulamıyor? Bu da ayrı bir mesele olarak karşımıza çıkıyor. Bir diğer husus AB üyesi ülkeler, Kanada, Avusturalya göçü kendi sınırları dışında durduruyor. Örneğin, Afrika ülkeleri ile anlaşma yapıyor. Niye kendi gemisini açık denizde göçü durdurmak için kullanmıyor? Çünkü siz açık denizde bir geminizi kullanıp, örneğin sahil güvenliği kullanıp, orada göçü engelleyeyim derken ölüme sebebiyet verirseniz uluslararası hukuka göre sorumlusunuz.

Ne yapıyor Avrupa ülkeleri? Başka ülkelerin askerini veya polisini, sahil güvenliğini ya da idari birimlerini sınırlarda, denizlerde kullanarak göçü bizzat kendi orda engellemeye çalışıyor. Örneğin, AB'nin Frontex diye bir gücü var. Bu güç, açık denizlerde ve diğer devletlerin kara suları içerisinde gemiye bir personel gönderiyor ama o gemi ya bir Afrika ülkesinin ya da başka bir ülkenin… Örneğin, Libya'nın gemisi ve orada göçü manevra yapıp hava sahasından helikopterle, denizden de gemilerle engellerken insanların hayatını kaybetmesine sebebiyet verdiği zaman sorumlu kendisi olmuyor. Böylece uluslararası hukukta herhangi bir yasa dışı iş de yapmıyor görüntüsü kazanarak, başka ülkelerle yasa dışı bir biçimde engelliyor. Kendi ülkesine gelen yasa dışı göçmenleri, Nauru gibi daha birçok ada ülkesinin yanı sıra Uganda, Ruanda gibi ülkelere göndererek onları buralarda tutuyor. Ama zaten bu ülkelerin hem ekonomik hem politik sıkıntıları hem de iç kargaşaları, kabileler arası savaşları olduğu için buralara giden yasa dışı göçmenler de bu ülkelerde kesinlikle kalmak istemiyorlar. Göçün dışsallaştırılması veya küçük ada devletlerine yönlendirilmesi göçün *offshoring* yapılması, bu AB üyesi ülkeler de dâhil, uygulanan bir yöntem olarak karşımıza çıkıyor.

Biz peki, ne yapıyoruz? Az önce dedim ya maalesef son yıllarda, özellikle de Türkiye'nin ulusal, bölgesel riske atılması söz konusu ama içeriden de biz buna nasıl bir destek veriyoruz? Birincisi, Türkiye sınırlarını koruyamıyor. Bunu az önce de söyledim. Bütün bu son yapılanlara rağmen Afganistan'dan Türkiye'ye yönelen ciddi bir göç var. Uluslararası hukuka göre bir Afganistan vatandaşı önce İran'a gidiyor ve İran'dan Türkiye'ye geldiği için biz kesinlikle Afganları Türkiye'ye almamalıyız. Bizim kendi iç mevzuatımız bunu bize yasaklıyor. Taraf olduğumuz uluslararası anlaşmalar da bunu bize yasaklıyor. Neden? Çünkü İran'a ayak bastıkları zaman İran onlar için ilk iltica ülkesi, güvenli üçüncü ülkedir. Güvenli üçüncü iltica ülkesinden gelen yabancıları Türkiye kabul etmek zorunda değil. Bir diğer husus, milyonlarca yabancı Türkiye'de yasa dışı olarak çalışıyor. Şu anda Türkiye'de, Çalışma ve Sosyal Güvenlik Bakanlığının 2023 verilerine göre, 407 bin yabancı çalışma izni başvurusu yapmıştır. Sadece 329 bini kabul edilmiş durumda.

Peki, gerisi? Demek ki Türkiye'de milyonlarca yabancı yasa dışı çalışıyor ve bunların çalışma izni yok. Bunlar, Türkiye açısından nasıl bir güvenlik zafiyeti yaratıyor? Çünkü çalışma iznini alırken belirli belgeler sunmaları gerekiyor ve inceleme yapılıyor. Oysaki bu, şu anda mümkün değil. Suriyeliler, Türkiye'de taşınmaz mal edinemez. Bu durum 1929 ve arkasından 1939 ve 1966 yıllarda alınan kararlarca yasaklanmış durumda. Neden? Önce Suriye, toprak reformu adı altında Türk vatandaşlarının taşınmaz malına herhangi bir bedel ödemeksizin el koymuştur. Bizim de 1926-1927 yılında yürürlüğe giren özel bir kanunumuz var. 1062 sayılı Kanun, bu kanun, ülkelerinde Türk vatandaşlarının mal varlığına el koyan devletlerin vatandaşlarının Türkiye'deki mal varlığına el koyulması için misilleme yapma yetkisini veriyor. Biz de Suriyelilerin, Türkiye'deki mal varlığına el koyduk. 2009-2011 yılında Esad-Erdoğan görüşmesinde, bu iki devlette kalan her bir devletin vatandaşının emlakının akıbeti konuşulmuş ve neredeyse çözüme ulaştırılırken Suriye krizi patlak vermiştir. Misilleme kararları yürürlükteyken hâlâ Suriyelilerin Türkiye'de taşınmaz nasıl aldığını benim aklım almıyor. Hukuka aykırıdır. Bu alınan ve verilen tapuların derhâl iptal edilmesi gerekiyor. Suriye vatandaşları Türkiye'de, Türk vatandaşlığını kazanamaz. Bunu, ben söylemiyorum. Bizim 5901 sayılı Kanun'umuz ve bunun uygulama yönetmeliği söylüyor. Ne diyor bunlar? Diyor ki yabancıyı Türk vatandaşlığına alırken bir güvenlik soruşturması yapacaksın. Peki, Türkiye 2013 yılında Suriye ile olan diplomatik ilişkisini kesmişti. Şimdi, dolayısıyla da Türkiye'de bulunan bir Suriyeli ki Suriyelilerin neredeyse %95'inin kayıtları ve geçici koruma kimlik belgeleri beyanları üzerine düzenlendi. Yani benim annem şu, babam şu, şurada doğdum, şu kadar çocuğum var… Kendileri dedi ve bizim yetkililer de ona göre kayıt yaptı. Siz kendi beyanı üzerine kaydı olan, kendi ülkesinde suç işlemiş mi işlememiş mi bilmediğiniz bir kişiyi nasıl vatandaşlığa alırsınız? Çünkü bizim vatandaşlık kanunu emrediyor. Hangi yabancıyı Türk vatandaşlığına alacaksan, güvenlik soruşturmasını yapacaksın. İkincisi, niye alınamaz? Özel bir düzenleme var bizim vatandaşlık kanunu uygulama yönetmeliğinde. Eğer bir kişi Türkiye'de iltica statüsünde bulunuyorsa asla vatandaşlığa alınmaz. Dolayısıyla sen nasıl oluyor da binlerce, yüz binlerce

Suriyeliye vatandaşlık veriyorsun? Sayılar da sürekli değişiyor. İçişleri Bakanı bir açıklamasında, 328 diyor. Bir hafta sonra 150 bin, yani arada bir uçurum da var. Bir diğer husus, Türkiye ile AB arasında Geri Kabul Anlaşması yapıldı. Bu anlaşma, hukuken henüz yürürlükte değil. Dolayısıyla henüz yürürlükte olmayan bir anlaşmaya istinaden biz hâlâ AB üyesi ülkelerden yasa dışı göçmenleri geri alıyoruz. Bu anlaşma yürürlükte olmadığına göre, çünkü anlaşmanın hukuken yürürlüğe girebilmesi için yapılması gereken prosedürler var, teknik detayına girmeyeceğim, bu prosedürler tamamlanmamış durumda. Dolayısıyla da bu durumda biz, bu geri kabul anlaşmasını işletemeyiz. Bu da hukuka aykırı. Pakistan ile geri kabul anlaşması yaptık ama niye Pakistan ile geri kabul anlaşmasını işletip de Türkiye'de bulunan Pakistanlıları kendi ülkelerine geri göndermiyoruz? Bu da ayrı bir konu. Yemen ile biz geri kabul anlaşması yaptık. Yemen, radikal grupların olduğu bir ülke ve biliyorsunuz iç çatışmaları da var. Bu anlaşmanın yürürlüğe girebilmesi için Cumhurbaşkanı tarafından onaylanması gerekiyor. 2017'de imzaladık ama aradan geçen uzun zamana rağmen niye bu anlaşma onaylanmıyor? Son olarak Türkiye, (2024-2028) 12. Kalkınma Planı'nda yasa dışı göçü engelleyeceğini ve bunun için sayıları şeffaf bir şekilde açılayacağını belirtiyor. Ama şöyle diyeyim, yasa dışı göçü engellemek için biz idari kapasitemizi artıracağız. Türkiye'nin en büyük kurumu Göç İdaresi Başkanlığıdır ve binlerce personeli ile 81 ildeki yapılanması hiçbir bakanlıkta yok. Polis ve jandarma da yine göç alanında katkıda bulunuyor. Bütün bu birikimle bu yapıyla sen, yasa dışı göçü engelleyemiyorsan, 500-600 personel istihdam ederek zaten engelleyemezsin. Türkiye'nin bu yasa dışı yapmış olduğu işlemler ulusal güvenliğimizi, bölgesel güvenliğimizi ve uluslararası güvenliği de riske atıyor.

4.2. KATILIMCILARIN SUNUMLARI / *PRESENTATION of the PARTICIPANTS*

Katılımcı sunumları, oturumlara ve afişteki sıraya göre aşağıda sunulmuştur.

&

Participant presentations are presented below according to the sessions and the order in the poster.

4.2.1. Izabela KAPSA[5]: *Contemporary Dilemmas of the Digital State: Balancing Civic Inclusiveness with the Right to Refrain from Technology*

As governments increasingly adopt digital technologies to streamline services, improve governance, and engage citizens, the concept of the digital state has emerged as a cornerstone of modern administration. Artificial Intelligence (AI) and other digital tools offer significant opportunities for civic inclusiveness by enhancing access to public services, improving transparency, and facilitating participatory governance. However, the growing dependence on these technologies raises important dilemmas surrounding individual rights, particularly the right to refrain from using technology. This paper explores the delicate balance between fostering civic inclusiveness through technology and respecting individuals' autonomy to opt out of digital engagement.

Digital tools have profoundly transformed the way citizens interact with the state, enhancing efficiency, accessibility, and inclusiveness in governance and public services. These advancements are particularly advantageous for marginalized groups, such as individuals with disabilities or those residing in remote areas, who face unique challenges in accessing traditional government services. Accessible digital platforms, incorporating features such as screen readers, text-to-speech applications, and keyboard navigation, play a crucial role in fostering digital inclusiveness for individuals with disabilities (Jaeger & Bertot, 2010; Raja, 2016; Almufareh et al., 2024). Similarly, the digitalization of public services reduces geographic barriers for rural populations, enabling them to engage in civic activities and access essential social services without the need for physical travel (Naldi et al., 2015; Lan & Peng, 2018; Meyn, 2020).

AI-driven platforms further enhance the user experience by delivering personalized and context-sensitive services. For example, AI technologies can optimize healthcare delivery, streamline access to public information, and automate routine administrative tasks, enabling governments to address citizens' specific needs efficiently (Kathuria & Rana, 2023; Carayannis et al., 2024; Dilip et al., 2025). Furthermore, e-governance initiatives, such as online voting systems and digital public forums, simplify traditionally complex processes like voting and civic consultations, promoting higher levels of participation and engagement in democratic practices (Hacker & van Dijk, 2000; Zissis & Lekkas, 2011;

[5] Assoc. Prof. Dr. hab., Kazimierz Wielki University, Bydgoszcz (Poland), Faculty of Political Sciences and Administration, E-Mail: izabela.kapsa@ukw.edu.pl, ORCID: 0000-0003-2342-3682

Baxter, 2017; Khatun et al., 2017; Musiał-Karg & Kapsa, 2019; Kapsa, 2021).

Digital tools have significantly transformed the interaction between citizens and the state, enhancing efficiency, accessibility, and inclusivity. This transformation has led to the development of the digital state, a concept that integrates technology into public administration to better serve citizens. Legal frameworks at both national and European levels have been instrumental in guiding this evolution, ensuring that digital services are developed to promote broad citizen participation in the technological revolution. At the European level, the Digital Services Act (DSA) establishes clear rules for online platforms, aiming to create a safer digital space by protecting users' rights and fostering innovation. This regulation enhances transparency and accountability, ensuring that digital services operate fairly and inclusively across the EU. Complementing the DSA, the European Declaration on Digital Rights and Principles (2022) underscores the EU's commitment to an inclusive, fair, safe, and sustainable digital transformation. This declaration defines citizens' rights in the digital space, emphasizing the importance of accessibility and participation for all individuals, including those who may be hesitant or unable to engage with technology. Nationally, particular states have implemented various initiatives to improve the accessibility of digital public services.

These legal frameworks and initiatives aim to bridge the digital divide, ensuring that all citizens, including marginalized groups and those in remote areas, are included in the technological revolution. By promoting digital literacy, enhancing accessibility, and safeguarding individual rights, governments strive to balance the advancement of digital services with the autonomy of individuals who may choose to refrain from digital engagement. However, challenges remain in ensuring that the rapid digitalization of public services does not inadvertently exclude those who are unwilling or unable to participate in digital interactions. Ongoing efforts are necessary to provide alternative access points and support systems, ensuring that the transition to a digital state is truly inclusive and respects individual choices.

Many strategic documents and government actions demonstrate concern for digitally excluded citizens, including the elderly, women, and individuals lacking digital skills. The evolution of strategic goals is evident, shifting focus from mere access to technology, as emphasized in initiatives like eEurope 2002, toward ensuring availability and security, encompassing aspects such as personal data protection and cybersecurity, as outlined in the General Data Protection Regulation (GDPR) and the 2030 Digital Compass. However, there is a notable lack of attention toward citizens who intentionally choose not to engage with digital state resources, often due to a lack of trust in digital solutions. To address this, some countries have implemented hybrid solutions, offering public services through both analog and digital means (e. g. the city of Winterthur in Switzerland and WinLab – a hybrid platform that combines digital and analog interactions to engage residents in smart city initiatives). Additionally, efforts are underway to increase trust in the digital state, aiming to boost participation in its resources (Pöysti, 2018). Implementing opt-in clauses, as described in the ePrivacy Directive, could also enhance user autonomy

and data protection. Article 5(3) of the directive mandates that users must provide informed consent (opt-in) before any information is stored or accessed on their devices, such as through cookies, unless the cookie is strictly necessary for the service requested by the user. Additionally, users must be given the option to withdraw their consent (opt-out) at any time, ensuring they maintain control over their personal data and privacy (Ranchordás, 2022).

These measures aim to balance the advancement of digital services with the autonomy of individuals who may choose to refrain from digital engagement, ensuring that the transition to a digital state is inclusive and respects individual choices. However, there remains no clear resolution on how to reconcile the dilemma of further developing the digital state while upholding citizens' rights to abstain from technology use. Ongoing discussions emphasize the need for inclusive digital strategies that respect individual choices and ensure equitable access to public services, regardless of one's willingness to engage digitally. Addressing these challenges requires a nuanced approach that balances technological advancement with respect for individual autonomy. Legal frameworks must be adaptable, ensuring that digital services are accessible and inclusive without becoming obligatory. Moreover, ethical guidelines should govern the use of AI and data collection to protect privacy and prevent unwarranted surveillance. By considering these factors, governments can foster a digital state that upholds both innovation and individual rights.

Even many international organizations supports governments in digitally transforming their public services, advocating for accessible and co-created digital service solutions built on inclusive, user-centric and equitable digital public infrastructure ensuring that all citizens, including those who may be reluctant to engage digitally, have access to public services (EU, OECD, UN), there remains a pressing need to develop digital strategies that respect individual choices, protect fundamental rights, and ensure equitable access to public services, thereby fostering a digital state that balances innovation with individual autonomy. As the digital state expands, concerns regarding the right to refrain from technology grow. Many individuals, whether due to privacy concerns, lack of access, or personal preference, may wish to opt out of digital systems. The question of how governments can ensure that those who choose not to use technology are not excluded remains open.

Keywords: Civic Inclusiveness, Digital Autonomy, Digital State, Right to Refrain from Technology, Technological Abstention

4.2.2. Kamila SIERZPUTOWSKA[6]: *Cybersecurity Threats as one of the Challenges for NATO in the Face Of The Russian - Ukrainian War*

The Russian-Ukrainian conflict has significantly highlighted the strategic importance of cybersecurity for NATO's eastern flank. Cyberattacks have emerged as a critical element in Russia's hybrid warfare strategy, posing threats not only to Ukraine but also to NATO member states in Eastern Europe, including Poland, Estonia, and Lithuania. These attacks, often targeting critical infrastructure, government institutions, and key economic sectors, have amplified vulnerabilities across the region, challenging the stability and security of the alliance. The increasing sophistication and frequency of such cyber operations necessitate a multifaceted response from NATO, emphasizing the development of cyber resilience, enhanced cooperation among member states, and improved awareness of cyber threats.

Russia's long-standing use of cyber tools as instruments of destabilization has become a defining characteristic of its engagement in the hybrid warfare domain. Cyberattacks are employed to disrupt essential services, gather sensitive information, and spread misinformation, ultimately undermining the sovereignty and governance of targeted states. In NATO's eastern region, these attacks not only destabilize individual nations but also strain collective defense mechanisms, challenging the alliance's ability to respond cohesively. In particular, critical infrastructure such as energy grids, transportation systems, and communication networks has become focal points of malicious cyber activities. The targeting of these assets demonstrates the interdependence of digital and physical domains, underscoring the urgency for NATO to adapt its security architecture to address these emerging threats effectively.

The Eastern European NATO member states, being geographically closer to the conflict and often directly in Russia's sphere of influence, bear the brunt of these cyber operations. Poland, Estonia, and Lithuania have reported a surge in cyber incidents since the onset of the Russian-Ukrainian conflict (Microsoft Digital Defense Report, 2024). These attacks have ranged from Distributed Denial of Service (DDoS) campaigns to more sophisticated and coordinated efforts to breach sensitive systems. The operational and economic costs of these cyber intrusions are substantial, disrupting services and eroding public trust in government and private sector institutions. Furthermore, the psychological impact of persistent cyber threats adds to the overarching goals of hybrid warfare by fostering a climate of uncertainty and fear.

In response to these challenges, NATO has recognized the critical need to bolster its cyber capabilities and has taken steps to integrate cyberspace into its broader defense strategy. One of the key aspects of this effort is enhancing the cyber resilience of member states. This involves not only fortifying the technical infrastructure but also fostering a culture of cyber vigilance and preparedness. By promoting the adoption of robust cybersecurity standards and encouraging the development of national cyber

[6] Dr., Kazimierza Wielkie University in Bydgoszcz, Poland.

defense strategies, NATO aims to reduce vulnerabilities and improve the overall capacity of member states to withstand and recover from cyberattacks.

Strengthening cooperation among NATO members is another cornerstone of the alliance's approach to countering cyber threats. The inherently transnational nature of cyberspace demands a coordinated response that transcends national borders. NATO has emphasized the importance of information sharing, joint exercises, and collaborative frameworks to improve situational awareness and readiness. Initiatives such as the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), based in Estonia, have become instrumental in facilitating research, training, and collaboration in the field of cybersecurity. These efforts underscore NATO's commitment to building a collective defense posture that integrates cyber capabilities as a fundamental element of its operations.

Another critical component of NATO's strategy is raising awareness of cyber threats and fostering a deeper understanding of the evolving nature of cyber warfare (Pernik, 2022, p. 60-63). This involves educating policymakers, military personnel, and the general public about the risks associated with cyberattacks and the measures needed to mitigate them. Public awareness campaigns, workshops, and strategic communications are employed to counter misinformation and build resilience against psychological and informational aspects of hybrid warfare. By fostering a well-informed and vigilant society, NATO aims to reduce the effectiveness of cyberattacks as tools of destabilization (Bindt et al, 2017, p. 11-16; Dyner, 2023, p. 1-2; Miron&Thornton, 2022, p. 117-121; Miron&Thornton, 2024; p. 2-22).

The Russian-Ukrainian conflict has also underscored the importance of integrating cyber defense into NATO's broader security framework. Cyberspace is now widely recognized as the fifth domain of warfare, alongside land, sea, air, and space. This paradigm shift requires NATO to treat cyber operations as an integral component of its military planning and decision-making processes (RAND, 2019). The alliance has begun to incorporate cyber scenarios into its joint exercises and war games, ensuring that member states are prepared to respond effectively to cyber contingencies. Moreover, NATO's focus on deterrence extends to the cyber domain, with efforts to communicate the alliance's capabilities and resolve to potential adversaries.

Despite these advancements, significant challenges remain in addressing cyber threats in the context of hybrid warfare. One of the primary difficulties lies in attributing cyberattacks to specific actors with a high degree of confidence (Smeets, 2023, p. 1343-1362; Liebetrau 2022, p. 136-138; Vičič&Harknet, 2024, p. 901-910;). The anonymity afforded by cyberspace enables adversaries to obscure their identities, complicating the task of holding perpetrators accountable. This lack of clear attribution can hinder NATO's ability to respond decisively and may embolden malicious actors to continue their activities with impunity. To address this issue, NATO is investing in advanced threat intelligence capabilities and fostering closer cooperation with private sector partners, who often possess critical

insights into cyber threats.

Another challenge is the rapid pace of technological change, which continuously alters the landscape of cyber warfare. Emerging technologies such as artificial intelligence, quantum computing, and the Internet of Things (IoT) present both opportunities and risks for NATO's cybersecurity efforts. While these technologies offer new tools for defense and resilience, they also expand the attack surface and create vulnerabilities that adversaries can exploit. NATO must remain agile and forward-looking, ensuring that its cyber strategy evolves in tandem with technological advancements.

The ongoing Russian-Ukrainian conflict serves as a stark reminder of the evolving nature of modern warfare and the central role of cyber operations within it. For NATO, the lessons learned from this conflict extend beyond the immediate challenges posed by Russia's cyber activities. They underscore the broader need to adapt to a world where the boundaries between physical and digital threats are increasingly blurred. By prioritizing cyber resilience, fostering cooperation, and embracing innovation, NATO can strengthen its collective security in the face of emerging hybrid threats.

In conclusion, the Russian-Ukrainian conflict has brought cybersecurity to the forefront of NATO's strategic agenda, highlighting its critical importance for the alliance's eastern flank. The increasing frequency and sophistication of cyberattacks in the region demand a comprehensive and coordinated response that integrates cyberspace into NATO's defense framework. By enhancing resilience, fostering collaboration, and raising awareness, NATO can effectively counter the cyber threats posed by hybrid warfare and safeguard the security of its member states. The lessons learned from this conflict will undoubtedly shape the alliance's approach to cybersecurity in the years to come, ensuring that it remains prepared to address the challenges of an increasingly interconnected and contested world.

Keywords: Cybersecurity, NATO, Cyberspace, Cyberstability, Cyber War

4.2.3. Şükran ORUÇ[7] & Özlem ÇILDIRIM KOCABIYIK[8]: *Dijital Dönüşümde Güvenlik Algısının Değişen Yüzü: Siber Güvenlik*

Dijital teknolojilerin hızla gelişmesi ve internet kullanımının yaygınlaşmasıyla dijital dönüşüm, tüm alanlarda kendini göstermeye başlamıştır. Dijital dönüşüm, yeni fırsatlar ve değerler yaratırken bireylerin yaşamlarında önemli değişikliklere yol açmakta ve sosyal yapıları dijital teknolojilerle güçlendirmektedir (Bozkurt vd., 2021, s. 40). Özellikle internet üzerinden gerçekleştirilen işlemler ve dijitalleşen hizmetler, bireylerin kişisel bilgilerini ve dijital varlıklarını daha önce hiç olmadığı kadar

[7] Dr. Öğr. Üyesi, İstanbul Beykent Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, E-Posta: sukranoruc@beykent.edu.tr, ORCID: 0000-0002-8176-4058

[8] Arş. Gör., İstanbul Beykent Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, E Posta: ozlemcildirim@beykent.edu.tr, ORCID: 0000-0001-9873-005X

riske atmaktadır. Bu durum, siber güvenliğin önemini her geçen gün artırmaktadır. Siber güvenlik, siber alanı, örgütleri ve bireyleri korumak için kullanılan bir dizi politika, araç, kavram ve teknolojilerle tanımlanır (Akt., Pavlova, 2020, s. 242).

Günümüz dijital dünyasında, bireylerin güvenlik tehditlerine karşı farkındalık sahibi olmaları, kişisel güvenliklerini sağlamaları açısından kritik bir rol oynamaktadır. Bu noktada, dijital dünyada yetişen "dijital yerliler" olarak da nitelendirilen Z Kuşağı, zamanlarının büyük kısmını dijital platformlarda geçiren ve medya ortamında olgunlaşan bir nesil olarak siber güvenlik tehditlerine karşı diğer kuşaklara göre daha fazla risk altındadır (Gümüş, 2020, s. 385; Nair ve Sadasivan, 2019, s. 44). Dolayısıyla bu kuşağın dijital güvenlik konusundaki farkındalık düzeyinin bireysel, organizasyonel ve toplumsal güvenlik açısından büyük öneme sahip olduğu düşünülmektedir. Ancak ilgili yazın incelendiğinde, Z Kuşağı'nın siber güvenlik farkındalığı ve davranışları üzerine yürütülen araştırmaların sınırlı olduğu görülmektedir (Yiğit ve Seferoğlu, 2019; Erdal vd., 2023). Ayrıca siber güvenlik konusunda yapılan çalışmaların genel anlamda teknolojiyi nasıl kullandıkları üzerine odaklandığı, buna karşın tehdit algılamaları gibi konuları göz ardı ettiği dikkat çekmektedir (Saeed vd., 2023; Pavlova, 2020; Karakaya ve Yetgin, 2020; Ünal ve Ergen, 2018). Bu bağlamda araştırma, Z Kuşağı'nın siber güvenlik farkındalık düzeylerini belirlemeyi ve bu farkındalığın çeşitli demografik özelliklere göre nasıl farklılaştığını incelemeyi amaçlamaktadır. Ayrıca dijital dünyada daha güvenli bir gelecek için gerekli adımların atılmasına ışık tutmayı hedeflemektedir.

Araştırmada nicel araştırma yaklaşımı benimsenmiş ve alan araştırması deseni kullanılmıştır. Veriler, Erol vd. (2015) tarafından geliştirilen "Kişisel Siber Güvenliği Sağlama Ölçeği" ve katılımcıların demografik bilgilerini (cinsiyet, sınıf, online alışveriş yapma durumu, yaş, haftalık internet kullanma süresi, günlük ortalama sosyal medya kullanma sıklığı, kişisel siber güvenliği sağlama bilgi ve becerilere sahip olma durumu, eğitim görülen bölüm ve siber saldırıya maruz kalma durumu) içeren anket aracılığıyla toplanmıştır. Ölçek; kişisel gizliliği koruma, güvenilmeyenden kaçınma, önlem alma, ödeme bilgilerini koruma ve iz bırakmama olmak üzere 5 boyuttan oluşmakta olup 25 maddeden oluşan 5'li Likert tipi bir ölçek kullanılmıştır. Araştırmanın evreni İstanbul'daki bir vakıf üniversitesinin İktisadi ve İdari Bilimler Fakültesinde öğrenim gören 2764 öğrenci olup veriler, kolayda örnekleme yöntemiyle 400 öğrenciden yüz yüze görüşerek toplanmış ve 338 geçerli anket verisi analizlere esas oluşturmuştur.

Veri analizi için SPSS 27 ve AMOS istatistik programları kullanılmıştır. Toplanan veriler, frekans analizi, doğrulayıcı faktör analizi, güvenilirlik analizi, tanımlayıcı istatistik, bağımsız örneklem t testi ve tek yönlü varyans analizi (ANOVA) ile analiz edilmiştir. Gruplar arasındaki farklılaşmalar Post-Hoc Testi (Tukey) ile değerlendirilmiş ve tüm analizlerde anlamlılık düzeyi 0,05 olarak kabul edilmiştir. Verilerin normalliği, çarpıklık (skewness) ve basıklık (kurtosis) değerleri hesaplanarak incelenmiş, sonuçlar -1,488 ile 1,481 arasında bulunmuş ve bu değerler kabul edilebilir sınırlar içinde olduğu için verilerin normal dağılım gösterdiği varsayılmıştır (Tabachnick ve Fidell, 2012). Verilerin analizine

başlamadan önce ön analizler yapılmış ve veriler analiz için hazır hâle getirilmiştir. Ardından Doğrulayıcı Faktör Analizi (DFA) ile ölçeğin yapı geçerliliği test edilmiştir ve elde edilen uyum iyiliği değerlerinin iyi ve kabul edilebilir seviyelerde olduğu (x^2/df: 1,441; GFI: 0,919; CFI: 0,967; AGFI: 0,901; RMR: 0,079; RMSEA: 0,036) tespit edilmiştir (Meydan ve Şeşen, 2015; Karagöz, 2019: 133). Ölçeğin güvenilirliği ise Cronbach's Alpha (α) katsayısı hesaplanarak test edilmiştir. Kişisel Siber Güvenliği Sağlama Ölçeği için Cronbach's Alpha değeri 0,809; Kişisel Gizliliği Koruma boyutu için 0,829; Güvenilmeyenden Kaçınma boyutu için 0,921; Önlem Alma boyutu için, 0,875; Ödeme Bilgilerini Koruma boyutu için 0,919 ve İz Bırakmama boyutu için 0,720 olarak hesaplanmıştır. Bu anlamda ölçeğin geneli ile boyutlarına ilişkin elde edilmiş olan 0,70 ve üzeri Cronbach's Alpha değerleri, ölçeğin geneli ile boyutlarının yeterli sayılabilecek ölçüde güvenilir olduğuna işaret etmektedir (Nunnally, 1978).

Z Kuşağı'nın Kişisel Siber Güvenlik Farkındalığı

Araştırma kapsamında öncelikle Z Kuşağı'nın kişisel siber güvenliği sağlama genel ortalaması $\bar{x}$=3,7857 olarak bulunmuştur. Boyutlar açısından incelendiğinde ise "kişisel gizliliği koruma" için $\bar{x}$=3,6905; "güvenilmeyenden kaçınma" için $\bar{x}$=4,0392; "önlem alma" için $\bar{x}$=3,6041; "ödeme bilgilerini koruma" için $\bar{x}$=4,2500 ve son olarak "iz bırakmama" için $\bar{x}$=3,7648 olarak elde edilmiştir. Bu bulgular Z Kuşağı'nın siber güvenlik farkındalık düzeyinin ortalamanın üzerinde olduğunu göstermektedir. Ayrıca ölçekte yer alan kişisel siber güvenliği sağlamaya yönelik ifadelerinden en yüksek ortalamaya $\bar{x}$=4,4556 ile "Şahsi bilgisayarım dışında kullanılan bilgisayarlarda bilgilerimin kalmamasına dikkat ederim." ifadesinin buna karşın en düşük ortalamaya $\bar{x}$=3,2367 ile "E-posta ile gelen kimlik doğrulama mesajlarını (kullanıcı adı, şifre vb. istekler) cevaplarım." ifadesinin sahip olduğu görülmüştür.

Demografik Özellikler ve Kişisel Siber Güvenlik Arasındaki Farklılaşmalar

Demografik özellikler ve kişisel siber güvenlik arasındaki farklılaşmalar incelendiğinde, cinsiyet ve online alışveriş yapma durumu açısından "kişisel siber güvenliği sağlama" düzeyinde anlamlı bir farklılaşma saptanmamıştır. Boyutlar açısından incelendiğinde, ilk olarak cinsiyet açısından "önlem alma" ve "iz bırakmama" boyutlarında anlamlı farklılaşmalar saptanmıştır ($p<0,05$). Erkekler "önlem alma" (μ=3,8292) konusunda kadınlara (μ=3,3320) göre daha yüksek puan alırken kadınlar, "iz bırakmama" (μ=3,8938) konusunda erkeklerden (μ=3,6581) daha yüksek puanlar almıştır. Bu bulgular, kadınların iz bırakmama konusunda daha dikkatli davrandığını, erkeklerin ise önlem alma konusunda daha fazla çaba harcadığını göstermektedir. Online alışveriş yapma durumu açısından ise sadece "güvenilmeyenden kaçınma" (μ=4,0724; $p<0,05$) ve "ödeme bilgilerini koruma" (μ=4,2790; $p<0,05$) boyutlarında anlamlı farklılaşmalar saptanmıştır. Bu sonuçlar, online alışveriş yapan bireylerin, güvenilmez sitelerden kaçınma ve ödeme bilgilerini koruma konusunda daha yüksek farkındalık sergilediğini ortaya koymaktadır.

Sınıf düzeyi ile kişisel siber güvenlik arasında sadece "güvenilmeyenden kaçınma" boyutunda anlamlı bir farklılaşma saptanmıştır (F = 4,368, p = 0,005). Tukey Testi, bu farklılaşmanın 2. sınıf ile 1., 3. ve 4. sınıf öğrencileri arasında gerçekleştiğini göstermektedir. 3. sınıf öğrencileri, "güvenilmeyenden kaçınma" davranışını $\bar{x}$ = 4,1941 ile diğer gruplardan daha belirgin bir şekilde sergilemektedir. Bu bulgu, 3. sınıf öğrencilerinin diğer gruplara göre daha yüksek bir farkındalık ve dikkat gösterdiğini ortaya koymaktadır. Yaş ile kişisel siber güvenlik arasında sadece "önlem alma" boyutunda anlamlı bir farklılaşma saptanmıştır (p < 0,05). Tukey Testi, bu farklılaşmanın 23 yaş ve üzeri katılımcılar ile 17-19 yaş arası katılımcılar arasında olduğunu ortaya koymaktadır. 23 yaş ve üzeri katılımcılar, $\bar{x}$ = 3,9333 ile 17-19 yaş arası katılımcılara ($\bar{x}$ = 3,4043) kıyasla daha fazla "önlem alma" davranışı sergilemektedir. Bu bulgu, 23 yaş ve üzeri bireylerin siber güvenlik konusunda daha dikkatli ve temkinli davrandığını göstermektedir. Haftalık internet kullanım süresi ile kişisel siber güvenlik arasında sadece "iz bırakmama" boyutunda anlamlı bir farklılaşma saptanmıştır (p < 0,05). Tukey Testi, bu farklılaşmanın 1-10 saat internet kullanan katılımcılar ile 21 saat ve üzeri internet kullanan katılımcılar arasında olduğunu göstermektedir. 1-10 saat internet kullanan katılımcılar, $\bar{x}$ = 4,0064; 21 saat ve üzeri kullananlara ($\bar{x}$ = 3,6526) kıyasla daha fazla "iz bırakmama" davranışı sergilemektedir. Bu bulgu, haftalık 21 saat ve üzeri internet kullanan bireylerin, siber güvenlik konusunda daha temkinli davrandığını göstermektedir. Kişisel siber güvenliği sağlama bilgi ve becerilerine sahip olma durumu açısından, "kişisel siber güvenliği sağlama" ve "önlem alma" boyutunda anlamlı farklılaşmalar saptanmıştır (p<0,05). Tukey Testi sonuçları, "kişisel siber güvenliği sağlama" bilgi ve becerisine sahip katılımcıların ($\bar{x}$=3,8817), sahip olmayanlara ($\bar{x}$=3,6777) kıyasla daha yüksek puanlar aldığını ve bu bireylerin güvenliklerine daha fazla özen gösterdiğini ortaya koymaktadır. Benzer şekilde, "önlem alma" davranışı açısından da bilgi ve beceriye sahip katılımcılar ($\bar{x}$=3,8448), sahip olmayanlar ($\bar{x}$=3,3321) ve fikri olmayanlara ($\bar{x}$=3,4418) kıyasla daha yüksek puanlar almışlardır. Bu bulgular, kişisel siber güvenliği sağlama bilgi ve becerilerine sahip bireylerin daha dikkatli ve bilinçli davrandığını ortaya koymaktadır. Eğitim görülen bölüm açısından "kişisel gizliliği koruma" (F=6,903; p<0,001) ve "iz bırakmama" (F=3,207; p=0,008) boyutlarında anlamlı farklılaşmalar gözlemlenmiştir (p<0,05). Tukey Testi, bu farklılaşmanın yönetim bilişim sistemleri (YBS) öğrenimi gören katılımcılarla işletme, iktisat öğrenimi görenler; ayrıca lojistik öğrenimi gören katılımcılarla işletme öğrenimi görenler arasında olduğunu göstermektedir. Puan ortalamalarına bakıldığında, YBS öğrenimi gören katılımcıların ($\bar{x}$=3,9554), işletme ($\bar{x}$=3,3105) ve iktisat ($\bar{x}$=3,4537) bölümlerindeki katılımcılara kıyasla daha yüksek puanlar aldığı saptanmıştır. Lojistik öğrenimi gören katılımcıların ise ($\bar{x}$=3,8107), işletme öğrenimi görenlere ($\bar{x}$=3,3105) kıyasla daha yüksek puanlar aldığı saptanmıştır. İz bırakmama davranışı açısından yapılan Tukey Testi ise, farklılaşmanın iktisat öğrenimi gören katılımcılarla YBS ve lojistik yönetimi öğrenimi görenler ve bankacılık-finans öğrenimi gören katılımcılarla YBS ve lojistik yönetimi öğrenimi görenler arasında olduğunu ortaya koymaktadır. Puan ortalamaları incelendiğinde, iktisat öğrenimi gören katılımcılar ($\bar{x}$=4,0061), YBS ($\bar{x}$=3,5817) ve lojistik yönetimi ($\bar{x}$=3,5446) öğrenimi görenlere

kıyasla daha yüksek puanlar alırken bankacılık ve finans öğrenimi gören katılımcılar ($\bar{x}$=3,9856) ise, YBS ($\bar{x}$=3,5817) ve lojistik yönetimi ($\bar{x}$=3,9856) öğrenimi görenlere kıyasla daha yüksek "iz bırakmama" davranışı sergilemiştir. Bu bulgular, öğrenim görülen bölümün kişisel siber güvenlik davranışları üzerinde önemli bir etkisi olduğunu göstermektedir. Günlük sosyal medya kullanım süresi ve siber saldırıya maruz kalma durumu ile kişisel siber güvenliği sağlama ve boyutları arasında anlamlı bir farklılaşma bulunmamıştır ($p > 0,05$).

Sonuç olarak, bu araştırma, dijital dönüşümle birlikte değişen güvenlik algısının, siber güvenlik farkındalık düzeyine etkilerini ve Z Kuşağı'nın demografik özelliklere göre nasıl farklılaştığını incelemiştir. Araştırma bulguları, Z Kuşağı'nın genel olarak siber güvenlik konusunda ortalamanın üzerinde bir farkındalık düzeyine sahip olduğunu göstermektedir. Karacı vd. (2017, 2091), benzer şekilde araştırmalarında öğrencilerin siber güvenlik davranışlarının yeterli düzeyde olduğunu tespit etmiştir. Erdal vd. (2023, s.1) çalışmalarında, siber güvenlik algısı ölçeğinin alt boyutlarından "güvenilmeyenden kaçınma" boyutunun en yüksek ortalamaya sahip olduğunu; "kişisel gizliliği koruma" boyutunun ise en düşük ortalamayı aldığını tespit etmişlerdir. Bulgular, ayrıca demografik faktörlerin kişisel siber güvenlik davranışlarını etkilediğini ortaya koymaktadır. Cinsiyet ve sınıf düzeyinin, siber güvenlik davranışlarında bazı boyutlarda anlamlı farklılıklara yol açtığı görülmüştür. Erkeklerin önlem alma konusunda, kadınların ise iz bırakmama konusunda daha dikkatli oldukları tespit edilmiştir. Ayrıca online alışveriş yapma durumu ile güvenilmeyen sitelerden kaçınma ve ödeme bilgilerini koruma davranışları arasında da farklılıklar gözlemlenmiştir. Yazında da yürütülen araştırmalarda, cinsiyetin siber güvenlik tutum ve davranışları üzerindeki etkisinin ele alındığı görülmektedir. Bu kapsamda bazı araştırmalar, cinsiyet açısından farklılaşma bulmazken (Subramaniam, 2017, s. 9; Yan vd., 2018, s.19) bazı araştırmalarda ise, erkek öğrencilerin (Gökmen ve Akgün, 2015, s. 61; Karacı, vd., 2017, s. 2081) veya kadın öğrencilerin (Tekerek ve Tekerek, 2013; Karacı, vd., 2017, s. 2081) siber güvenlik bağlamında daha yüksek bir farkındalık sergilediğini ortaya koymuştur. Yine Ünal ve Ergen'in (2018, s. 191) araştırmasında, kadınların yazılım güncelleme sıklığının erkeklerden yüksek olduğunu ortaya koymuştur.

Araştırma bulguları; yaş, haftalık internet kullanımı ve eğitim görülen bölüm gibi faktörlerin kişisel siber güvenlik davranışları üzerinde etkili olduğunu göstermektedir. Ünal ve Ergen (2018, s. 212) tarafından yapılan bir çalışmada, internette geçirilen sürenin artışıyla birlikte proaktif farkındalık seviyesinin yükseldiği gözlemlenmiştir. Bu da internet kullanım süresi az olan bireylerin, siber güvenlik davranışlarını daha az sergilediklerini ortaya koymaktadır. Yiğit ve Seferoğlu (2019, s. 186), özellikle 3. ve 4. sınıf öğrencileri ile haftada 6-10 saat internet kullanan bireylerin, siber güvenlik davranışları açısından daha yüksek bir düzeyde olduklarını tespit etmişlerdir. Ayrıca öğrencilerin sosyal medya kullanımı ile siber güvenlik algısı arasında anlamlı bir ilişki bulunmamıştır. Çalışma, katılımcıların kişisel güvenlik bilgisi ve becerilerine sahip olup olmalarına göre siber güvenlik farkındalıklarının

farklılaştığını da göstermektedir. Siber güvenlik konusunda bilgi ve beceriye sahip katılımcıların daha yüksek güvenlik önlemleri aldıkları ve daha bilinçli davrandıkları gözlemlenmiştir. Buna karşın siber saldırıya maruz kalma durumu ile kişisel güvenlik davranışları arasında anlamlı bir fark bulunmamıştır. Sonuç olarak Z Kuşağı'nın dijital güvenlik konusunda farkındalığa sahip olduğu, ancak bu farkındalığı destekleyecek daha fazla eğitime ve farkındalık artırıcı programlara ihtiyaç duyduğu anlaşılmaktadır. Üniversiteler ve diğer eğitim kurumlarında, özellikle Z Kuşağı'na yönelik, demografik özelliklere dayalı özelleştirilmiş siber güvenlik eğitimlerinin güçlendirilmesi gerektiği vurgulanmaktadır. Bu eğitimlerin, gençleri siber tehditlere karşı daha bilinçli ve güvenli davranmaya yönlendirecek şekilde yapılandırılması büyük önem taşımaktadır. Elde edilen bulgular, Z Kuşağı'nın dijital güvenlik konusunda daha fazla farkındalık geliştirdiğini ve bu farkındalığı artırmak için daha fazla eğitim ve farkındalık programına ihtiyaç duyduğunu ortaya koymaktadır. Üniversiteler ve diğer eğitim kurumlarında, özellikle Z Kuşağı'na yönelik siber güvenlik eğitimlerinin güçlendirilmesi ve artırılması gerekmektedir. Bu eğitimlerin, demografik özelliklere dayalı olarak özelleştirilmesi, bu kuşağın siber tehditlere karşı daha bilinçli ve güvenli bir şekilde davranmalarını sağlamak adına önemlidir.

Anahtar Sözcükler: Z Kuşağı, Siber Güvenlik Farkındalığı, Demografik Özellikler

4.2.4. Elfadil ORSAD[9]: *The Changing Architecture of Security: The Role of Cyber Security and Artificial Intelligence*

As global security threats evolve, the architecture of security is shifting to address the complexities of modern digital landscapes. This research explores how cyber security and artificial intelligence (AI) are becoming integral to reshaping security frameworks and policies worldwide. With cyber-attacks becoming more sophisticated, state and non-state actors increasingly exploit vulnerabilities in critical infrastructure, economic systems, and communication networks. Cyber security has emerged as a key pillar in national defense, requiring continuous innovation in detection, response, and prevention mechanisms.

Artificial intelligence plays a pivotal role in enhancing cyber security by automating threat detection, identifying patterns in vast amounts of data, and predicting potential attacks before they occur. AI-driven solutions such as machine learning models, neural networks, and natural language processing can rapidly assess and counteract threats, reducing human error and reaction times. However, the increasing use of AI also introduces new challenges, including ethical concerns, biases in AI decision-making, and the potential for AI-driven cyber-attacks.

This paper examines the convergence of cyber security and artificial intelligence in the context of a changing security architecture. It discusses how governments and organizations must adapt to these

[9] Independent Researcher, Egypt, E-Mail: elfadilelfatih2024@gmail.com

technologies, balancing innovation with regulation to safeguard both national security and individual privacy. As the architecture of security evolves, the role of AI in cyber defense strategies will continue to grow, shaping the future of security in the digital age.

Keywords: Cyber Security, Artificial Intelligence

4.2.5. Chenghao Sun[10] & Xueyu Zhang[11]: *From Risk to Opportunity: Addressing National Security Challenges of Open-Source AI*

In recent years, open-source artificial intelligence (AI) has made remarkable strides in closing the performance gap with closed-source models (Seger, E., Dreksler, N., Moulange, R., Dardaman, E., Schuett, J., Wei, K., ... & Gupta, A., 2023). Current predictions suggest that the capabilities of open-source AI are rapidly approaching those of large, proprietary models. Some open-source models, such as the Llama model (Seger, E., Dreksler, N., Moulange, R., Dardaman, E., Schuett, J., Wei, K., ... & Gupta, A., 2023), have already surpassed closed-source models in terms of performance and computational capacity. This shift is driven by the openness, adaptability, and regulatory transparency of open-source AI, which has gained significant attention due to its lower entry costs, flexibility in adapting to diverse scenarios, and democratized nature. The decentralized nature of open-source models empowers a broader range of developers, allowing for innovation outside the control of single large corporations or nations (Eiras, F., Petrov, A., Vidgen, B., de Witt, C. S., Pizzati, F., Elkins, K., ... & Foerster, J. , 2024). As a result, open-source models are not only becoming tools for enhancing individual productivity but are also pivotal in promoting technological innovation across various industries. Despite these advantages, open-source AI presents a host of challenges, particularly in terms of national security. The risks associated with open-source AI can be broadly categorized into technological risks, regulatory risks, and the potential for malicious use.

Technologically, open-source models are more prone to vulnerabilities and algorithmic biases (Desouza, K. C., Dawson, G. S., & Chenok, D., 2020). Due to lower development investments and the involvement of "unprofessional developers" at later stages, these models are more susceptible to technical flaws compared to their closed-source counterparts. Furthermore, the absence of robust regulatory oversight makes it more difficult to address these flaws and the ethical risks associated with algorithmic bias. Even as closed-source models face issues related to discrimination and fairness, open-source models are at an even greater risk of encountering such problems.

Regulatory risks stem from the nature of open-source models, which, once distributed, are difficult to retract or regulate. While many open-source models include access licenses in their code (Neumann, T.,

[10] Center for International Security and Strategy, Tsinghua University, Beijing, China, E-Mail: sch0625@gmail.com & sunchenghao@tsinghua.edu.cn

[11] Center for Area Studies of Nankai University's College of Foreign Languages, Tianjin, China.

& Jones, B. , 2024), the decentralized, peer-driven nature of open-source communities often results in a lack of effective enforcement (Qi, X., Zeng, Y., Xie, T., Chen, P. Y., Jia, R., Mittal, P., & Henderson, P. , 2023). With low barriers to entry, open-source models may attract countless downstream developers who are often reluctant to regulate these models, especially since they do not generate direct profit. This self-regulating approach (Neumann, T., & Jones, B., 2024) leaves many open-source models unmonitored, making it challenging to ensure compliance with standards or to mitigate potential risks effectively.

The combination of these technological and regulatory vulnerabilities makes open-source AI models highly susceptible to malicious use. These models could be exploited by terrorists, transnational criminal organizations, or rogue states to launch cyberattacks, spread propaganda, or even develop biotechnologies and weapons. The potential for such uses poses a significant threat to national security, as open-source AI models can be easily accessed, modified, and deployed with little oversight.

Regarding the overall effectiveness of AI governance, if the international community cannot effectively regulate open-source AI models, there is a high risk of current AI governance frameworks developing significant gaps. First, the capabilities of open-source AI models have gradually approached those of closed-source models, showcasing immense application potential (Goldstein, J. A., Chao, J., Grossman, S., Stamos, A., & Tomz, M. , 2024). Second, there is widespread recognition of the significant potential of AI technology in society, with potential users increasingly enhancing their development and application capabilities based on open-source models. Consequently, if the international community fails to effectively regulate open-source AI, countries may face security risks such as the leakage of confidential data and personal privacy, cyberattacks, and the proliferation of lethal autonomous weapons.

Given that the failure of open-source AI model regulation may lead to or exacerbate national security risks, the international community must reassess the technological characteristics of open-source AI and explore avenues for collaboration. Referring to the possibility of international cooperation on open-source AI models, this paper argues that certain attributes of open-source AI facilitate inter-state cooperation, while the high regulatory costs and lack of effective incentives require capable nations to work together.

Existing research indicates that the dual-use nature of AI technologies makes it difficult for nations to determine the ultimate purpose of another country's acquisition of these technologies (Schmid, S., Riebe, T., & Reuter, C. , 2022). In this context, the transparency of regulation in open-source AI plays a crucial role in bridging the trust gap created by dual-use technologies. The openness and accessibility of open-source AI inherently provide more opportunities for transparency in its development and deployment, offering a mechanism for international monitoring and regulation.

Artificial intelligence has already become deeply integrated into national defense infrastructures (JR., 2024), with countries such as the US and the UK actively establishing national AI security research institutes. Meanwhile, the increasing military integration (JR., 2024) of AI means that the leakage of related technologies and algorithms could result in far more than just commercial losses; it could lead to significant national security vulnerabilities. Since nations typically do not employ open-source AI models for critical strategic or defense purposes, this alleviates concerns about the proliferation of core technologies.

A key factor hindering international cooperation in AI governance is the mutual distrust between nations (Wang, Y., & Chen, D. , 2018). Taking China-U.S. AI technology collaboration as an example, while dialogues on AI between the two countries continue, many U.S. official documents regard China, which possesses AI technology, as a threat, asserting that the U.S. must maintain a technological edge over China to safeguard national security (Selva, 2018). This perception of the nation itself as a threat obstructs the orderly development of essential technological cooperation between countries. Regarding open-source AI technologies, currently, few state actors have integrated them into defense or military industries. However, due to their relative accessibility and development flexibility, open-source AI technologies are more likely to be acquired by non-state actors, who may engage in criminal activities or actions that endanger national security and public safety. As countries collectively face the security risks posed by the malicious use of open-source AI by “non-state actors”, they are also more likely to avoid perceiving each other as risks in governance discussions.

Finally, relevant nations can enhance mutual trust and promote cooperation in closed-source AI governance by taking the lead in regulatory and application collaborations within the open-source AI field. Collaborative efforts in open-source AI can serve as a foundation for broader partnerships, demonstrating the potential for international cooperation in addressing global challenges such as cybersecurity, ethical AI, and public safety. Additionally, by fostering joint research and development initiatives, nations can identify common goals and align their efforts, ultimately facilitating smoother transitions to cooperative models in more sensitive areas of AI governance, including closed-source technologies. This approach not only strengthens international relations but also ensures that the development of AI benefits society as a whole while minimizing risks to national security and global stability.

Given risks of open-source AI models, the international community faces an urgent need to reassess its approach to open-source AI governance. The failure to regulate these models could create significant gaps in current AI governance frameworks, further exacerbating national security risks. Fortunately, the attributes of open-source AI models showcase positive impacts on international cooperations on AI governance and risks managements. By fostering cooperation among nations and stakeholders, it is possible to mitigate the risks associated with open-source AI and harness its potential for positive socio-

economic development while safeguarding national and global security. Moreover, relevant nations can enhance mutual trust and promote cooperation in closed-source AI governance by taking the lead in regulatory and application collaborations within the open-source AI field.

Keywords: Open-Source AI, National Security, Technological Risks, Regulatory Risks, Potential for Malicious Use

4.2.6. Sumanta BHATTACHARYA[12] & Bhavneet KAUR[13]: *Regulatory Framework and Policy Implications for Implementation of AI and ML for Upgrading Economic Sector in Banking and Trade Sectors*

The implementation of Artificial Intelligence (AI) and Machine Learning (ML) in the field of banking and trade has been known to provide possibilities aimed at strengthening economical frameworks and improve various choices. The purpose of this paper will be to consider whether there is an appropriate legal and policy landscape for AI and ML to be adopted in these vital economic sections.

Implementation of AI and ML in banking and finance boosts fraud detection, risk control, customer support through chatbots, and product differentiation, and ML expected value, trading, and large data analysis. Nevertheless, the fast-growing AI and ML applications introduce a number of issues that can only be solved through appropriate legal regulation. Some of the challenges are as follows: How to achieve data privacy and security, how to explain the workings of an algorithm, conflict of ethics, issues regarding bias in the decision-making process and how to appraise the errors made by the model.

According to the policy implication, the government and regulatory authorities should set the rules on AI transparency and data protection and regulation of applications that use AI to be fair and bias free. Remarkably, today there is no significant legal regulation of AI management, financial reporting, and security in both banking and trade. It has to promote innovation at the same time it has protective measures against abuse, hacking and other malicious activities, and system failure that may prevail out of artificial intelligence in the financial sector.

It should also be noted that the existing and envisaged regulatory measures should address development of the PPPs; AI awareness; and consideration of the digital divide. Cross-border transaction, which forms a major part of the international trade, is an area where AI related advancements can be effectively implemented, provided there are unified approaches at the international level.

Therefore, it is immensely clear that the deployment of AI as well as ML in the Bank and Trade brings

[12] Dr., PhD scholar in Asian International University , and Policy Analyst, M.Tech, MA in Development Studies, M.Sc in Environmental Science , LLB, MA in Security and Defence Law, MA in Economics, MBA DIA & D & DG and GS, PGDEDS, PGDHUR, MPI (Oxford University), E-Mail: sumanta.21394@gmail.com, ORCID: 0000-0003-2563-2787

[13] Sachdev Political Science Hons (Calcutta University) MA in Development Studies, MA in Sociology, LLB, Post Graduate Diploma in Human Rights, E-Mail: bhavneet829@gmail.com, ORCID: 0000-0001-9156-0086

numerous benefits to the growth of the economy. But to do this effectively and sustainably, to avoid abuse of created opportunities and prevent the formation of monopolies or concentrated control over vital economic sectors and processes, a balanced regulation approach is required.

Keywords: Economical Frameworks, AI Transparency, Balanced Regulation Approach

4.2.7. Orçun OLTULU[14]: *Askerî Tam Otonom Silahlarda Orantılılık ve Ayrım Gözetme Sorunu: Silahlı Çatışma Hukuku Bağlamında Bir İnceleme*

Bu çalışmanın temel araştırma sorusu; savaş alanlarının yeni aktörleri konumunda olan "askerî tam otonom silahlara" ilişkin potansiyel risk ve sorunlardan olan orantılılık ve ayrım gözetmenin, uluslararası silahlı çatışma hukuku nazarında karşılığının olup olmadığı ve bu sorunlarla başa çıkma stratejilerinin neler olabileceğidir. Yaşadığımız yüzyılda bilgi teknolojisinde meydana gelen devrim niteliğindeki gelişmeler, askerî teknolojilerin de gelişmesini tetiklemiştir. Böylece devletlerin ordularında, güvenlik ve savunma sistemlerinde; bilim insanları, mühendisler, üniversiteler ve özel şirketlerle yapılan iş birlikleriyle birçok gelişme yaşanmış ve savaşların niteliği değişmiştir. Bu bağlamda askerî tam otonom silahların, teknolojinin savaşlar açısından yarattığı dönüşümün en son halkası olduğunu söylemek mümkündür. Askerî tam otonom silahlar, gelişmiş sensör teknolojilerine sahiptir. Yapay zekâ algoritmaları sayesinde bir karar anında, o karara etki eden parametreleri göz önünde bulundurarak kendi kararını alıp uygulayabilmektedir. Veri setlerini ya da simülasyon ortamlarını baz alarak zaman içerisinde ideal davranışları öğrenip bu bağlamdaki yetkinliklerini artırma potansiyeline sahiptir. İnsan müdahalesi olmaksızın tamamen kendi başlarına sez-karar ver-uygula şeklindeki döngüyü gerçekleştirebilen ve insanla iletişim kurmaya ihtiyaç duymayan sistemlerdir (Scharre, 2020).

NATO Bilim ve Teknoloji Örgütünün (STO) "Bilim ve Teknoloji Eğilimleri 2020-2040" raporunda, askerî otonom sistemlerin gelecekte şu konularda değişiklik yaratacağı ifade edilmiştir: 1. Güç Yapısı; 2. Etkililik; 3. Karşı Önlemler; 4. Oğullaşma (Swarming); 5. Lojistik; 6. Durumsal farkındalık; 7. Ölümcüllük; 8. Manevra Kabiliyeti; 9. Hayatta Kalma; 10. Sürdürülebilirlik; 11. Kentsel Operasyonlar; 12. Siber Görevler (NATO, 2020). Aynı rapora göre, askerî tam otonom sistemlere ilişin "özerklik"; bir sistemin bilgiyi kendisine ve duruma ilişkin bağlamsal anlayışa yönelik hedeflere ulaşmak için farklı eylem planları arasından bağımsız bir şekilde oluşturup seçerek, bu bilgiyle belirsiz durumlara yanıt verme yeteneğidir. Askerî tam otonom silahlara ilişkin tartışma başlatan kavram da "özerklik" olmuştur. Konunun uzmanı bilim insanları tarafından öne sürülen çekincelerin ve çeşitli sivil toplum örgütleri tarafından yürütülen kampanyaların ana temaları, 1. Askerî tam otonom silahların küresel silahlanma yarışını öncü devletler lehine adaletsiz şekilde daha da arttıracağı; 2. Algoritmik ayrımcılık; 3. Orantılılık

[14] Av., Doktora Öğrencisi, Hacettepe Üniversitesi, E-Posta: avukatorcunoltulu@gmail.com, ORCID: 0000-0003-1353-8451

ve ayrım gözetme, şeklindedir.

Hukuki anlamda orantılılık, araçlar ve amaçlar arasında kurulan makul ilişkiyi ifade etmektedir. Buna bağlı olarak silahlı çatışma hukuku açısından ifade ettiği anlam, "elde edilmek istenen avantaj ile üçüncü taraflara verilebilecek zararlar arasındaki ilişki" şeklindedir. Orantılılıktan sonra ayrım gözetmeye bakıldığında, ayrım gözetmenin temel amacı; silahlı çatışma taraflarının birbirlerine yönelik gerçekleştirdikleri saldırılarda saldırı kapsamını muhariplerle sınırlı tutarak sivil ve savaşan ayrımı yapmaları ve böylece saldırıları yalnızca meşru hedeflere yöneltmektir (Gül, 2021). Paul Scharre'a göre, otonom silahların ayırt etme ilkesi kapsamında doğru şekilde sivil-askerî hedef ayrımı yapabilmesi önemli bir konudur. Bu doğrultuda, sistemler geliştirilirken hedef tanımanın yanı sıra yanıltıcı cisimlerin yani ortamdaki parazitlerin de ayırt edilebilmesine yönelik çalışmalar yapılması gereklidir. Otonom silahlar açısından orantılılık ilkesi ayırt etmeye kıyasla daha zorlu bir konu olup ayırt etme ilkesi konusuna çözüm bulunabilmesi muhtemel görünmektedir. Ancak hukukçular Kenneth Anderson, Daniel Reisner ve Matthew Waxman'ın da ifade ettiği üzere, orantılılık ilkesinin sınırları açısından kesin kabul görmüş bir formül henüz bulunmamaktadır (Scharre, 2020).

Askerî otonom silahların uluslararası savaş hukukunda açık şekilde düzenlenmesine ve hatta yasaklanmasına yönelik etkili bir adım olarak kabul edilebilecek "Otonom Silah Sistemlerine İlişkin 12 Eylül 2018 tarihli Avrupa Parlamentosu Kararı" vardır. Bu kararda vurgulanan temel hususlar şunlardır: Ölümcül otonom silah sistemlerinin benzeri görülmemiş ve kontrolsüz bir silahlanma yarışını tetikleyerek savaşı temelden değiştirme potansiyeline sahip olmuştur; ölümcül otonom silah sistemlerinin kullanımı, özellikle hedef seçimi ve müdahale gibi kritik işlevlerle ilgili olarak insan kontrolüne ilişkin temel etik ve hukuki soruları öne çıkarmıştır; makineler ve robotlar ayrım, orantılılık ve ihtiyat gibi hukuki ilkeleri içeren insan benzeri kararlar alamamaktadır; ölümcül otonom silah sistemlerinin kullanımı uluslararası insan hakları hukuku, uluslararası insancıl hukuk ve Avrupa normları ve değerlerinin gelecekteki askerî eylemlerle ilgili olarak uygulanmasına ilişkin temel soruları gündeme getirmiştir; herhangi bir ölümcül otonom silah sistemi, kötü yazılmış kod veya düşman bir devlet veya devlet dışı bir aktör tarafından gerçekleştirilen bir siber saldırı nedeniyle arızalanabilecektir; Avrupa Parlamentosu, ölümcül otonom silah sistemleri konusunda acilen ortak bir tutumun geliştirmeli ve benimsemelidir; anlamlı insan kontrolü olmadan saldırıların gerçekleştirilmesine olanak tanıyan ölümcül otonom silah sistemlerinin geliştirilmesi, üretimi ve kullanımının uluslararası olarak yasaklanması yönünde defalarca çağrıda bulunulduğu dikkate alınmalı ve bunların yasaklanmasına yönelik etkili müzakereler başlatılmalı (European Parliament, 2018). Konuyla bağlantılı olan ve geçmişte düzenlenmiş uluslararası hukuki metinlerden 24 Nisan 1863 tarihli "Lieber Talimatları", 9 Eylül 1880 tarihli "Oxford Kılavuzu", Aralık 1922-Şubat 1923 tarihleri arasında Lahey'de hukukçular komisyonu tarafından hazırlanan "Savaş ve Hava Harbi Zamanında Telsiz Telgrafın Kontrolüne İlişkin Kurallar", 1956 tarihli "Savaş Zamanında Sivil Nüfusun Maruz Kaldığı Tehlikelerin Sınırlandırılmasına

İlişkin Taslak Kurallar", 8 Haziran 1977 tarihli "12 Ağustos 1949 tarihli Cenevre Sözleşmelerine Ek ve Uluslararası Silahlı Çatışma Mağdurlarının Korunmasına İlişkin Protokol (Protokol I)", otonom silahlara ilişkin yapılan çeşitli uluslararası oturumlar, görüşmeler, konuya ilişkin ülke açıklamaları, yasaklama ve sınırlamaya ilişkin girişimler bir bütün olarak değerlendirildiğinde, orantılılık ve ayrım gözetme şeklindeki olası sorunların uluslararası silahlı çatışma hukukunda kendine yer bulması kısa vadede pek mümkün gözükmemektedir. Çalışmada literatür analizi, belge ve arşiv taraması yöntemleriyle toplanan veriler analiz edilerek bu sonuca ulaşılmıştır. Amaç, konuya teknoloji ve hukuk penceresinden çoklu bakış açısıyla yaklaşarak hem farkındalık yaratmak hem de yeni bir akademik tartışma alanı oluşturmaktır. Bu doğrultuda konunun teknolojik boyutuna ilişkin açıklamalar yapılırken çeşitli teknik raporlardan, yapay zekâ uzmanlarının ve otonom sistemlere ilişkin öncü bilim insanlarının görüşlerinden ve güncel dünya istatistiklerden yararlanılmıştır. Konunun hukuki boyutuna ilişkin olarak ise, hukuk metinlerden ve haber kaynaklarından yararlanılmıştır.

Anahtar Sözcükler: Askerî Otonom Silahlar, Orantılılık, Ayrım Gözetme, Silahlı Çatışma Hukuku

4.2.8. Giovanni ERCOLANI[15]: *The Emergence of Paranoid Security*

The main point of this study is to submit my concept of 'paranoid security' for an academic debate. My theory is that the zeitgeist (spirit of the time) of the historical period in which we live is characterized by paranoid security, which (1) is an autotrophic security system that feeds itself with the suspicion it produces; and (2) is a self-sustaining system in which security knowledge is fabricated (paranoization process) on the 'suspicion' of existential threat-insecurity, therefore producing paranoia security knowledge.

Some premises are necessary to structure my thesis. First, my idea of the emergence of Paranoid Security is framed between two concepts: (1) 'a theory is always for someone and some purpose' (Cox, 1981: 128); and (2) 'ordinary people are always taken in by appearances and by the outcome of an event'. And in the world, there are only ordinary people; the few have no place, while the many have a spot on which to lean (Machiavelli [1532] 2019: 126-128). Second, my position on this matter is extremely realistic, cynical, and provocative, is based on my academic and professional experiences, and it is expressed in the following points: (1) when we talk about 'politics' we talk about 'power', and in politics, there is not morality; (2) those in power (the legitimate Power-Knowledge-Language-Meaning-Security Structure [PKLMS]; the 'contemporary' Prince) want to keep and protect their power, and the 'others' want to conquer it; (3) I define the post-Athenians 'demo-cracy' as 'vulgo-cracy' (vulgo: the common ordinary people, the masses); (4) in 'vulgo-cracy' to conquer power or to maintain power the political leader must

[15] Dr., FRAI, University of Murcia, E-Mail: giovanni.ercolani@um.es, ORCID ID: 0000-0002-5099-5435

conquer the vulgo; and (5) how to conquer the vulgo? By appearing, by manipulating primordial fear (death); playing the emotional card; making use of propaganda-narrative; maintaining a constant paranoia.

When talking about paranoia I want to clarify that the term (1) comes from the Greek 'para-', 'beyond, irregular', and 'noos', 'mind'; (2) it is an irregularity of the mind, a mental disorder that distorts a person's perception of what is real; (3) is an instinct or thought process that is believed to be heavily influenced by anxiety, suspicion, or fear, often to the point of delusion and irrationality; and (4) paranoid thinking typically includes persecutory beliefs or beliefs of conspiracy concerning a perceived threat towards oneself.

The fact that I merged paranoia with security and securitization, is based on the work of Luigi Zoja's 'Paranoia – The Madness that Makes History' (2017). In his work, Zoja presents an insightful analysis of the use and misuse of paranoia throughout history and in contemporary society. Zoja combines history with depth psychology, contemporary politics, and tragic literature, resulting in a clear and balanced analysis presented with rare clarity. The devastating impact of paranoia on societies is explored in detail. Focusing on the contagious aspects of paranoia and its infectious, self-replicating dynamics, Zoja takes such diverse examples as Ajax and George W. Bush, Cain and the American Holocaust, Hitler, Stalin, and Othello to illustrate his argument. He reconstructs the emblematic arguments that paranoia has promoted in Western history and examines how the power of the modern media and mass communication has affected how it spreads. 'Paranoia' clearly examines how leaders lose control of their influence, how the collective unconscious acquires an autonomous life, and how seductive its effects can be – more so than any political, religious, or ideological discourse.

Once paranoia is employed in a security discourse-policy it evolves into a collective paranoia and it acquires the following features which defines the paranoization process: evolves into a psychic infection characterized by a relativization of truth; is based on constant suspicion which is fed by rumors in which the 'suspect' is already presented as 'guilty' and like the 'enemy-insecurity threat' is portrayed as inhuman and immoral; it is the main essence of post-truth politics (post-factual politics, post-reality politics). The leitmotiv of paranoia politics is 'the suspicion of.....the suspect is guilty'. The fact that the PKLMS structure has a suspect on something/someone already makes it guilty.

More importantly, though, is that this 'paranoid security' becomes the officially-authorized description of the world that frames human existence.

There is a strong relation between narrative and 'reality': for Galimberti (2011) humankind has never lived in the World, but always in its description which, in different historical periods, has been provided by religion, philosophy, science, and now technology. Humankind lives into the description-narrative of the world, and his relationship with it passes through the ideas that wrap the things: These descriptions-

narratives participate in the construction of the social reality (Searle, 1996) and the symbolic universe (Berger & Luckmann, 1991) in which humankind lives his existence; and description-narrative shapes the identity and the living space-place of the individual.

Therefore, in my approach, I follow Zoja (2017), who argues that the relationship between communication and paranoia has to be analyzed in order to prevent the dangers of a world driven by paranoia.

To sustain my theory, I take into consideration two very recent historical events in which the 'western-NATO-financial world-system' has experienced two different security threats: COVID-19 and the Russia-Ukraine War. Both of these existential threats have been accompanied by specific measures and protocols of action in which official narrative has constituted the structures of their own security-insecurity architecture. Security is a myth, and its architecture is primarily based on narrative (signifier; securitization process-security knowledge) which makes that security is a sacred text. The 'COVID-security narrative-protocol of action' had to deal with a 'critical security threat', whilst the 'RUSSIA-UKRAINE-security narrative-protocol of action' is still facing a more classical security threat framed inside a 'strategic studies approach' with global repercussion which unfortunately escaped from the 'mind' of the 'scientific experts/astrologists'.

However, what both security-insecurity events have in common is the fabrication of a 'paranoia broadcasting' in which narrative-language has replaced the search for truth. The securitization process which has been elevated in both cases to the official and authorized narrative-truth has been assembled following a formula in which the reader writes the book: according to the theory of textual cooperation there is a strong relation between a text and its specific reader (model reader) in which one contributes to the construction of the other.

In a post-Athenians democracy (vulgo-cracy; common people-cracy) the security-insecurity text has been produced to be fully understood and digested by the common people (impact in the democratic elections) and its language, like the Orwellian Ing-Soc of '1984', has been reduced and simplified to cancel and prevent misleading and personal interpretations. Meaning and interpretation are monopolies of the PKLMS structure.

Honestly, can we say that at the moment we know the truth about the COVID pandemic and its vaccines, and can we say the same about the Russia-Ukraine war? Do we really believe in anything that the official authorities have said and imposed on our societies about these two security events?

Already, both official-scientific-authorized narratives sustaining both paranoid security events are showing cracks in their monolithic edifice.

If we are not in a position to answer the above questions, and if we really retain some doubts, at least we are aware that behind these two different events, there is a struggle for power and money.

Therefore, this paranoia: (1) represents the new architecture of the security environment in which NATO countries experience their lives; (2) has replaced the 'security knowledge' in the sense that now security knowledge-securitization is paranoia; (3) has been imposed through a state of emergency in which even our daily life is under scrutiny; (4) it has been elevated to a cultural-moral-educational system and an ideology; and (5) has created a paranoid individual.

If we are interested to produce serious security knowledge (truth) we should approach the paranoid security narrative as a performative text (or even an agenda) in which the 'Emperor' is naked and ask ourselves: why all this silence around the events, and who profits from that silence (cui prodest)?

Is only by deconstructing the silence around the paranoia and the security knowledge (Ercolani, 2021) that we can start to doubt the veracity of the text-truth and develop a sane doubt inspired by the search for knowledge and not doxa and propaganda.

Veritas-truth and justitia-justice are tied together, and a return to a Socratic questioning in facing the 'paranoid security' is the methodology suggested in my study, because here the first and real victim of this politics is the very doubt that has always fueled the search for truth.

Keywords: Paranoid Security, Securitization, NATO, COVID-19, Russia-Ukraine War

4.2.9. Can DEMİR[16]: *NATO Doctrine of Information Operations and Key Takeaways for the Modus Operandi*

The security architecture of the international arena involves a continuum of competition comprising the relationships of cooperation, rivalry, confrontation and armed conflict (NATO, 2022b: 5-7). NATO plans and conducts activities to fulfill the three core tasks of defence and deterrence, crisis prevention and management and cooperative security (NATO, 2022a) in this full range of the continuum of competition.

NATO conducts a wide variety of operations and missions (NATO, 2019: 1-27,1-34), and Information Operations within the mindset of Strategic Communications are inherent in all these types of NATO activities. NATO's strategic communication is a two-pillar structure. The pillar of communication capabilities comprises subfields of psychological operations (PsyOps) and military public affairs (MilPA) (NATO, 2023a: 17), while the pillar of information capabilities comprises information activities and information operations (InfoOps) (NATO, 2023: 47). NATO's strategic communications mindset provides direct guidance to all PsyOps activities, MilPA activities, information operations and

[16] PhD Student, Turkish National Defense University Atatürk Strategic Studies and Graduate Institute, E-Mail: can.demir@msu.edu.tr, ORCID: 0000-0002-8338-2897

information activities as well as it provides guidance to all NATO military activities to ensure that they support NATO's narratives and messages (NATO, 2023b: 12).

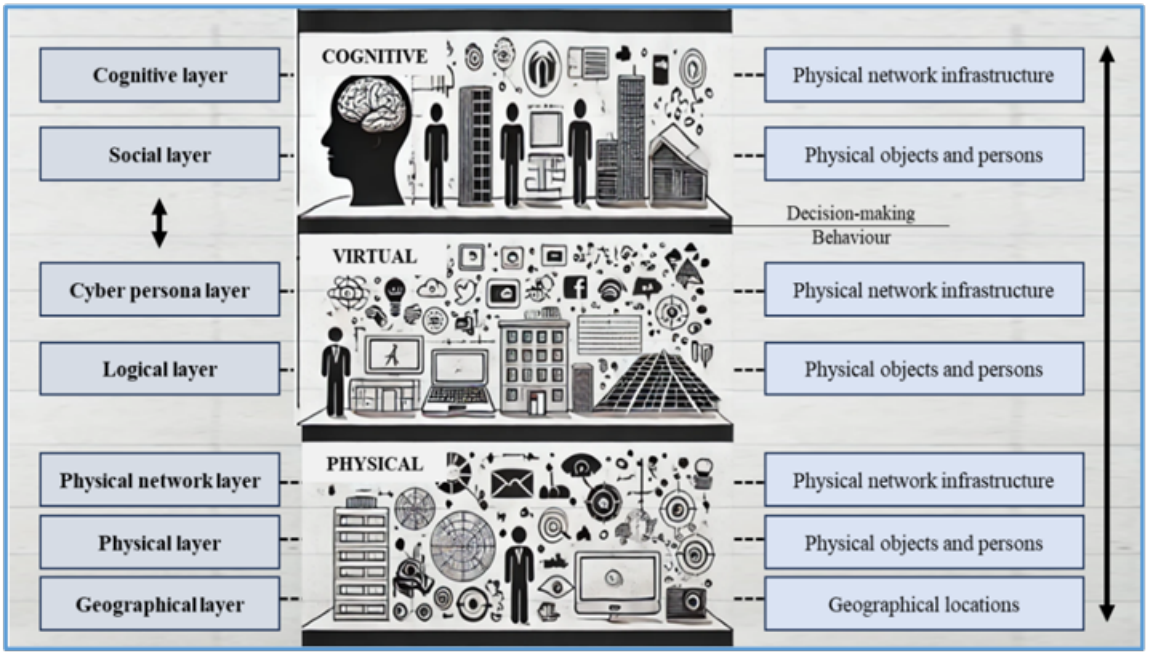
"Information Activities" is defined as "all kinds of military activities focused on creating cognitive effects", while "Information Operations" is defined as "a staff function to analyze, plan, assess and integrate information activities to create desired effects on the adversaries, potential adversaries and audiences in support of mission objectives" (NATO, 2023a: 14-15). Military kinetic actions like air raids, patrols, airborne operations and non-kinetic actions such as key leader engagements, for instance, all have cognitive effects on the adversary as individual information activities. When these activities and all other military activities dedicated to the creation of cognitive effects are analyzed, planned, integrated and assessed by a dedicated staff, they evolve into information operations. The way that NATO manages the whole system of information operations provides useful tips and guidelines for security mechanisms and organizations that have roles in information operations.

All kinds of information activities and information operations take place in the information environment. The information environment is a combination of all informational entities, agents, services and properties, processes, relations and interactions. This environment is very dynamic, undergoing changes with political and social circumstances as well as technological innovation (Röttger&Vedres, 2020, pp.2-3). In the realms of defense and security, the information environment, central in warfare and short of it in one aspect, is the entirety of systems, organizations and individuals that realize processes related to information (RAND Corporation, 2021: 1).

NATO defines the information environment as "the environment comprising information, individuals, organizations and systems that receive, process and convey the information, and the cognitive, virtual and physical space in which this occurs" (NATO, 2023a: 15). In the information environment, different layers relate to cognitive, virtual and physical effect dimensions. NATO has a behaviour-centric approach and uses these effect dimensions to provide a framework for comprehending the measurement, purpose, and consequence of military activities.

Figure 1

The Outline of the Information Environment



(NATO, 2023a, p.38)

A comprehensive information environment assessment (IEA) is a prerequisite to all strategic communications activities and information operations in particular. The assessment is a continuous process, and the level of comprehensiveness depends on the time and resources allocated to the process. Figure 2 (NATO, 2023a: 41) shows a clear picture of the IEA methodology applied in NATO doctrine.

Figure 2

The Information Environment Assessment Methodology in NATO Doctrine

Information Environment Analysis					Assessment
Baseline analysis	Human factor analysis	Communication analysis	Audience analysis	Behaviour analysis	Cognitive assessment
Country briefs	Cultural and social analysis	Narrative analysis	Orientation and link analysis	Cognitive effect analysis	Monitors and warning
Framework briefs	Institution analysis	Hostile communications analysis	Audience segmentation	Capability, opportunity, motivation and behaviour analysis	Behaviour driver assessment
Historical analysis	Gender analysis				
Cultural and social baseline	Information systems analysis	Own communications analysis	Cognitive effect determination		Assessment and evaluation criteria
Behaviour baseline	Physical terrain analysis	Earned communications	Potential target audiences	Monitors and warning	

The “baseline analysis” is the foundation for a comprehensive understanding of the environment. It is followed by the “human factors analysis”. For this, several templates can be applicable, but the PMESII/ASCOPE matrix outlined in Table-2 provides a more comprehensive analysis.

Table 1

PMESII / ASCOPE Analysis Matrix

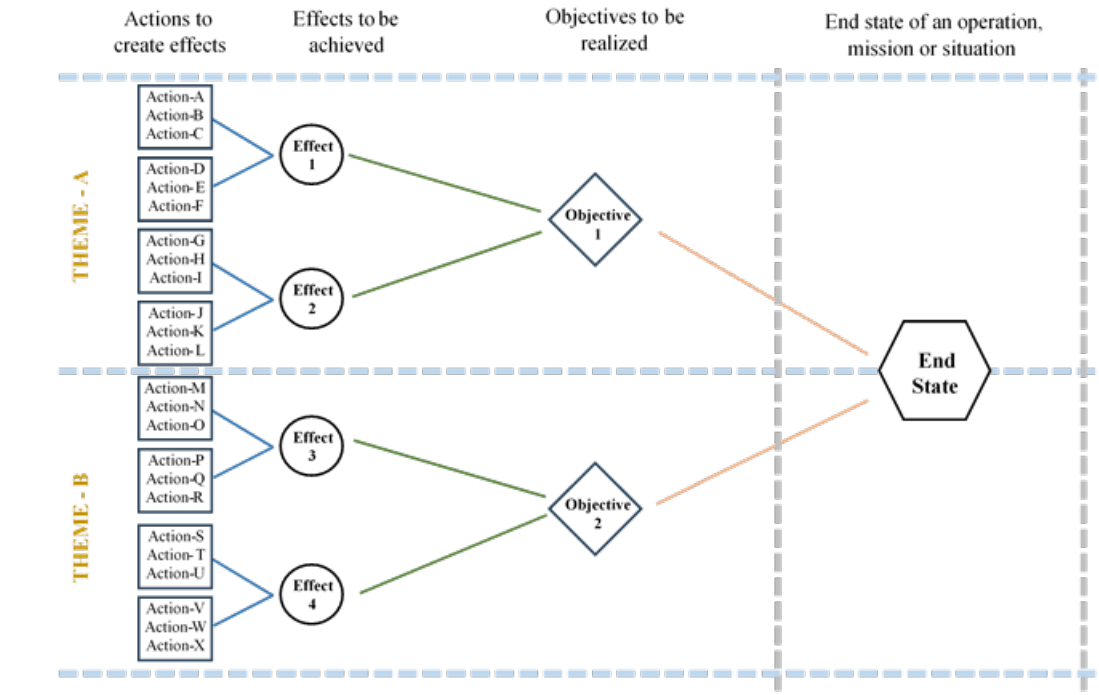
PMESII / ASCOPE	Political	Military/ security	Economic	Social	Infrastructure	Information
Area	*Regions, boundaries, etc.*	*Operation areas, security regions etc.*	*Agriculture, industry, waters etc.*	*Religious or ethnic boundaries etc.*	*Air, rail, water and road networks etc.*	*Coverage for media types etc.*
Structures	*Governance centers etc.*	*Police stations, military bases etc.*	*Industrial zones, economic centres etc.*	*Facilities, religious places etc.*	*Hospitals, power plants etc.*	*Comms and media structures etc.*
Capability	*Governance, political system etc.*	*Combat power, law enforcement bodies etc.*	*Finance markets, industrial etc.*	*Education levels, basic services etc.*	*Basic services and their effectiveness etc.*	*Data coverage, literacy, censorship etc.*
Organization	*Government, political parties etc.*	*Law enforcement, military, etc.*	*Businesses, companies, centers etc.*	*Religious, ethnic, charity groups etc.*	*Governance facilities, NGO facilities etc.*	*Organizations, media providers, etc.*
People	*Political/local, diplomatic leaders etc.*	*Military or security leadership etc.*	*Governance leaders, elites, etc.*	*Religious/ ethnic leaders, influencers etc.*	*Investors, contractors, NGOs etc.*	*Media influencers, journalists etc.*
Events	*National and local elections, Campaigns etc.*	*Wars, combats, operations, parades etc.*	*Market days, business holidays etc.*	*Religious or national events etc.*	*Investments, opening ceremonies etc.*	*Media campaigns, propaganda etc.*

“Communication analysis” comprises a detailed analysis of all narratives and communications by all parties of the information environment. This is followed by the “audience analysis” and “behaviour analysis”. Under these two components, analyses related to cognitive effects go through the brainstorming format of “social, technological, environmental, military, political, legal, economic and security” (STEMPLES) within which cognitive objectives are set and then later put to a “Criticality, Accessibility, Recoverability, Vulnerability, Effect, Recognisability” (CARVER) analysis. Capability, opportunity, motivation and behaviour (COM-B) model is also an integral part of the final step of the analysis. All analysis steps culminate in a detailed assessment of the information environment (NATO, 2023a: 40-52).

Coordination, harmonization, synchronization and alignment are integral aspects of NATO information operations activities. NATO uses specific tools to coordinate, harmonize and synchronize information activities. InfoOps activities at the military strategic level, operational level and tactical level are aligned wih each other through the utilization of specific documents which provide directions and guidance. Through these processes, actions which are considered to be information operations activities create specific effects which support the objectives and end state of an operation, mission or situation as illustrated in the information operations design provided in Figure 3.

Figure 3

A Generic Information Operations Design



Note. The design is produced by the author.

Information Operations is an indispensable aspect of current NATO missions and operations as well as the advanced planning for potential future conflicts. It is essential to recognize that all actions undertaken during military or security campaigns inherently convey strategic communications messages, thereby qualifying them as information activities. However, it is only through the analysis, planning, integration, and assessment of these activities that they evolve into true Information Operations. Information environment is unique for each mission or operation and a comprehensive information environment assessment is a prerequisite for successful information operations. For effective information operations, higher authorities are to release clear directions and guidance through framework documents to make sure that information activities are well aligned with the military strategic communications objectives and overall operational objectives, and support the end state of the subject operation or the mission. Moreover, the synchronization and orchestration of information activities at all levels is paramount to prevent redundancy and ensure that a lack of coordination does not undermine the success of the operation or mission.

Keywords: NATO, Strategic Communications, Information Operations, Information Environment, Information Environment Assessment

4.2.10. Federico PRIZZI[17]: *Key Leader Engagement, the Most Challenging Way in Warfighting to Influence Adversaries*

The aim of this study was to show what Key Leader Engagement (KLE) is and how it is related to the Information Operations and to the Strategic Communication (StratCom) in warfighting. It was also demonstrated how KLE is intended not only as a useful method to convey information to adversaries, but also to achieve military objectives that could not be accomplished with traditional combat activities. In order to operate effectively in the cognitive sphere and to influence a specific audience, it is essential that the engagement between the military Commander, that is the main negotiator, and his counterparts takes place at a strategic-operational level in the form of a Face-to-Face (F2F) conversation. Therefore, the preparation of Commanders is pivotal because they are responsible for carrying out the KLE and for the success of the influence strategies.

What KLE is

Before delving into the description of the operational characteristics of the KLE, it is necessary to clarify the terminology that is generally associated with the concept of engagement. First of all, an engagement is intended as any form of human interaction aimed at delivering influential messages in support of the overall Campaign Objectives. This means that engagements are not only carried out by commanders but also by soldiers with different ranks and roles, both at the operational and tactical level. In particular, KLEs are engagements between military leaders and the key decision-makers of approved audiences that have defined goals. Otherwise, Soldier-Level Engagements (SLEs) happen when soldiers interact with local populations on a daily basis. Consequently, SLE is likely to compromise the majority of engagements. This can occur as a Face-to-Face (F2F) encounter like, for instance, during a Market Patrol, or during scheduled meetings like the ones carried out by Civil Military Cooperation (CIMIC) operators or by Female Engagement Teams (FET). As well as the engagements organized by personnel from the logistic units with specific local or international contractors or medical visits carried out by military personnel on behalf of the local civilian population during the so called Medical Civic Action Programs (MEDCAPs).

The historical origin of the KLE and the general need to identify specific military actors to interact from the strategic to the tactical level in a specific operational context finds its contemporary origin in US-led counterinsurgency operations in Iraq and Afghanistan at the beginning of the 20th century. On that occasion, in fact, the exigency for a more active role of the commanders in knowing how to interact with the local authorities, both formal and informal, was recognized in order to reduce the causes of conflict and to allow civil society to return as quickly as possible to a situation of lasting peace.

[17] Indipendent Anthropologist, E-Mail: prizup@libero.it, ORCID: 0000-0001-7943-4570

Types of Engagements

Engagements can be of two main types: Face-to-Face or Virtual Engagement. The first is the preferred method of dialogue, because it allows participants to assess the effectiveness based on verbal, non-verbal, and paraverbal cues. Instead, Virtual Engagement is considered any engagement that can be developed through channels such as telephone, teleconference, videoconference, mail and email. The use of these means and, particularly of digital, and social media, provides opportunities but also big challenges, so much so that Virtual Engagements are generally used more to maintain active relationships with the counterpart rather than to reach lasting agreements. Moreover, engagements fall into two main categories: Deliberate and Dynamic. Deliberate, is a planned, and anticipated personal interaction designed to create a specific outcome. These engagements may be F2F interactions or interactions by other means such as telephone or video conference. Dynamic, is unanticipated, or impromptu, encounters for which neither soldiers nor leaders have conducted specific planning. Such encounters can occur frequently and in many circumstances. Soldiers' or leaders' ability to exploit them will depend heavily on training.

Engagement Team

Generally, the engagement team is composed of military and civilian personnel who must support the commander. The minimum composition includes a total of four people: the Commander as engager, the Note Taker, the Interpreter/Language Assistant and at least one Force Protection guy. To the team can then be added Subject Matter Experts (SMEs)/Advisors and also Media Operators if security and negotiating conditions allow it. Additionally, the team can use specific tools to be prepared before the meeting like the team's database, the engagement package, Post Meeting Minutes (PMM) of previous meetings.

The Engagement Planning

Planning a military operation has always been one of the most complicated aspects for a staff. Similarly, planning an engagement offers significant challenges not only for the commander but for the entire military contingent that depends on him. This is because, as anticipated at the beginning of this abstract, the KLE is planned and conducted when significant results on the battlefield cannot be achieved with traditional combat activities (i.e., kinetic ops). In order to carry out adequate planning of an engagement, you need to follow the 7 steps indicated here in the best possible way, taking into consideration that the time factor often does not allow you to delve into all the aspects as much as you would like:

1. Analysis of the objectives to be achieved with the negotiation;

2. Collection of information on the counterpart;

3. Study of the environment where the negotiation will take place;

4. Study of the environment from the point of view of the security procedures to be adopted;

5. Study of the environment from a cultural point of view;

6. Identification of possible negotiation strategies;

7. Dress Code and Weapon Code.

Why KLE is the most challenging way in warfighting to influence adversaries?

It is not easy to summarize the answer to this crucial question in a few words; however, it is possible to highlight a series of aspects that are only the result of numerous lessons identified and learned by the armed forces of different countries. Below we offer a short list of challenges:

1. The risk of physically exposing the commander (security);

2. Not all commanders have the ability to influence their counterparts (empathy);

3. There is often little time for staff and experts to prepare commanders;

4. Not all commanders appreciate being advised and prefer to handle the negotiation themselves in their own way;

5. Many commanders improvise their ability to engage and rely on their own abilities (excessive self-esteem);

6. The stay of commanders and contingents in the operational theatres is too short (6/12 months);

7. A KLE can only achieve lasting success with a long-standing relationship based on trust;

8. The nature of wars has constant changes and different operational needs, all of this can very likely frustrate the efforts made so far.

Keywords: Key Leader Engagement, Negotiation Strategies, Information Operations, Influence, Communication

4.2.11. Greg SIMONS[18]: *Security Versus Insecurity in a Transforming Global Order: The Role of the Fifth Dimension of Strategy*

The global security architecture is increasingly being thrown into upheaval and chaos as the geopolitical transformation away from the US-unipolar led Global North experiences relative decline in power and influence, and the multipolar Global South gains relative power and influence (Cooley & Nexon, 2020). As a declining global hegemony, the US and the Global North wish to retain their power and influence at the expense of the Global South and their aspirations to be subjects rather than objects of international

[18] Prof., Daffodil International University (Bangladesh), E-Mail: gregmons@yahoo.com, ORCID: 0000-0002-6111-5325

relations (Simons, 2021). US foreign and security policy is predicated upon the notion of a zero-sum game that is aimed at maintaining US global hegemony configured as a US-led unipolar order that is supported by a system of vassal and client states (Western, 2005). As Henry Kissinger once famously said, the US has no permanent enemies or permanent allies, only permanent interests.

This is predicated in the US geostrategic imperatives that were defined by Brzezinski (1997) in the Grand Chessboard – to keep client states obedient and protected, vassal states dependent and obedient, and to prevent the rise of other powers or blocs of powers that can challenge US hegemony. These behaviours are predicted by the theoretical perspective of realism in international relations (IR), which focuses upon self-interest and the accumulation of power (Flint, 2021). Even though foreign policy concerns the pursuit of self-interest through the projection of power and influence, it needs to have the façade of being more benevolent or necessary by other actors for the intended policy to be deemed as being more acceptable and therefore forestalls the accumulation of political will to work in opposition to those foreign policy actions

However, the role of constructivism in IR in its relation and interaction with realism is ignored. Constructivism concerns the creation and operationalisation of identity and culture to signal self in relation to others, but also what behaviour can be expected by the other. Foreign policy and security policy not only need to be defined and articulated, but they must also be perceived as being justified and legitimate, even if they are objectively not so (Mearsheimer & Walt, 2016). It is a question of accumulating political capital as a means towards moving foreign policy intention to foreign policy rhetoric to foreign policy action. A process that is far from being transparent and objective.

In the five dimensions of strategy (land, water, air, space and knowledge/information) (Lonsdale, 1999), the first four are tangible (physical) spaces for projecting influence and accumulating power. However, the fifth dimension (knowledge/information) is intangible (informational and cognitive) yet affects perception and actions in the other spaces. Influence and perception of audiences is influences by the three realms of the human environment – the physical realm, the information realm and the cognitive realm (Alberts et al., 2001). The physical realm is where people, places and events physically and objectively occur. The information realm is the attempt to interpret or represent actors and events occurring in the physical realm, which introduces elements of subjectivity. In the third, it is the cognitive realm which is where the world view of the individual is manufactured derived from the various information and knowledge encountered, where some new material is rejected based on existing biases and knowledge (Berniss & Arquilla, 2011). The use of information in political warfare, psyops and information warfare can be effective against an uninformed or ill-prepared audience and its objectives achieved (Chifu & Simons, 203). This often revolves around the propositional premise of getting a target audience to do something that they would not ordinarily do without manipulation, which benefits the agenda of the communicating party (Western, 2005).

Given the incomplete global transformation and the desire of the US to entrench (Dobbins et al., 2019), the role of information operations to engineer reality and consent will only increase in scale and intensity. However, measure of activity does not have to translate to measure of effect on the target. The use of the fifth dimension of strategy in the environment of 21st century international relations in the context of a transforming geopolitical order offers the incumbent hegemon the possibility to defend their position covertly and indirectly at low financial cost and less likely to trigger a long, costly and unpredictable kinetic war by subverting their opponent and to justify their policy position as well as accumulate legitimacy and political capital (Beilenson, 1972). Using information is intended to bring about desired and anticipated cognitive effects that stack advantages for the communicator in the physical realm.

A good illustration of the above theory can be found in the way the US and the Rules Based Order characterise and narrate different armed conflicts around the globe, the result is dependent on whether it involves 'worthy' or 'unworthy' victims and whether an actor involved is an 'ally' or opponent of the Global North (Zollmann, 2017). The intended effect is to obstruct the foreign policy choices to limit the success of an opponent or competitor to achieve their interests and objectives, and to increase the realisation of an ally or themselves to achieve foreign policy interests and objectives. Words are symbolic and potentially carry power through the ability to define actors and an event, which restricts other alternative definitions and an actor that is defined is more likely to be forced into a defensive and reactive posture in international relations that renders them as an object and not a subject of the environment.

Before the outbreak of a kinetic war in Ukraine in February 2022, there was (and still is) an intensive non-kinetic war of organised persuasive communication to engineer and manufacture the perception and consent of audiences by establishing an orthodoxy of knowledge (the appearance of highly debateable and politicised 'facts' and 'knowledge') (Simons, 2022). This was intended to trap Ukraine and Russia into a line of foreign policy that would most likely result in a kinetic war. A similar line of narrative of 'imminent' and 'inevitable' invasion that was applied to Russia in connection with Ukraine was also applied to China with reference to Taiwan. Another very striking feature has been the invocation of genocide against Russia's actions in Ukraine and Chinese alleged actions in Xinjiang province, which were in the form of assertions or allegations. Yet, genocide and ethnic cleansing by Israel in Gaza were denied in spite of the massive amount of social media material that demonstrates it, by video material uploaded by Israeli soldiers, mass media reporting, witness testimonies etc. Hence, the intention is to limit foreign policy choices of China and Russia through a deceptive reputational threat to deal with threats, and to free the hand of Israel to continue their illegal and unethical actions through attempts to protect their reputation and shield their actions.

Keywords: Security, Global North, Global South, Information Operations, Geopolitical Transformation, Realism, Constructivism

4.2.12. Erdal ARSLAN[19]: *Uluslararası Terörizm ile Mücadelede NATO'nun Rolü*

Giriş

NATO, ülkemizin tam yetkiyle söz sahibi olduğu önemli bir uluslararası örgüttür. Bu bakımdan NATO üyeliği Türkiye için önemlidir. Tarihin en başarılı savunma ittifakı olarak anılmaktadır. 2010 Kasım ayında gerçekleştirilen Lizbon Zirvesi'nde kabul edilen Stratejik Konsept, İttifakın kendisini günün koşullarına uyarlama yolunda yaptığı önemli bir güncelleme olarak kabul edilmektedir. Ülkemizin 1952'de üyesi olduğu NATO, uluslararası güvenlik ve savunma politikamızın temel unsuru olma özelliğini günümüzde de sürdürmektedir.

NATO üyeliğinin 72. yıl dönümünü 18 Şubat 2024 tarihinde kutlayan Türkiye, İttifakı kendisinin de ayrılmaz bir parçası olduğu Avrupa-Atlantik bölgesinin güvenliğinin dayanağı olarak görmeye devam etmektedir. Soğuk Savaş sonrası konvansiyonel tehdidin büyük ölçüde azalmasının ardından son yılarda, özellikle Rusya ile Ukrayna arasındaki savaş nedeniyle bu tehdit yeniden gündeme gelmiştir. Diğer taraftan terörizm, bölgesel istikrarsızlıklar, kitle imha silahları ve bunları fırlatma vasıtalarının yayılması; ayrılıkçı mikro ve etnik milliyetçilik, aşırı dinci akımlar, örgütlü suç, uyuşturucu ve insan ticareti, kitlesel göç gibi geleneksel olmayan, asimetrik güvenlik risk ve tehditleri ortaya çıkmıştır. Bugün, terörizm uluslararası toplum ve İttifakın güvenliği için en ciddi tehditlerden birini teşkil etmektedir.

Türkiye'nin İttifakın genişleme stratejisine bakış açısı ise, Avrupa-Atlantik alanının bütününde güvenlik ve istikrarın daha da pekişmesine katkıda bulunduğu yönündedir. Türkiye de 28-29 Haziran 2004 tarihlerinde İstanbul'da gerçekleştirilen NATO Zirvesi'nde, terörizme karşı yürütülen küresel mücadeleye müttefiklerce yapılmakta olan katkıların güçlendirilmesi için genişletilmiş bir tedbirler paketi üzerinde İttifakın diğer üyeleriyle görüş birliğine varmıştır.

Çalışmada, ilk olarak NATO'nun terörizmle ilgili çalışmaları ortaya konacak, daha sonra NATO ve terörizm ilişkisi NATO kaynaklarında terörizm tanımı çerçevesinde ele alınacak ve son olarak NATO ve terörizmle mücadele konusuna değinilecektir.

NATO'nun Terörizmle İlgili Çalışmaları

NATO'nun birimi olan Terörizme Karşı Savunma Mükemmeliyet Merkezi (Centre of Excellence Defense Against Terrorism, COE-DAT) isminden de anlaşılacağı üzere, terörizm ile ilgili çalışmalar yapmaktadır. Bu çalışmalardan bazıları şu şekildedir:

i. Terörizm ve Teknoloji (2004),

ii. Hibrit Savaşta Terörle Mücadelenin Rolü (2016),

[19] Prof. Dr., Selçuk Üniversitesi, E-Posta: erdalarslan@selcuk.edu.tr, ORCID: 0000-0003-4892-2963

iii. Terörizmde Kriz Yönetimi Seminer Raporu (2019),

iv. Terörizm Uzmanları Konferansı ve Terörizme Karşı Yönetici Düzeyinde Savunma Semineri (TEC 2020, TEC 2021),

v. Krizde SOF Rolleri/CT Yönetimi Semineri (2022).

Bu çalışmalarda terörizmin tanımı yapılmış, terörizmin çeşitleri ele alınmış, NATO'nun terörizmle mücadele yöntemlerine değinilmiş ve gelecekte karşılaşılabilecek terörizm faaliyetleri ve bunlarla mücadele yöntemleri ile ilgili öngörülerde bulunulmuştur.

NATO Kaynaklarında Terörizm Tanımı, NATO - Terörizm İlişkisi

NATO, tarih boyunca en başarılı ittifaklardan biri ve çağdaş dünyada en uzun ömürlü ittifak olarak tanımlanmaktadır. Bu ittifakın başarılı ve uzun ömürlü olması, farklı tehditlere uyum sağlama yeteneğine bağlanmaktadır. Tarihsel süreç içerisinde ortaya çıkan olaylar, NATO'nun ittifak sisteminin bozulmadan yeni ortamlara uyum sağlamasıyla sonuçlanmıştır. NATO, alaka düzeyini korumak için küresel arenadaki yeni gelişmelere uyum sağlamaya sürekli olarak çabalamaktadır. Bu bağlamda terörizm ve terörle mücadeledeki son gelişmelere göre kendi kriz yönetim sistemini uyarlamanın gerekip gerekmediğini anlamak, terörizmde kriz yönetimi yöntem ve politikalarını açıklayarak boşlukları tespit etmek ve ortak ülkeler için öneriler geliştirmek amacıyla çalışmalar yapmaktadır. Bu çalışmalar çerçevesinde NATO, devletlerin terörizme yaklaşımını bir kriz türü olarak tanımlamıştır. Bu yaklaşım, önceki deneyimleri kapsamakta ve farklı ulusların kriz yönetim yöntemlerini karşılaştırmaktadır. NATO, yaptığı çalışmalarla pratik ve teorik açıdan terörizmin son ve gelecekteki muhtemel eğilimlerini ortaya koymaya çalışmakta; hem terörizmin geleceğini tahmin etmek hem de terörizmin hangi yöne evrilebileceğini belirlemeye çalışmaktadır (Crisis Management in Terrorism: 1).

Bu çerçevede terör ve kriz birlikte ele alındığında kriz, bir terör eyleminin anıdır. Ancak teröristlerin bakış açısından, terör eylemi kriz değil; bu eylem planlı, uzun vadeli bir stratejinin sadece bir başlangıç noktası olarak değerlendirilmektedir. Terör, bir sonucun veya çıktının adı değil bir yöntemin adı olarak tanımlanmakta, rasyonel bir seçim uygulaması olarak değerlendirilmekte, terörizmi gerçekleştirenlerin bunu rasyonel bir zihinle yaptığı belirtilmektedir. Terör, belirli bir zaman ve bağlamın "zayıfları" tarafından hâkim gücü "güçlüler" arasında yeniden dağıtmak için kullanılan bir araç olarak tanımlanmaktadır. Terör saldırılarına yol açan nedenler; bireysel (kişisel, psikolojik), örgütsel (taktiksel, politik) ve farklı güdülerle bir araya gelme (din, ekonomik, milliyetçilik) şeklinde sayılabilmektedir (Crisis Management in Terrorism, s. 6-8). Terörizm ve ortaya çıkaracağı sonuçlar ile ilgili yapılması gereken; bir ulus olarak bunun farkında olmak, buna hazırlıklı olmaktır ve bu, terörü önlemenin başlangıç noktasıdır. Terörü önleme de kriz yönetiminin kritik bir parçasıdır (Crisis Management in Terrorism: 12).

NATO ve Terörizmle Mücadele

NATO Kriz Müdahale Sistemi (NATO Crisis Response System, NCRS), NATO'da kriz yönetimiyle ilgilenen kilit siyasi ve askerî aktörlerin sorumluluklarını belirlemektedir. NATO Kriz Yönetimi Stratejik Konsepti'nin (NATO Crisis Management Strategic Concept, NCMSC) temel amacı; güvenlik ortamını analiz etmek, izlemek, ilgili eylemleri ve önlemleri üstlenmek olarak ifade edilmektedir. Bu nedenle NATO'da kullanılan bir kriz tanımı: "... tarafların öncelikli değerlerine, çıkarlarına veya hedeflerine yönelik bir tehdit olan ulusal veya uluslararası bir durumdur" (Crisis Management in Terrorism: 14).

NATO Antlaşması'nın 3'üncü maddesi, krizle başa çıkmayı ifade eder: "… Taraflar, ayrı ayrı ve birlikte, sürekli ve etkili öz yardım ve karşılıklı yardım yoluyla silahlı saldırıya karşı bireysel ve kolektif kapasitelerini koruyacak ve geliştireceklerdir". Bu nedenle uluslar, kendi kapasitelerini geliştirmek için yanıt verirler. Ayrıca, 4'üncü madde istişareye atıfta bulunur: "… Taraflardan herhangi birinin toprak bütünlüğü, siyasi bağımsızlığı veya güvenliği tehdit edildiğinde birlikte istişare edeceklerdir" (Crisis Management in Terrorism: 14).

Antlaşmanın 5'inci maddesi, 11 Eylül'den sonra gündeme gelmiş olup bir üyeye karşı yapılan silahlı saldırının tüm üyelere yapılmış sayılacağını hükme bağlamaktadır. 7'nci maddede ise "... Antlaşma, BM üyesi olan tarafların Şart kapsamındaki hak ve yükümlülüklerini veya Güvenlik Konseyinin uluslararası barış ve güvenliğin sağlanması konusundaki temel sorumluluğunu hiçbir şekilde etkilemez ve etkilediği yönünde yorumlanamaz." denilmektedir. Kriz yönetimi tanımı, "Krizleri yatıştırmak, silahlı çatışmaya dönüşmesini önlemek ve/veya ortaya çıkarsa ortaya çıkan düşmanlıkları sınırlamak için alınan koordineli eylemler" olarak belirtilmektedir. Kriz yönetimi hedefleri; çatışmayı önlemeye katkıda bulunmayı, krizleri çatışmaya dönüşmelerini önlemek için etkili bir şekilde yönetmeyi, zamanında sivil ve askerî hazırlık yapmayı (kapsamlı ulusal savunma), kontrol etmeyi, saldırıyı veya saldırganı durdurmaya ve geri çekilmeye ikna etmeyi ve normal düzeni yeniden kurmayı kapsamaktadır (Crisis Management in Terrorism: 15-16).

Sonuç

NATO üyesi ülkeler tarafından Türkiye'ye bazı örtülü ve açık ambargolar uygulanmıştır. Ancak bu ambargolardan bazıları kaldırılmış veya kaldırılma çalışmaları yapılmaktadır. NATO'yu oluşturan ülkelerin vatandaşlarına sadece ırksal, dinsel, etnik, kültürel, dilsel veya coğrafi birtakım bağlantılarla kendilerine yakın buldukları topluluklarla kaynaşmaktan ziyade yeni bir kimlik, NATO üst kimliği ile birlikte yaşamanın ve dünyayı hak ettiği şekilde daha yaşanabilir bir yer yapmanın artık zamanının geldiği vurgulanmalıdır.

Her devlet, kendi milliyetçileri de dâhil olmak üzere her türlü ırkçılığı, her türlü etnik ve dinî sapkınlığını ortadan kaldıracak ulusal ve uluslararası projeler üretmeli ve kimse benim milletim, benim dinim, benim

kurduğum örgüt (terör örgütü) dememelidir. Doğa, nasıl ki doğal afetlerde sınır, ulus ve din kavramını tanımadan tüm yıkım gücüyle hareket edip yeryüzünü yeniden şekillendiriyorsa ulus devletler de aynı doğal afetleri örnek alarak din, ırk, ulus ayrımı yapmaksızın afetlerin tersine, yeniden planlamayla dünyayı daha yaşanabilir kılma çabası içerisine girmelidir.

Anahtar Sözcükler: NATO, Terörle Mücadele, Terörizm

4.2.13. Aybars ÖZTUNA[20]: *Evaluating Chinese Naval Infrastructure Developments in the South China Sea Through Geospatial Intelligence*

Introduction

The South China Sea (SCS) has emerged as a focal point of geopolitical tension, largely due to China's expansive maritime claims and subsequent infrastructure developments. This research provides a comprehensive analysis of Chinese naval infrastructure changes in the SCS, employing geospatial intelligence (GEOINT) to monitor, assess, and interpret these developments. The study underscores the strategic importance of the SCS, its resources, and the geopolitical implications of China's assertiveness in the region.

Background

The SCS is bordered by several Southeast Asian nations and serves as a critical maritime route, rich in resources like fish, oil, and gas. Its significance has led to longstanding territorial disputes among China, Vietnam, the Philippines, Malaysia, Brunei, and Taiwan. The historical context of these disputes is rooted in the early 20th century. The area's strategic and economic importance has drawn global attention from major powers like the United States, which has vested interests in maintaining freedom of navigation and regional stability. This strategic waterway is not only a lifeline for regional economies but also a significant factor in global trade and energy security.

Methodology

The research leverages geospatial intelligence to analyze satellite imagery from sources such as Google Earth. This method provides a unique vantage point for assessing naval activities and infrastructure developments. The study focuses on the construction of artificial islands by China and the establishment of military installations. Geospatial analysis includes examining changes over time, identifying new constructions, and evaluating the implications of these developments on regional stability. This approach combines data from multiple satellite passes to identify the changes in the region, offering insights that are critical for both regional policymakers and international observers.

[20] Res. Asst., Johns Hopkins University; Researcher, All Source Analysis; CEO, Geospatial Intelligence Institute, E-Mail: aoztuna1@jh.edu & oztunaaybars@gmail.com ORCID: 0000-0003-4434-9792

Findings

China has constructed several artificial islands in the SCS, particularly in the Spratly Islands. These islands serve as bases for military operations, equipped with runways, ports, radar installations, and missile shelters. The research identifies six major artificial islands, highlighting their strategic positioning along key trade routes. These constructions not only expand China's physical presence in the region but also serve as a statement of power and territorial control, directly challenging the claims and sovereignty of other nations in the SCS.

The artificial islands are equipped with substantial military infrastructure. This includes long runways capable of accommodating large military aircraft, hangars, radar and communication facilities, and missile shelters. The study details the specific capabilities of these installations, noting their potential impact on regional security dynamics. This militarization enables China to project power far beyond its mainland, threatening the delicate balance of power in the region and potentially restricting the movement of other nations' military and commercial vessels.

China's infrastructure developments have heightened tensions with neighboring states and increased the risk of conflict. The artificial islands enhance China's ability to project power and assert its territorial claims, challenging the maritime rights of other nations under international law, particularly the United Nations Convention on the Law of the Sea (UNCLOS). This situation has led to increased militarization and defensive postures by other claimant nations, contributing to an arms race that exacerbates regional instability.

The dredging and land reclamation activities associated with artificial island construction have significant environmental consequences. The study discusses the disruption of marine ecosystems and the potential long-term impact on biodiversity in the region. The destruction of coral reefs and the alteration of natural habitats can have a cascading effect on the marine food chain, impacting local fisheries and livelihoods.

Analysis of Key Locations

One of the most heavily fortified islands, Fiery Cross Reef, features extensive military facilities, including a runway, hangars, and defensive weaponry. Satellite imagery reveals continuous upgrades and expansions, emphasizing its strategic importance. This reef has been transformed into a hub of military operations, serving as a base for both defensive and offensive capabilities in the region.

Mischief Reef is another critical site, showcasing China's commitment to establishing a robust military presence in the SCS. The research highlights the presence of military vessels, air defense systems, and surveillance equipment. The reef's development has been a point of contention with the Philippines, which also lays claim to the area, leading to increased diplomatic strains and potential flashpoints for conflict.

Subi Reef has been transformed into a major military outpost, with satellite imagery capturing the construction of extensive infrastructure. The study notes its proximity to contested areas, increasing the likelihood of confrontations. Its development underscores the strategic importance China places on controlling access and asserting dominance in the region.

Challenges and Risks

The militarization of the SCS by China poses a significant challenge to regional stability. The study explores the reactions of neighboring countries and the role of international actors like the United States in countering China's assertiveness through Freedom of Navigation Operations (FONOPs). These operations are designed to challenge excessive maritime claims and ensure the free flow of trade and navigation, but they also risk escalating tensions and sparking confrontations.

The research examines the legal avenues pursued by affected nations, particularly the Philippines' victory at the Permanent Court of Arbitration in 2016. It discusses the limitations of international legal mechanisms in enforcing compliance and resolving disputes. The study suggests that while legal victories are significant, they must be supported by diplomatic and strategic efforts to be effective.

Conclusion and Policy Recommendations

The study concludes that China's naval infrastructure developments in the SCS represent a strategic move to consolidate its claims and enhance its regional influence. These developments, marked by the construction of artificial islands and the establishment of military installations, reflect a broader strategy to assert dominance over one of the world's most crucial maritime regions. The findings underscore the urgency for a coordinated international response to uphold maritime law, particularly the United Nations Convention on the Law of the Sea (UNCLOS), and ensure regional stability. The policy recommendations emphasize the importance of strengthening diplomatic engagements among claimant states and international actors to foster dialogue and reduce tensions. Enhancing regional security cooperation through joint maritime patrols, intelligence sharing, and conflict prevention mechanisms is also crucial. Leveraging geospatial intelligence for continuous monitoring and analysis of Chinese activities can provide real-time insights that inform policy decisions. This multi-faceted approach, combining legal, diplomatic, and military strategies, is essential to address the complexities of the SCS disputes effectively. Policy recommendations include strengthening diplomatic engagements, enhancing regional security cooperation, and leveraging geospatial intelligence for continuous monitoring and analysis.

Future Research Directions

The research highlights the importance of ongoing monitoring of geopolitical developments in the SCS to understand the evolving strategic landscape. Future studies could delve into the effectiveness of international diplomatic efforts, particularly the role of multilateral forums such as ASEAN and the

United Nations in mediating disputes and fostering cooperative security arrangements. The impact of technological advancements in surveillance, such as the use of drones and advanced satellite imagery, could be explored to assess how they enhance or challenge existing security frameworks. Additionally, investigating the environmental consequences of sustained military activities, including the long-term effects on marine biodiversity and coastal ecosystems, can provide critical insights into the ecological trade-offs of geopolitical strategies. Furthermore, exploring the socio-economic impacts on local communities, such as disruptions to fishing industries and livelihoods, and the potential for regional cooperative frameworks that promote sustainable development, could offer a holistic understanding of the SCS's challenges and opportunities.

Keywords: South China Sea (SCS), Geospatial Intelligence, Satellite Imagery

4.2.14. İbrahim İRDEM[21] & Murat UZUNPARMAK[22]: *Siber İstihbaratın Küresel Güvenlik Mimarisine Etkisi*

Küreselleşme olgusunun hız kazanması, güvenliğe ilişkin potansiyel tehdit ve riskleri daha karmaşık hale getirerek devletlerin güvenlik anlayışını yeniden gözden geçirmelerini zorunlu hâle getirmiştir. Devletlerin güvenlik stratejilerini tatbik ederken azami özen göstermesi gereken temel güvenlik alanlardan birisi de hiç şüphesiz siber güvenlik olmuştur. Dünya genelinde siber saldırılardaki artış, vatandaşların kişisel bilgilerinin ele geçirilmesinden veri ihlallerine, kamu hizmetlerinin kesintiye uğramasından finansal sistemlerin çökmesine, diplomatik bilgilerin deşifre olmasından ulusal güvenlik zafiyetine kadar çok sayıda soruna yol açabilmektedir. Bu nedenle ilgili devlet otoritelerinin gerek ülke içinden gerekse ülke dışından gelebilecek her türlü siber saldırıya karşı teyakkuzda olmasına yönelik güçlü koruma sağlayan ve iyi işleyen siber güvenlik yönetimine ihtiyacı bulunmaktadır.

Dünya çapında pek çok ülke artık siber tehditlere karşı koruma mekanizması geliştirmek ve siber saldırı yeteneklerini güçlendirmek amacıyla siber güvenliğe ilişkin stratejiler benimsemektedir. Siber saldırılardan en çok etkilenen ülkelerin başında Amerika Birleşik Devletleri (ABD) ve Rusya Federasyonu (RF) gelmektedir. ABD siber güvenlik stratejisinde 21. yüzyıl itibarıyla askerî güvenlik ve istihbarat açısından hedefler belirlemiş, ABD Savunma Bakanlığı, İç Güvenlik Bakanlığı, Federal Soruşturma Bürosu (FBI) ve Merkez Haber Alma Örgütü (CIA) başta olmak üzere gerek ilgili kurumlar gerekse yerel düzeyde hazırlanan mevzuatlar kapsamında çalışmalar yürütmeye başlamıştır. ABD ve Rusya arasındaki siber uzayda üstünlük kurma mücadelesi Rusya'nın askerî gücünü artırma hedefi yanında siber savunma alanında devasa boyutta yatırımlar yapmasını beraberinde getirmiştir. Rusya, ulusal strateji belgelerinde siber güvenlik tedbirlerine geniş şekilde yer vermiştir (Darıcılı ve Özdal,

[21] Doç. Dr., Polis Akademisi Başkanlığı, E-Posta: ibrahimirdem33@gmail.com, ORCID ID: 0000-0003-0559-3418

[22] Dr., İçişleri Bakanlığı, E-Posta: muzunparmak@gmail.com, ORCID ID: 0000-0002-3027-401

2017: 124-125). Ancak önleyici tedbirler yanında Rusya, siber espiyonaj ve siber kontrespiyonaj faaliyetlerini de sürdürmüştür. Bu konuda önemli bir örnek olarak 2022'de Ukrayna'ya saldırması ile süren çatışmalar öncesinde Ukrayna'daki elektrik santrallerine gerçekleştirilen siber saldırılar Rusya'nın askerî savaş yöntemi yanında siber savaş yöntemine de yer verdiğini aşikâr şekilde ortaya koymaktadır. Hatta Rusya-Ukrayna savaşı sırasında da iki ülkenin hacker grupları arasında siber çatışmalar süregelmiştir. Batı ülkelerinin Ukrayna'ya yönelik Rusya'dan gelebilecek saldırılara karşı verdiği destek Ukrayna'nın siber saldırılara karşı savunmasında ve saldırı kapasitesinde önemli ilerlemelere sebep olmuştur. Çin Halk Cumhuriyeti (ÇHC) ise, dünyada en fazla siber güvenlik uzmanına sahip ülke olarak gerek iç güvenlik açısından gerekse de ABD ve Rusya hegemonyası karşısında siber alanda bir Pekin Etkisi yaratmak amacıyla siber güvenliğe ciddi önem atfetmektedir. Siber alanda asimetrik strateji arayışı içinde olan Çin'in en önemli hedefleri arasında bir siber süper güç olmak ve dünya teknoloji lideri olarak küresel alanda öne çıkmak gelmektedir. Politika önceliğini dijital teknolojiye veren Çin, siber yönetişime yönelik kurumsal bir çerçeve oluşturmuştur. Türkiye ise dünyadaki gelişmelere paralel olarak siber güvenliğe ilişkin stratejik önlem ve adımlara yer vermiştir. 2012'de Siber Güvenlik Kurulu oluşturulmuş, bu kurula siber güvenliğe ilişkin politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik karar alma yetkisi verilmiştir. Bununla birlikte başta Millî İstihbarat Teşkilatı olmak üzere Emniyet Genel Müdürlüğüne bağlı Siber Suçlarla Mücadele Daire Başkanlığı, Jandarma Genel Jandarma Genel Komutanlığı Siber Suçlarla Mücadele Daire Başkanlığı, Türk Silahlı Kuvvetleri bünyesindeki Siber Savunma Komutanlığı, Bilgi Teknolojileri ve İletişim Kurumuna bağlı Ulusal Siber Olaylara Müdahale Merkezi, Cumhurbaşkanlığı Dijital Dönüşüm Ofisine bağlı Siber Güvenlik Dairesi Başkanlığı siber güvenlik alanında çalışmalar yürüten kurumlar olarak öne çıkmaktadır. 2018'de Cumhurbaşkanlığı Savunma Sanayii Başkanlığı himayesinde ve Dijital Dönüşüm Ofisinin de desteğiyle Türkiye'de ulusal siber güvenlik sistemi ekosistemi kurmayı amaçlayan, siber güvenlik ürünlerini geliştirmeye ve bu ürünlerin kullanımının yaygınlaştırılmasını amaçlayan Türkiye Siber Güvenlik Kümelenmesi kurulmuştur (Türkiye Siber Güvenlik Kümelenmesi, 2023). Türkiye'nin 2020-2023 yılları arasını kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planında ise siber tehditlere ilişkin eğilimler değerlendirilerek hedefler ortaya konulmuştur. Bu doğrultuda karşılaşılabilecek siber tehditlerin etkisinin azaltılması ve Türkiye'nin siber güvenlik alanında dünyada üst sıralarda yer alması amaçlanmıştır. Kritik alt yapıların korunması ve mukavemetin artırılması, ulusal kapasitenin geliştirilmesi, organik siber güvenlik ağı, yeni nesil teknolojilerin güvenliği, siber suçlarla mücadele, yerli ve millî teknolojilerin geliştirilmesi ve desteklenmesi, siber güvenliğin milli güvenlikle entegrasyonu, uluslararası iş birliğinin artırılması hususları stratejik amaçlar arasında yer almıştır (Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, 2020: 6)

Hem dünyada hem de Türkiye'de siber tehditlere ilişkin saldırı riskleri gün geçtikçe artmaktadır. Bu nedenle gerek ulusal güvenliğin sağlanmasında gerekse dünya genelinde güvenliğin muhafazasının temininde siber istihbarat önemli bir domino taşıdır. Bu bağlamda devletlerin otorite sahibi olduğu

ülkeler üzerinde bireysel çabalarına ek olarak siber istihbarat alanında iş birliğinin sağlanması, siber tehditlerle mücadele açısından gereklilik arz etmektedir.

Siber istihbarat, esasında siber tehditler hakkında bilgi toplama, işleme ve analiz etme sürecidir. Siber istihbaratla siber saldırıların önlenmesi ve azaltılması amaçlanmaktadır. Siber istihbaratta siber alan içerisindeki siber güvenlik tehditlerinin, risklerin ve fırsatların tanımlanarak izlenmesi; potansiyel güvenlik açıkları hakkında bilgi toplanması, bilgilerin işlenmesi, analiz edilmesi ve yayılması ön plandadır. Saldırganların taktiklerinin, tekniklerinin ve yöntemlerinin geniş çaplı olarak değerlendirildiği siber istihbarat sayesinde saldırıların tanımlanması, olası bir saldırıya karşı hazırlık ve saldırının bertaraf edilmesi hedeflenmektedir.

Her ne kadar devletler birbiriyle mücadele ve üstün gelme arzusu çerçevesinde kendi istihbarat kapasitesini güçlendirmeye çalışsa da siber istihbarat aynı zamanda küresel güvenliğin sağlanmasında önemli bir işleve sahiptir. Hem evrensel düzeyde kişisel veriler ve bilgi güvenliği konusundaki standartların korunması hem de ülkeler arasındaki koordinasyon sayesinde müşterek tehditlere karşı daha hızlı ve etkili müdahalede bulunmak amacıyla siber yönetişim ya da siber alanı istihbarata entegre edecek şekilde "siber istihbarat yönetişimi" tatbik edilmelidir.

Siber tehditlerin önlenmesi sadece devletlerin tek başına siber güvenlik önlemleri almasından ziyade yönetişim odaklı politikalar sayesinde güvenli ve dirençli bir dijital ortamın temin edilmesiyle mümkündür. Risk değerlendirmesini öne çıkaran, geniş kapsamlı, çeşitli paydaşların beklentilerini esas alan, katılımcı, proaktif bir yönetişim stratejisi izlenmelidir. Ayrıca devletler arasında siber alanla ilgili uluslararası yükümlülük ve sorumlulukları içeren antlaşmaların gerçekleştirilmesi, birbirlerine karşı yönelebilecek siber saldırıları caydırıcı bir etki doğurabilmektedir. Böylece küresel anlamda karşılaşılabilecek ortak tehditlere karşı etkin bir mücadele sağlanacak, devletlerin ve ilgili kuruluşlarının dijital verileri korunarak kamuoyunda sosyo-ekonomik açıdan istikrar ve güven tesis edilebilecektir.

Siber güvenliğe yönelik mevcut ve potansiyel tehditlerin izlenmesinde, analiz edilmesinde, proaktif stratejilerin geliştirilmesinde siber istihbarat; siber güvenlik yönetimini güçlendirmekte ve devletleri siber saldırılara karşı hazırlıklı ve dayanıklı kılmaktadır. Özellikle son yıllarda siber saldırıların bir savaş aracı olarak kullanıldığı göz önünde bulundurulursa devletlerin hem vatandaşlarının siber alandaki güvenliğini sağlamak hem de saldırıların başlıca hedeflerinden olan kurum ve kuruluşlarını siber saldırılara karşı korumak için etkin siber istihbarat stratejisi izlemesi gerekmektedir. Bununla birlikte siber istihbarat ülkeler arasında koordinasyonu ve iş birliğini de güçlendirerek uluslararası güvenlik sorunlarının erken tespitinde ve bertaraf edilmesinde, siber saldırılara karşı etkili koruma sistemi oluşturulmasında küresel güvenliğe katkı sunmaktadır.

Anahtar Sözcükler: Küreselleşme, Siber Güvenlik, Siber İstihbarat

4.2.15. Laçin AKYIL[23]: *Avrupa Birliği'nin Yeni Bir İstihbarat Servisi Oluşturmasının Türkiye-Avrupa Birliği İlişkilerine Olası Etkileri*

Bu çalışmada, Avrupa Birliği (AB) tarafından gelecekte bütünleşik bir istihbarat servisi oluşturulmasına giden süreç ve oluşturulacak muhtemel yeni istihbarat servisinin Türkiye-AB ilişkilerini nasıl etkileyeceği ele alınmıştır. Bu doğrultuda AB'nin istihbarata yönelik faaliyetlerini, güvenlik konusu üzerinden literatür taraması ile açıklamak hedeflenmiştir. Çalışmanın amacı, uzun yıllar Türkiye ile istihbarat ilişkisini sürdüren AB'nin, yeni bir istihbarat servisi oluşturması ihtimalinde, bu durumun avantaj ve dezavantajlarının neler olabileceği hususunda bazı senaryolar üzerinden çıkarımlarda bulunmaktır. Çalışma, hem Türkiye'nin gelecekteki istihbarat ve güvenlik ve politikalarına hem de AB ile ilişkilerine yön vermesi açısından önem arz etmektedir.

AB'de istihbarata yönelik bir girişim oluşturma tartışmaları uzun zamandır süregelmektedir. Nitekim geçmişten bu yana The Club of Berne, AB Askerî Personeli (European Union Military Staff-EUMS) İstihbarat Direktörlüğü, AB Kolluk İş Birliği Ajansı (European Union Agency for Law Enforcement Cooperation-EUROPOL), AB Uydu Merkezi (European Union Satellite Centre-SATCEN), AB Cezai Konularda Adli İş Birliği Ajansı (European Union Agency for Criminal Justice Cooperation-EUROJUST), AB İstihbarat ve Durum Merkezi (EU Intelligence and Situation Centre-EU INTCEN), Avrupa Sınır ve Sahil Güvenlik Ajansı (Frontex) vb. kurumlar, güvenlik alanında istihbarat sağlamak amacıyla faaliyetlerini yürütmektedir.

EU INTCEN, AB'nin özel sivil istihbarat kurumudur. Ancak kurumun istihbarat operasyonlarının üye ülkelerin sorumluluğunda olması ve kuruma ait görev tanımının stratejik analizleri değerlendirmekle sınırlı kalması, EU INTCEN'in işlevselliğini tartışılır hâle getirmiştir (Statewatch, n.d.). Bu durum, ulusal istihbarat birimlerinin hassas bilgileri paylaşmakta isteksiz olmasından kaynaklanmaktadır. Ayrıca günümüzde teknoloji, savaş ve terör gibi çeşitli sebeplerden dolayı devletlerin ve uluslararası örgütlerin güvenlik politikaları değişime uğramaktadır. Bu da ister istemez istihbarat servislerinin dinamiklerinin değişmesine yol açmaktadır. AB'nin güvenlik politikalarında ve dolayısıyla istihbarat paylaşımında önemli ortaklarından biri olan Kuzey Atlantik Antlaşması Örgütünün (North Atlantic Treaty Organization-NATO) işlevinin sorgulanıyor olması, AB'de istihbarat servisi oluşturma konusunda tartışmaların artmasına sebep olmuştur. 11 Eylül saldırıları, ABD'nin Afganistan ve Irak müdahaleleri gibi olaylar, NATO'nun barışı tesis etmesindeki gücünü tartışılır hâle getirmiştir (Birsel, 2012, s. 119). ABD'de 2017-2021 yıllarında iktidarda olan ABD Başkanı Donald Trump'ın 2017'de Brüksel'de gerçekleşen NATO Zirvesi'nde, NATO'yu "modası geçmiş bir kurum" şeklinde ifade etmesi, NATO'ya olan güven meselesini gündeme getirmiştir (Euronews, 25 Mayıs 2017). Trump döneminde, ABD'nin 2019'da NATO'nun görüşüne başvurmadan Suriye'de bulunan askerlerini çekmesine karşılık Fransa Cumhurbaşkanı Emmanuel Macron, NATO'nun "beyin ölümünün

[23] Dr. Öğr. Üyesi, İstanbul Arel Üniversitesi, E-Posta: lacinakyil@arel.edu.tr, ORCID: 0000-0001-7816-3131

gerçekleştiğini" belirtmiştir (BBC, 8 Kasım 2019).

Rusya-Ukrayna Savaşı ve AB sınırları içinde gerçekleşen terör olaylarının artması gibi etkenler de AB içinde istihbaratta yeni bir yapılanma ihtiyacını gözler önüne sermiştir. Avrupa Komisyonu Başkanı Ursula von der Leyen'in talebi üzerine Finlandiya Eski Cumhurbaşkanı Sauli Niinistö tarafından hazırlanan ve 30 Ekim 2024'te yayımlanan "Safer Together Strengthening Europe's Civilian and Military Preparedness and Readiness" adlı raporda, AB içinde yeni bir istihbarat yapılanmasının gerekli olduğu yönünde vurgu yapılmıştır. Raporda Niinistö'nün en önemli önerilerinden biri, bütünleşmiş bir AB istihbarat servisinin oluşturulmasıdır. Artan tehditlerin karşısında AB'nin kararlı bir eylemde bulunmasını sağlamak için istihbarattan daha iyi bir şekilde yararlanılması önemlidir. AB kurumlarındaki ve üye ülkelerdeki karar vericilerin, Birliğe yönelik tehditler ve gizli faaliyetler hakkında net ve zamanında istihbarata sahip olmaları gerekmektedir. Bu nedenle EU INTCEN ve AB Askerî İstihbaratı'ndan oluşan AB'nin Tek İstihbarat Analiz Kapasitesi'nin (Single Intelligence Analysis Capacity-SIAC) güçlendirilmesi gereklidir. AB düzeyinde istihbarat iş birliğinin güçlendirilmesi, politika alanları arasında düzenli ve yapılandırılmış istihbarat paylaşımı için önemlidir. Oluşturulması tartışılan bu yeni yapıda, üye ülkelerin ulusal dış istihbarat ve iç güvenlik servislerinin görevlerini taklit etmekten veya ulusal güvenlik konusundaki ayrıcalıklarına müdahale etmekten kaçınılmalıdır. Bunun yerine SIAC'ın, üye ülkelerin istihbarat toplama konusundaki ulusal kapasitelerine ilişkin ve tamamlayıcılık açısından bir güvenlik sağlayıcısı olarak AB'nin faaliyetlerini ve kurumsal liderliğini tam olarak destekleyecek bir servise dönüştürülmesine odaklanılması önemlidir. Üye ülkelerin yetkililerinin; casusluk, sabotaj ve terörizm ile organize suçlara karşı mücadelesini desteklemek için şifrelenmiş verilere yasal erişimi için sağlam bir çerçeve oluşturması gereklidir. Karşı istihbarat servislerinin, AB'de faaliyet göstermesini mümkün olduğunca zorlaştırmak için ortak eylemlerde bulunulması önemlidir. Üye ülkelerin karşı istihbarat uygulamalarındaki tutarsızlıkları ve yetersiz sınır ötesi bilgi paylaşımı gibi eksiklikleri, kötü niyetli aktörler tarafından istismar edilebilir. Bu sebeple AB'nin, hibrit tehditlere karşı üye ülkeler ve AB kurumları arasında daha iyi istihbarat paylaşımında bulunması gereklidir. İç ve dış güvenlik arasındaki bağlantılar, operasyonel ihtiyaçlar için geliştirilmiş kurumlar arası bilgi paylaşımı da dâhil olmak üzere istihbarat yapılarına daha iyi yansıtılmalıdır. Örneğin SIAC, EUROPOL ve Frontex gibi kurumların aralarında bir iş birliği bulunmasına rağmen bu iş birliği, operasyonel düzeyde stratejik politika ve kriz bilgilendirmeleri için resmî boyutta değildir (Niinistö, 2024).

AB gibi çok üyeli bir örgütte istihbarat toplama ve üretme konusunda farklı yaklaşımların bulunması kuvvetle muhtemeldir. Bunun için üye ülkelerin ortak istihbarat fikrine açık olabilecek bir kültüre hazır olmaları gereklidir. AB'ye üye ülkelerinin ortak bir istihbarat servisi oluşturması ve buna eşit düzeyde ilgi göstermesi oldukça zordur. Ayrıca istihbarat konusunda en hassas nokta, güven meselesidir. Dolayısıyla ortak bir istihbarat servisinin sağlanması için AB üye ülkelerinin birbirine güven duyması

gereklidir (Özcan, 13 Ocak 2015). Ancak AB'nin geçmiş tecrübelerinden yola çıkılarak, AB ülkelerinde güven duygusunun her bir üye ülkesinde aynı düzeyde olduğunu söylemek mümkün gözükmemektedir.

Türkiye açısından ele alındığında; AB'nin bütünleşik bir istihbarat servisi kurmasının, Türkiye-AB güvenlik iş birliğine yönelik bazı olası riskleri gündeme getirmektedir. Türkiye, AB'nin önemli güvenlik ortaklarından biridir. AB özellikle terörle mücadele, organize suçlar, sınır güvenliği ya da düzensiz göç gibi alanlarda Türkiye ile iş birliğini sürdürmektedir. Ancak Niinistö'nün raporunda ele aldığı üzere bütünleşik bir Avrupa istihbarat servisinin kurulması, Türkiye'nin bu alanlardaki AB ile olan güvenlik ortaklığını sınırlandırabilir ve Türkiye-AB ilişkilerinde asimetrik güç dengesine yol açabilir. Türkiye'nin AB tarafından bir "dış aktör" olarak tanımlaması, ikili arasındaki iş birliğinde bir dezavantaj durumu oluşturabilir. Özellikle de düzensiz göç ve terörizm alanlarında AB'nin kendi çıkarlarını gözetecek bir yaklaşım benimsemesi, Türkiye'nin güvenlik politikalarını doğrudan etkileyebilir. Bu noktada Türkiye'nin terörle mücadele konusundaki hassasiyetlerinin, AB tarafından göz ardı edilmesi ihtimali oluşabilir. Günümüzde istihbarat konusuyla ilintili olan veri güvenliği, siber güvenlik ve siber savaşlar, hem Türkiye'nin hem de AB'nin üzerinde önemle durduğu konular arasında yer almaktadır. Yeni bir istihbarat servisinin oluşturulması, Türkiye'nin, siber tehditlere karşı AB ile olan iş birliğinde geri plana düşmesine neden olabilir. Bu yeni muhtemel istihbarat sisteminin kurulması sonucunda Türkiye ve AB arasında artacak olan güven eksikliği ise ilişkileri tüm politika alanlarında olumsuz etkileme ihtimalini ortaya çıkaracaktır.

Anahtar Sözcükler: İstihbarat, Güvenlik, Avrupa Birliği, Türkiye- Avrupa Birliği İlişkileri

4.2.16. Atahan Birol KARTAL[24]: *İstihbarat ve Teknoloji: Yeni Kaynakların Yönetimi*

Giriş

İstihbaratın tanımımı yapmak gerekirse, "düşman veya gelecekte düşman olabilecek yabancı ülkeler, hâlen ve gelecekte ortaya çıkabilecek operasyon alanları ile ilgili bilgilerin toplanması, işlenmesi, bu bilgilerin bir bütün hâline getirilmesi, değerlendirilmesi, analizi ve yorumlanmasından kaynaklanan bilgiler" olarak tanımlayabiliriz (Karasoy, 2022). İstihbarat dendiğinde aklımıza mücadele gelebilir, mücadele deyince de savaş. Yani savaş, aslına bakıldığında istihbarat ile iç içedir. İstihbarat yapılmadan bir savaştan başarı beklenemez. Savaş olgusunu inceleyen en eski askerî stratejistlerden olan, askerî strateji üzerine yazdığı yazılarını topladığı "Savaş Sanatı" adlı eserine sahip Çinli komutan ve askerî stratejist Sun Tzu'dan beri istihbarat, bir savaşta ve bir çatışmada düşmana üstünlük sağlamanın en önemli aracı olarak değerlendirilmiştir. Düşman bize zarar vermek istemektedir ancak düşmanın niyetini

[24] Dr. Öğr. Üyesi, İstanbul Beykent Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi (İngilizce) Bölümü, E-Posta: atahankartal@beykent.edu.tr, ORCID: 0000-0003-3098-1981

anlamak, bize hangi oranda zarar verebileceğini bilmek önemlidir. (Taban & Aydilek, 2023).

Yeni nesil savaş (YNS) alanlarında yapılan çekişmeler, mücadeleler ve muharebeler, fiziki ortamdan sanal alanlara doğru yönelmiştir. Çünkü artık son yıllarda güvenlik anlayışı, devleti merkeze almaz; sadece askerî tehditlere indirgenebilen bir yaklaşım olmaktan çıkmıştır. Güvenlik, siber alan güvenliğine doğru yönelmeye başlamıştır (Karasoy, 2022).

Siber güvenlikten konuşuyor isek siber alanın güvenliğinden de bahsetmemiz gerekir. Siber istihbarat kavramı da bu sebeple çok önemlidir. Siber istihbaratın tanımını şu şekilde verebiliriz (Karasoy, 2022):

> *"Bir ülkenin siber uzaydaki cihazları, enerji üreticileri, kabloları, internet servis sağlayıcıları, sunucuları vb. donanımlarla birlikte yazılımları ve bundan başka siber güvenlik, siber saldırı, siber istihbarat vb. faaliyetlerde bulunacak teknokratların, görevlilerin nitelik ve nicelik gibi özellikleriyle ilgili bilgi toplanması ve analiz edilmesidir."*

Siber güvenliğin tanımın yapan Uluslararası Telekomünikasyon Birliği de bu tanımı şu şekilde yapmıştır, buna göre siber güvenlik, *"Siber uzayda, kullanıcılar ve organizasyonların varlıklarını korumak amacı ile kullanılan politikalar, risk yönetimi yaklaşımları, araçlar, güvenlik kavramları, güvenlik önlemleri, uygulamalar, kurallar, eylemler, eğitimler ve teknolojilerin bütünü,"* olarak tanımlanır (Karasoy, 2022).

Karasoy ve Babaoğlu (2020) siber güvenliğin üzerinde durulmasının nedenlerini şöyle sıralamıştır:

-Bireylerin sanal ortamda bulunması

-Özel sektörün ticari faaliyetleri için internet kullanımındaki artış

-Devletin kritik alt yapılarının internete bağlı olması

-Kamu hizmetlerinin internet üzerinden verilmesi (E-Devlet)

Alt yapılar sayesinde birbirine bağlı elektronik cihazların birbirine bağlanması, buradan bilgi edinilmesi ve bu bilginin kullanıldığı faaliyet alanı siber alan, siber ortam veya siber uzay olarak tanımlanır. Bu alan çeşitli verileri global olarak depolar (Yılmaz, 2020). Farklı bir ifade ile siber alanda verileri inceleyerek bu verilerden istihbarat elde etmedir siber istihbarat. Aynı zamanda hedefine aldığı dijital cihazlara sızarak, bu cihazdaki bilgileri elde ederek istihbarat toplama faaliyetidir. Siber istihbarat faaliyeti icra edilirken açık kaynaklardan da yararlanılır ve bu bilgiler derlenir. Hedef ülkenin kritik denebilecek altyapılarına yapılan saldırılar da siber istihbaratın ilgi alanıdır (Karasoy, 2022).

Siber istihbaratın önemli bir tarafını siber tehdit istihbaratı oluşturur ki bu güvenlik kurullarının siber saldırıları önleme ve bu saldırılara karşılık verme kabiliyetinin oluşturulmasına meydan verir (Karasoy,

2022).

Günümüzde elektronik cihazların sayıları günden güne artmaktadır. Bunların arasında cep telefonlarını, bilgisayarları, uyduları, kameraları sayabiliriz. Bu elektronik cihazlar veri üretmektedir ve bu üretilen verilerin bir araya gelmesi ile büyük veri setleri oluşmaktadır ki biz buna "büyük veri" demekteyiz. Büyük veriyi oluşturan unsurlar o kadar karmaşıktır ki bunlar arasında örüntüler tespit ederek analiz yapıp anlamlı bilgiler elde etmek için "makine öğrenmesi" olgusundan yararlanmak gerekmektedir. Bu büyük veriyi inceleyen makineler bir örüntü tespit ettiklerinde, bunu kullanıcılara iletmekte ve bu örüntüler anlamlandırılmaktadır. Bu da veri madenciliği veya bilgi madenciliği olarak tanımlanmaktadır (Yılmaz, 2022).

Yapay zekâ, yeni otonom sistemler ve insansız hava araçlarının savaşın karakterini değiştireceği açıktır. Bu yeni gelişmeler devletlerin savunma sistemlerini değiştireceği gibi istihbarat yapılarını da etkileyecektir. Bu etkileme akıllı savaş ve akıllı istihbaratı ortaya çıkaracaktır. Rusya-Ukrayna Savaşı'nda bizlerin, sıradan vatandaşların, ellerindeki akıllı telefonlar veya bilgisayarlar vasıtası ile istihbarat toplayıcısı olabildiklerini gördük. Vatandaşların çektiği resimler ve videolar istihbarat birimleri tarafından analiz edilerek, değerlendirmeler yapılarak elde edilen bilgiler gerekli yerlere ulaştırılmaktadır (Yılmaz, 2022).

Siber uzay, uluslararası alanda daha büyük bir risk oluşturmaya başlamıştır. Riskin sınırları belli olmayan saldırmanın artık çok az maliyetli olduğu yeni bir güvenlik alanı ortaya çıkmıştır. Büyük orduları olan, kara ve denize hâkim devletlerin karşısında daha güçsüz ve küçük devletler siber uzayı asimetrik boyutta kullanabilmektedir. Bu sebeple devletler bu konuda yatırımlar yapmaya başlamıştır. 2016'da yapılan NATO Varşova Zirvesi'nde, siber uzay da bir harekât sahası olarak tanımlanmıştır ve ülkelerin iş birliklerini artırması istenmiştir. Daha sonra 2018'deki NATO Brüksel Zirvesi'nde, Belçika'nın Mons şehrinde Siber Operasyonlar Merkezinin kurulmasına karar verilmiştir (Polat, 2020).

Siber Terörizm

Artan internet kullanımı, bazı tehditleri de beraberinde getirmiştir. Bu tehditlerden biri de siber terörizmdir. Siber terörizm; siyasi mercileri, kişi ve kurumları baskı altına almak, çalışamaz hâle getirmek amacıyla yapılır. Resmî kuruluşların veri tabanlarına ve bilgisayarlarına saldırı gerçekleştirilerek bu kuruluşlar tehdit edilir ve onlara zarar vermeye çalışılır. Sosyal ağlar üzerinden yapılan ve terörü destekleyen faaliyetler de bu kapsamda değerlendirilir. Terör örgütleri tarafından bu siber saldırıların kullanılmak istenmesinin en büyük sebebi, güvenlikle ilgili birimlerin saldırı yapan teröristi bulmasının zor olmasıdır. Ayrıca kimin tarafından yapıldığının bilinmesi çok zor olan bu saldırılar, daha maliyetsizdir ve terörist açısından ölüm riski çok azdır. Saldıran teröristlerin silaha, bombaya ihtiyacı yoktur (Yılmaz, 2020).

Bilgi teknolojilerindeki değişimler, özellikle küresel anlamda uyduların kullanılması, yeni insansız hava araçları gibi yeni keşif ve gözetleme tekniklerinin kullanılması ve ayrıca yeni gelişmelere paralel olarak bunların iletişim ve istihbarat alanında kullanılması, istihbaratın geleneksel sistemin dışına çıktığının işaretidir. Ayrıca hedef ülkelerin altyapılarına gönderilen bilgisayar virüsleri sayesinde bu tesislerin çalışamaz hâle geldiği görülmektedir. Teknolojik gelişmelerin istihbaratın dönüşümündeki etkileri internetin de kullanılması ile birlikte düşünüldüğünde daha iyi anlaşılacaktır (Yılmaz, 2020).

İstihbarat Analizi

Analiz yapma, istihbarat çarkının en önemli aşamalarındandır. İstihbaratın işlenmesini ve bu işlenmiş malzemenin anlamını çözümleyerek gerekli yerlere iletilmesini, analistler gerçekleştirir. Bir bakıma, raporlama aşaması biter bitmez istihbarat analizi başlar, denilebilir. İstihbarat analizi, karar vericiye karar vermesinde yardımcı olur. Aslında yapılan, belirsiz ortamı ortadan kaldırarak fırsatlar sunmaktır. Dijital olarak gelişim ve dönüşüm, istihbarat çarkının tamamına bir avantaj sağlar. İstihbarat analizi yapmakla görevli olanlar, tehditleri daha kısa sürede ortaya çıkararak karar vericileri bilgilendirir. Bu hızı kazanmak için dijital gelişim ve dönüşümün hızlı bir şekilde gerçekleştirilmesi gerekmektedir. Ancak günümüzde, dijital çağın getirdiği geniş bilgi ve veriler sebebiyle istihbarat analisti olarak görev yapanların çok fazla zorluklarla karşılaştığı görülmekte ve bu kadar çok bilgiyle mücadele etmesi beklenmektedir.

Soğuk Savaş'ın bitiminden sonra açık kaynak istihbaratı (*Open Source Intelligence*, OSINT) artışa geçmiştir. Dijital açık kaynak istihbaratının kullanılmasındaki artış; akıllı telefonların kullanımının artması, vatandaşların ülkelerindeki olaylarla ilgili büyük miktarda içeriği uygulamalar vasıtası ile paylaşması, bu verilerin bir maliyetinin olmaması ve herkesin rahatlıkla erişebilmesi, analistler tarafından yapılacak analizlere açık olması ile ilgilidir. Dijitalleşme sonucu erişilemez alan neredeyse kalmamıştır. Açık kaynak istihbaratının kolay erişilebilirliği bir kolaylık getirmesine rağmen bu kaynakların analiz birimlerince analiz edilmesi gereklidir. Açık kaynak istihbaratının sağladığı verilerin çokluğu ve kapsadığı alanın büyüklüğü, istihbarat analizi yapanları bilgisayar kullanımına itmiştir. Verileri toplamak, muhafaza etmek, analizini yapmak, insanın kapasitesini zorlayacağından yeni teknolojileri kullanmak bir zorunluluk hâline gelmiştir. İyi istihbaratı kötü istihbarattan ayırmak için yapılan çalışmalar buna en güzel örnektir. SOCMINT yani sosyal medya istihbaratı, sosyal medyanın büyük oranda kullanılması sebebiyle istihbarat elde etme açısından önemlidir. Kamuoyu duyarlılığı ve toplumun etkilenmesi açısından kıymetlidir. Bazı olayların kim tarafından, nasıl yapıldığı; suçların neden ve nasıl meydana geldiği gözlemlenebilir. Suça katılanları neyin motive ettiği ortaya konabilir (Taban & Aydilek, 2023).

2012'ye kadar Türkiye'de siber güvenlik ile ilgili yapılan çalışmalar Bilgi Teknolojileri ve İletişim

Kurumu tarafından yapılmıştır. Daha sonra bu görev yine 2012'de Ulaştırma ve Altyapı Bakanlığına verilmiş ve Siber Güvenlik Kurulu kurulmuştur. Bu kurul, Türkiye'nin siber güvenlik ile ilgili faaliyetlerinde önemli ölçüde çalışmalar yapmıştır. Nitekim 2013-2014 Eylem Planı'nda, kamuda bilgi teknolojileri ve sistemlerinin güvenliğinin sağlanması hedeflenmiş, kamusal alanlarda kritik sistem güvenliğinin sağlanması amaçlamış, siber saldırıya uğrayan sistemler varsa bunların tekrar normale dönmesi ve siber saldırı yapanların yakalanması için kurumlar arasında koordinasyonlu çalışmalar öngörülmüştür. Ancak siber uzayın hızlı dönüşümü bazı sorunları da beraberinde getirmiştir. Bunların arasında; güvenlik açıklarına devlet içerisinde koordineli bir şekilde karşılık verilememesi, strateji ve eylem planlarının devlet içerisinde geliştirilmesinde etkisiz kalınması ve siber istihbaratın daha güçlü bir yapıya kavuşturulması konuları vardır. Bu sebeple Türkiye'de, Millî İstihbarat Teşkilatına bağlı olarak siber istihbarat çalışmaları öncelikle Elektronik/Teknik İstihbarat Başkanlığı tarafından yapılmıştır. Ancak siber tehditlerin artması ve siber savaşların ülke güvenliği bakımından giderek daha ciddî riskler ve tehditler getirmesinden dolayı siber istihbarat çalışmalarını daha detaylı ve koordineli gerçekleştirmek için Siber İstihbarat Başkanlığı adı altında yeni bir birim kurulması için çalışmalara başlanmıştır. 2023'te kurulan bu başkanlık, tehditlere karşı siber savunma kabiliyetini ve korunmayı artırmayı amaçlamıştır. (Kırbaşoğlu & Hasançebi, 2023).

Sonuç

21. yüzyılın bilgi ve akıl çağı olacağı açıktır. Her şeyin (silah, araba, şehir, ziraat…) akıllısı olacaktır. Teknolojik ve bilimsel istihbarat anlayışı ile aynı zamanda istihbaratın elde edilmesindeki hız da ön plana çıkacağından yapay zekâ kullanan sistemlere geçilmelidir. Bu anlamda, "büyük veri" toplamak kadar özellikle kamu kurumlarında ve devletin güvenlik ile ilgili kurumlarında kendi verilerimizi korumak da önemlidir. Hazırlanacak yapay zekâlı sistemler tanıma, teşhis, tespit ve hedefleme istihbaratı sağlamalıdır. Silah, araç ve sistemlerin yapay zekâlı hâle (otonom, tam otonom) getirilmesi için NATO ülkeleri ile ortak çalışmalar yapılmalıdır. Savaş alanında her sivil ve askerin bir toplama vasıtası olacağı teknolojiye dayalı bir sistem kurulmalıdır. Teknolojik istihbarata karşı koyma da çok büyük önem arz etmektedir.

4.2.17. Stanislav MYŠIČKA[25]: *The PRC Military Base in Djibouti and China's Growing Security Presence in Africa*

The opening of the Chinese naval military base in Djibouti, first officially announced in 2015 (with the arrival of naval forces in July 2017), clearly symbolizes not only the growing security presence of the

[25] Asst. Prof. Dr., Department of Political Science, University of Hradec Králové, Czech Republic, ORCID: 0000-0002-4118-0007

People's Republic of China (PRC) on the African continent but also plays an important role in its evolving global security strategy. Unlike many logistical bases from Southeast Asia to West Africa, the Djibouti base is the PRC's first openly acknowledged military installation on foreign soil. This contribution examines the issue from the perspective of Chinese official discourse, utilizing reporting and commentary from state media outlets and state and party institutions regarding the negotiation and opening of the Djibouti base, as well as reactions to news reports about potential future bases. The goal is to present and analyse how China frames and understands the establishment of military bases (and, to a lesser extent, other support facilities) abroad. I will also focus on the part of China's discourse that compares its military bases to the extensive network of U.S. military installations across the globe, highlighting the differences emphasized by China. The Djibouti base, along with other, less significant logistical facilities, and how they are perceived by the PRC's key foreign policy decision-makers, are crucial for an overall assessment of contemporary Chinese foreign policy. Moreover, the insights gained from this analysis will provide new perspectives on the long-term changes in China's view of state sovereignty's importance and limitations, which is clearly visible in its growing security presence (and exposure) on the African continent. In the past decade or so, the PRC has significantly established firm security relations with many African governments, engaged in regional peacekeeping, boosted its military diplomacy and is selling significantly more weapons and military material to Africa than ever before.

Keywords: China, Djibouti, Africa, Military Base, Security

4.2.18. Marina GLASER[26]: *Peculiarities of the Influence of the Political and Informational "Landscape of Betrayal" on the Intensity of Internal Terrorist Activity in the Context of an External Conflict [The Case of Russia During the Special Military Operation (SMO)]*

With the launch of the SMO and the task of forming a national consensus around its goals, the problem of countering the use of the Internet by foreign intelligence services has become relevant for the Russian special services. However, here we are faced with a paradox. On the one hand, with over 100 million users, Russia is one of the largest social media markets in the world. More than seven out of ten Russians use social media, which is higher than the global social media average (Melkadze, 2024). According to Mediascope, which measures the audience of all media in Russia, users spend an average of about an hour on social networks. Of these, 43 minutes are devoted to the Russian platform VKontakte, which makes it the "first choice screen". VKontakte is becoming an important tool for everyday communication of both citizens and government agencies (Users Spend 10 Times More Time, 2024).

In 2024, Telegram became the main platform for news consumption in Russia: 20% of users read news

[26] Prof., National Research University, Higher School of Economics (HSE), Faculty of World Economy and World Politics, Department of International Relations, Moscow, Russia, E-mail: mglaser@hse.ru

in the app (From Which Forums, Blogs, Social Media, 2024). According to a study of the active audience of social networks in Russia, the number of authors in social media in Russia increased to 69 million in 2024. By March 2024, compared to March 2023, the volume of monthly content increased by 29%, and the number of monthly active authors increased by 9% (In Russia, the Number of Authors in Social Media Reached, 2024).

On the other hand, according to public opinion polls, television remains the main source of news for Russians. In March 2024, according to Levada Center, two-thirds of Russians (65%) noted television as their main source of news (The Role of Television and the Internet, 2024). According to the FOM agency, 75% of Russians watch television programs almost every day or from time to time during the week (News Information and Television How Russians Get, 2024). At the same time, its mention as a source of information has decreased from 90% in the early 2010s to 61% in 2021–2022 and 56% in 2024 (Time and Money, 2024).

Popularity of television as the main source of information is higher among older Russians (85%), with secondary education and below (69%); people who barely have enough for food (59%). Young Russians more often get news from alternative sources: social networks (57%), Telegram channels (43%) and online publications (39%). With higher education, people more often consume news from social networks, online sources and Telegram channels (43%, 38%, 30% respectively).

Contradiction

The number of authors on social networks in Russia grew in 2024, but the audience of readers of Telegram channels stabilized in 2023–2024 after a sharp increase in the spring of 2022. Independent bloggers and journalists are losing their audience.

Research Problem

On the one hand, the demand for social networks and messengers in Russia opens up broad prospects for intelligence and operational work for the special services of other countries. But in this case, their field of vision mainly includes young people (high recruitment vulnerability) and people with higher education, who have low recruitment vulnerability. The still high popularity of television as the main source of information among older people, people with secondary education and the “poor” (who do not use social networks) narrows the possibilities of foreign intelligence services and removes people with high recruitment vulnerability from their field of vision. As a result, in both the first and second cases, the scale of the recruiting contingent is significantly reduced while maintaining the key task of forming a “landscape of betrayal”.

Working Concepts

Recruitment vulnerability is the predisposition of a recruitment candidate to establish permanent

business relations with a foreign intelligence service or the totality of all motives, life circumstances and character traits of the object of recruitment interest that make it fundamentally possible for him to establish contact with a foreign intelligence service (Doronin, 2024).

Political and information landscape is the art of creating anthropogenic compositions using natural (community) and artificial (information technology) components.

“Landscape of betrayal” is a violation of trust, moral boundaries of the community, a transition to a different set of norms and values, a space of uncertainty, fear and general mistrust.

The political and informational “landscape of betrayal” is an anthropogenic composition that uses various websites, social networks and instant messengers as a “relief,” violations of collectively recognized community norms as a “climate,” traitors and recruiters as “water,” and a specific information system consisting of its interacting components as “flora and fauna.”

The Key Question is

How does the formation of a political and informational “landscape” of betrayal in social networks and messengers of the country (Russia) in the context of an external conflict affect the increase in the scale and potential of the recruiting contingent and the strengthening of terrorist destabilization?

Hypothesis

The political and informational “landscape of betrayal” formed by foreign intelligence services in the largest Russian-language social networks on the one hand increases the number of terrorist attacks, but on the other hand, has virtually no effect on the scale and potential of the recruiting contingent. The reasons are:

1. The peculiarities of recruitment vulnerability of candidates suitable for recruitment: youth, people with psychological characteristics, drug addicts and marginals, people with openly pro-Ukrainian/opposition views.

2. Socio-psychological taboos of violation of national collective identity and ontological security. There are no dynamic changes, polarization, internal conflict, or uncertainty in society, despite the external conflict. Therefore, citizens do not consider violation of loyalty to the authorities to be extremely important for society. And especially for young people with higher education. That is, for those who could become valuable agents with real or potential intelligence capabilities.

3. Political and social control. Security forces hold citizens accountable for saved images, publications or reposts, and the list of prohibited topics is constantly expanding.

It can be argued that the political and informational “landscape of betrayal” formed by foreign intelligence services in the largest Russian-language social networks doesn’t exist. The main goal of foreign intelligence services remains unachieved.

4.2.19. Zarina M. LAZAROVA[27]: *The Changing Architecture of Security: Zangezur Corridor's Economic Importance*

In a dynamically changing global order, the security architecture is increasingly linked to economic interests and strategic infrastructure projects. The Zangezur Corridor, situated in the heart of the South Caucasus, is emerging as a vital node connecting Azerbaijan with Nakhchivan and Türkiye, while holding the potential to transform trade routes between Europe and Asia. This corridor symbolizes broader geopolitical and economic trends that are reshaping paradigms of security and influence in the region. Its implementation enhances the region's importance as a transport hub and energy route, offering opportunities for connectivity and development. However, these prospects are closely tied to regional security complexities, where the interests of key global and regional players converge. The Zangezur Corridor highlights the delicate balance between fostering economic integration and addressing strategic interests, which underpins the evolving security framework in the region.

The opening of the Zangezur Corridor presents both significant opportunities and challenges, with broad geopolitical, economic, and security implications. Geopolitically, the corridor strengthens connectivity between Azerbaijan, its exclave Nakhchivan, and Türkiye, thus potentially fostering closer cooperation and integration among these nations. This enhanced connectivity could lead to a more unified and strategically cohesive bloc, with the potential to strengthen the regional influence of Azerbaijan and Türkiye. At the same time, the corridor's opening may alter regional dynamics, particularly concerning Armenia's position. Armenia, historically a key player in controlling critical transit routes, might perceive the Zangezur Corridor as shifting the balance of influence in the region. As such, the corridor could catalyze adjustments in Armenia's geopolitical and security strategies, including potentially reinforcing ties with Russia and Iran, each of which may hold differing views on the corridor's implications.

Economically, the Zangezur Corridor offers substantial potential for regional development and integration, particularly in the context of energy security and trade. The corridor could serve as a vital route for transporting Caspian energy resources to European markets, thereby supporting Europe's efforts to diversify its energy supply and reduce dependence on traditional transit routes. Additionally, the corridor holds the potential to boost trade, investment, and infrastructure development in the region. By connecting Central Asia, the South Caucasus, and Europe, the corridor could facilitate new business opportunities, enhance logistical capabilities, and promote regional economic growth. Investment in infrastructure, including new roads, railways, and energy pipelines, could foster greater economic interdependence and reduce the likelihood of conflict by creating shared interests among regional actors.

Despite its potential, the Zangezur Corridor's development introduces important security considerations. From a defense perspective, the corridor could allow for more efficient movement of personnel and

[27] Student, Rakovski National Defence College, E-Mail: z.lazarova@rndc.bg

resources between Azerbaijan and Nakhchivan, enhancing Azerbaijan's defense capabilities. However, this development may raise concerns in Armenia, which could view the loss of control over critical routes, particularly in the southern Syunik region, as a security threat. These changes could prompt Armenia to reassess its military strategies and potentially increase defeounse investments, particularly in areas adjacent to the corridor. In this context, the role of external actors, especially Russia, becomes increasingly significant. As a key regional power, Russia may need to play a mediating role, balancing the interests of Azerbaijan, Armenia, and other regional stakeholders. Russia's presence could be crucial in preventing escalation and maintaining stability, yet its involvement may complicate the management of competing interests.

In addition to conventional security concerns, the Zangezur Corridor introduces several hybrid threats, which encompass a range of non-traditional security challenges. With increased connectivity, the region becomes more vulnerable to cyberattacks, which could target the infrastructure that supports trade, energy flow, and regional stability. Cyber threats could disrupt economic activities and affect critical sectors such as energy, transportation, and communication. Furthermore, the heightened visibility of the corridor could attract the attention of terrorist organizations seeking to exploit the situation for ideological or political purposes. Terrorist groups could target infrastructure, transportation hubs, and energy pipelines to disrupt regional stability and provoke tensions among countries. These threats could be exacerbated by the underlying political and historical grievances in the region, creating opportunities for extremist groups to sow discord.

The introduction of the corridor could also lead to increased competition over narratives. Disinformation campaigns, particularly those aimed at distorting the economic or political impact of the corridor, could destabilize the region. Such campaigns might fuel nationalist sentiments or deepen existing divides, potentially leading to internal unrest. As the corridor's influence grows, the region may also face challenges related to migration. The improved connectivity might facilitate labor movement across borders, which could create economic opportunities but also raise concerns about irregular migration or human trafficking. The management of these migration flows will require coordinated regional policies to prevent potential security risks and ensure that migration becomes a source of regional development rather than instability.

On a broader scale, the Zangezur Corridor's strategic importance could position the South Caucasus as a critical node within the Middle Corridor, linking Asia and Europe. This shift could attract international attention from major global powers such as China, the European Union, and the United States, which are all working to strengthen connectivity across Eurasia. As global powers engage with the region to develop trade and energy routes, the geopolitical environment may become more complex, requiring nuanced diplomacy and the careful balancing of regional and global interests. External involvement, while beneficial for development, could also shift existing alliances and complicate the management of

regional relations.

In conclusion, the Zangezur Corridor represents a multifaceted opportunity for regional growth, economic integration, and energy diversification, but it also introduces a range of security challenges. While the corridor could enhance connectivity, promote economic development, and improve energy security, it is also likely to affect the geopolitical balance in the South Caucasus. Addressing the security challenges, particularly the risks associated with hybrid threats, terrorism, and cyberattacks, will require comprehensive regional cooperation and effective risk management. The success of the Zangezur Corridor will depend on the ability of all stakeholders to engage in constructive dialogue, foster cooperation, and navigate the complexities of regional and global security. A balanced and inclusive approach will be essential to ensure that the corridor serves as a catalyst for sustainable peace, stability, and prosperity in the South Caucasus and beyond.

Keywords: Zangezur Corridor, Caucasus, Azerbaijan, Europe-Asia Connectivity, Economic Security, Regional Security, Security Architecture

KAYNAKÇA / *BIBLIOGRAPHY*[28]

Ablon, L., Binnendijk, A., Hodgson, Q. E., Bilyana, L., Romanosky, S., Senty, D., Thompson, J. A. (2019). Operationalizing Cyberspace as a Military Domain: Lessons for NATO. Santa Monica, CA: RAND Corporation, 2019. https://www.rand.org/pubs/perspectives/PE329.html

Alberts, D. S., Garstka, J. J., Hayes, R. E. & Signori, D. A. (2001). *Understanding information age warfare*. McLean (VA): CCRP.

Almufareh, M. F., Kausar, S., Humayun, M., & Tehsin, S. (2024). A conceptual model for inclusive technology: advancing disability inclusion through artificial intelligence. *Journal of Disability Research*, 3(1), 1-11.

Ashraf, A. & F. Anastasia. (2004). *Terrorism and technology*. NATO Centre of Excellence Defence Against Terrorism, Ankara, Türkiye.

Baxter, D. J. (2017). E-governance and e-participation via online citizen budgets and electronic lobbying: Promises and challenges. *World Affairs*, 180(4), 4-24.

BBC. (8.11.2019). Fransa Cumhurbaşkanı Macron: NATO'nun beyin ölümü gerçekleşti. https://www.bbc.com/turkce/haberler-dunya-50342428

Beilenson, L. W. (1972). *Power through subversion (p. iii)*. Washington, DC: Public Affairs Press.

Bemis, B. M., & Arquilla, J. (2011). *Cooking up psychological operations: The ingredients of successful PSYOP*. Naval Postgraduate School.

Berger, P. and Luckmann, T. (1991). *The social construction of reality*. London: Penguin Books.

Bindt, P., Faesen, L., Farnham, N., Frinking, E., Klimburg, A., Rõõs, H., Rademaker, M. (2017). Cyber as a Domain Concept and Capabilities. *The Hague Centre for Strategic Studies*. https://hcss.nl/wp-content/uploads/2022/06/NATO-Cyber-as-a-Domain-HCSS-2017.pdf

Birsel, H. (2012). Başlangıçtan günümüze NATO sorunsalı "Madalyonun İki Yüzü". *SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi*, (25), 109-124.

Bozkurt, A., Hamutoğlu, N. B., Kaban, A. L., & Taşçı , G. (2021). Dijital bilgi çağı: Dijital toplum, dijital dönüşüm, dijital eğitim ve dijital yeterlilikler. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 7(2), 35-63.

Brzezinski., Z. (1997). *The Grand Chessboard: American Primacy and its geostrategic imperatives*. New York: Basic Books.

Carayannis, E. G., Askounis, D., Andoutropoulou, M., & Zotas, N. (2024). Leveraging AI for enhanced eGovernment: Optimizing the use of open governmental data. *Journal of the Knowledge Economy*, 1-36.

Chifu, I., & Simons, G. (2023). *Rethinking Warfare in the 21st Century: The Influence and effects of*

[28] Bildiri sahiplerinin ilettikleri kaynaklar tek başlık altında toplanmıştır.

&

The references provided by the paper authors have been compiled under a single heading.

the politics, information and communication Mix. Cambridge University Press.

Cooley, A., & Nexon, D. H. (2020). (No) Exit from liberalism?. *New Perspectives*, 28(3), 280-291.

Cox, R. (1981). Social forces, states and world orders: beyond international relations theory. *Millennium - Journal of International Studies*, 10(2), 128.

Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı (2020). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2020-2023. http://www.sp.gov.tr/tr/temel-belge/s/202/Ulusal+Siber+Guvenlik+Stratejisi+ve+Eylem+Plani+_2020-2023

Darıcılı, A. B. & Özdal, B. (2017). "Rusya Federasyonu'nun siber güvenlik kapasitesini oluşturan enstrümanların analizi", *Bilig*, 83, 121-146.

Desouza, K. C., Dawson, G. S., & Chenok, D. (2020). Designing, developing, and deploying artificial intelligence systems: Lessons from and for the public sector. *Business Horizons*, 63(2), 205-213.

Dilip, R., Manasa, M. G., Chandrashekhar, L., Nethravathi, H. M., Tejashwini, N., AnilKumar, K. B., & Pramanik, S. (2025). Using AI to Improve the Supply of Digital Government Solutions. In: *Planning Tools for Policy, Leadership, and Management of Education Systems* (pp. 155-184). IGI Global.

Dobbins, J., Cohen, R.S., Chandler, N., Frederick, B., Geist, E., DeLuca, P., Morgan, F.E., Shatz, H.J. and Williams, B. (2019). *Extending Russia*. Competing from Advantageous Ground, Santa Monica: RAND Corporation.

Doronin, A. (2024). Mass media in intelligence and counterintelligence. *Invisible Dimension*, (2), 3–23.

DSA (2022). The Digital Services Act package. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

Dyner, A. M. (2023) Russia Continuing Cyberthreats against NATO Countries Bulletin of the Polish. *Institute of International Affiairs*. No. 172 (2291). https://pism.pl/publications/russia-continuing-cyberthreats-against-nato-countries

Eiras, F., Petrov, A., Vidgen, B., de Witt, C. S., Pizzati, F., Elkins, K., ... & Foerster, J. (2024). Near to mid-term risks and opportunities of open source generative ai. arXiv preprint arXiv:2404.17047.

Ercolani, G. (2021). The anthropological gaze: deconstructing the security knowledge. *Κοινὴ . The Almanac of Philosophical Essays*, (pp-37-54).

Erdal, N., Filiz, M., & Budak, O. (2023). Kişilik özelliklerinin siber güvenlik algısı üzerine etkisi: Z kuşağı örneği. *Sinop Üniversitesi Sosyal Bilimler Dergisi*, 7(1), 643-670.

Erol, O., Şahin, Y. L., Yılmaz, E. ve Haseski, H. İ. (2015). Kişisel Siber Güvenliği Sağlama Ölçeği geliştirme çalışması. *International Journal of Human Sciences*, 12(2), 75-91. doi: 10.14687/ijhs.v12i2.3185.

Etzioni, O. "No, the experts don't think superintelligent AI is a threat to humanity". 15.12.2023 tarihinde https://www.technologyreview.com/2016/09/20/70131/no-the-experts-dont-think-superintelligent-ai-is-a-threat-to-humanity/ adresinden erişildi.

Euronews. (25.05.2017). Trump: 'NATO ülkeleri sorumluluklarını yerine getirmeli'. https://tr.euronews.com/my-europe/2017/05/25/trump-nato-ulkeleri-sorumluluklarini-yerine-getirmeli

European Commission. (2000). eEurope 2002: An information society for all. Office for Official Publications of the European Communities. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/55f8648e-281b-47a5-93f3-10018c147a5b/language-en

European Commission. (2021). 2030 Digital Compass: The European way for the Digital Decade. Office for Official Publications of the European Communities. Retrieved from https://op.europa.eu/en/publication-detail/-/publication/d4220021-8d20-11eb-b85c-01aa75ed71a1/language-en

European Commission. (2022, December 15). European Declaration on Digital Rights and Principles. Retrieved from https://digital-strategy.ec.europa.eu/en/library/european-declaration-digital-rights-and-principles

European Parliament and Council of the European Union. (2002). Directive 2002/58/EC of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Official Journal of the European Communities, L 201, 37–47. Retrieved from https://eur-lex.europa.eu/eli/dir/2002/58/oj

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. Retrieved from https://eur-lex.europa.eu/eli/reg/2016/679/oj

European Parliament. (2018). "European Parliament resolution of 12 September 2018 on autonomous weapon systems(2018/2752(RSP)". 16.12.2023 tarihinde https://www.europarl.europa.eu/doceo/document/TA-8-2018-0341_EN.pdf?redirect adresinden erişildi.

Flint, C. (2021). *Introduction to geopolitics*. Routledge.

FOM. (2024, November 29). News information and television: How Russians get news and which sources they trust most. https://fom.ru/SMI-i-internet/15104

Futureoflife.org. (2018). 09.12.2023 tarihinde https://futureoflife.org/recent-news/handful-of-countries-including-the-us-and-russia-hamper-discussions-to-ban-killer-robots-at-un/ adresinden erişildi.

Galimberti, U. (2011). *Psiche e techne – L'uomo nell'eta' della tecnica*. Milano: Feltrinelli.

Geertz, C. (1979). *The interpretation of cultures*. Basic Books.

Goldstein, J. A., Chao, J., Grossman, S., Stamos, A., & Tomz, M. (2024). How persuasive is AI-generated propaganda?. *PNAS nexus*, 3(2).

Gökmen, Ö. F., & Akgün, Ö. E. (2015). Bilgisayar ve öğretim teknolojileri eğitimi öğretmen adaylarının bilişim güvenliği bilgilerinin çeşitli değişkenlere göre incelenmesi. *Cukurova University Faculty of Education Journal*, 44(1), 61-84.

Grotius, H. (1967). *Savaş ve barış hukuku*. (S. L. Meray, Çev.). Ankara: Ankara Üniversitesi Basımevi.

Gümüş, N. (2020). Z kuşağı tüketicilerin satın alma karar tarzlarının incelenmesi. *Yaşar Üniversitesi E-Dergisi*, 15(58), 381-396.

Hacker, K. L., & van Dijk, J. (Eds.). (2000). *Digital democracy: Issues of theory and practice*. Sage.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/liebercode-1863 adresinden erişildi.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/oxford-manual-1880 adresinden erişildi.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/hague-rules-1923 adresinden erişildi.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/icrc-draft-rules-1956 adresinden erişildi.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 adresinde erişildi.

ICRC. "International humanitarian law databases" 16.12.2023 tarihinde https://ihl-databases.icrc.org/en/ihl-treaties/ccw-1980 adresinden erişildi.

IPSOS. (2019). 09.12.2023 tarihinde https://www.ipsos.com/sites/default/files/ct/news/documents/2019-01/human-rights-watch-autonomous-weapons-pr-01-22-2019_0.pdf adresinden erişildi.

Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, 27(4), 371-376.

JR., J. R. (2024, 10 24). The White House. Retrieved from Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence: https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-se

Kaku, M. (2019a). *İnsanlığın geleceği*. (A. C. Çevik, Çev.). Ankara: ODTÜ Yayıncılık.

Kaku, M. (2019b). *Geleceğin fiziği*. (Y. S. Oymak ve H. Oymak, Çev.). Ankara: ODTÜ Yayıncılık.

Kaku, M. (2019c). *Olanaksızın fiziği*. (E. Tarhan, Çev.). Ankara: ODTÜ Yayıncılık.

Kapsa, I. (2021). Analytical framework for researching citizen participation in the era of e-democracy. *Przegląd Europejski*, (4), 13-24.

Karacı, A., Akyüz, H. İ., & Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi*, 25(6), 2079-2094.

Karagöz, Y. (2019). *SPSS AMOS META Uygulamalı nitel-nicel-karma bilimsel araştırma yöntemleri*

ve yayın etiği. Ankara: Nobel Yayıncılık.

Karakaya, A., & Yetgin, M. A. (2020). Karabük Üniversitesi çalışnalarına yönelik kişisel siber güvenlik üzerine araştırma. *Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(2), 157-172.

Karasoy, A. & Babaoğlu, P. (2020). Türkiye'de Elektronik Devletten Dijital Devlete Doğru. *Karadeniz Sosyal Bilimler Dergisi*, 12(23), 397-416.

Karasoy, H. A. (2022, Mayıs). Yeni Nesil Savaş ve Siber İstihbarat. *Güvenlik Bilimleri Dergisi*, 223-240.

Kathuria, S., & Rana, S. (2023). Linking Customer E-Service Quality with Artificial Intelligence-Based Business Environment. In *Artificial Intelligence in Customer Service: The Next Frontier for Personalized Engagement* (pp. 259-279). Cham: Springer International Publishing.

Khatun, R., Bandopadhyay, T., & Roy, A. (2017). Data modeling for E-voting system using smart card based E-governance system. *International Journal of Information Engineering and Electronic Business*, 9(2), 45.

Kırbaşoğlu, F. & Hasançebi, M. (2023). Siber Güvenlik ve Siber İstihbarat Kavramları Üzerine Bir Değerlendirme. 6. International Scientific Researches and Innovation Congress, 318-322.

Lan, C. I. C., & Peng, L. P. (2018). E-participation, rural regime, and network governance: A case of Balien River conservation. *Sustainability*, 10(11), 3908.

Levada-Centre. (2024, April 18). The role of television and the Internet as the main sources of news and the top most popular Russian journalists. https://www.levada.ru/2024/04/18/rol-televideniya-i-interneta-kak-glavnyh-istochnikov-novostej-i-top-naibolee-populyarnyh-rossijskih-zhurnalistov/?Utm_source=mailpoet&utm_medium=email&utm_source_platform=mailpoet&utm_campaign=newsletter-post-title_81

Liebetrau, T. (2022). Organizing cyber capability across military and intelligence entities: collaboration, separation, or centralization. *Policy Design and Practice*, 6(2), 131-145. https://doi.org/10.1080/25741292.2022.2127551.

Lonsdale, D. J. (1999). Information power: Strategy, geopolitics, and the fifth dimension. *The Journal of Strategic Studies*, 22(2-3), 137-157.

Machiavelli, N. ([1532] 2019). *II Principe.* Torino: Einaudi.

McDonald, Coby (2015): The Good, the Bad and the Robot: Experts are trying to make machines be "Moral". 10.12.2023 tarihinde https://alumni.berkeley.edu/california-magazine/online/good-bad-and-robot-experts-are-trying-make-machines-be-moral/ adresinden erişildi.

Mead, M., & Métraux R. (2000). *The study of culture at a distance*. Berghahn Books.

Mearsheimer, J. J., & Walt, S. M. (2016). The case for offshore balancing: A superior US grand strategy. *Foreign Aff.*, 95, 70.

Melkadze, A. (2024, December 12). Number of social network users in Russia from 2020 to 2029 (in millions). *Statista*. https://www.statista.com/statistics/569043/predicted-number-of-social-network-users-in-russia/

85

Meydan, C.H. ve Şeşen, H. (2015). *Yapısal eşitlik modellemesi AMOS uygulamaları*. Ankara: Detay Yayıncılık.

Meyn, M. (2020). Digitalization and Its Impact on Life inRural Areas: Exploring the Two Sides of the Atlantic: USA and Germany. In: Patnaik, S.; Sen, S.; Mahmoud, M.S. (eds.). *Smart Village Technology: Concepts and Developments*. Cham, 99.116.

Microsoft Digital Defense Report (2024) The foundations and new frontiers of cybersecurity.

Microsoft Threat Intelligence Overview. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

Miron, M., Thornton, (2022). Winning Future Wars: Russian Offensive Cyber and Its Vital Importance: in Moscow's Strategic Thinking. *The Cyber Defense Review*, 7(3), 117-135. https://cyberdefensereview.army.mil/Portals/6/Documents/2022_summer_cdr/CDR_V7N3_Summer_2022-SE-WEB-1.pdf?ver=oDnMjK7AGrLLtmFJPHUwxQ%3d%3d

Miron, M., Thornton, R. (2024). The use of cyber tools by the Russian military: Lessons from the war against Ukraine and a warning for NATO? *ACIG*, 3(1), 2-22. DOI: 10.60097/ACIG/190142

Mordorintelligence (2023): "Military Robots Market Size & Share Analysis-Growth Trends and Forecasts (2023-2028)". 17.12.2023 tarihinde https://www.mordorintelligence.com/industry-reports/military-robot-market#:~:text=Military%20Robots%20Market%20Analysis,period%20(2023-2028) adresinden erişildi.

Mum, A. (2016). *The Role of Counter Terrorism in Hybrid Warfare*. NATOs Centre of Excellence for Defence Against Terrorism (COE DAT).

Musiał-Karg, M., & Kapsa, I. (2019). Citizen e-participation as an important factor for sustainable development. *European Journal of Sustainable Development*, 8(3), 210-210.

Nair, A., Sadasivan, R., & Krishnan, A. (2019). Winning the talent game: HR gamification experience for Generation Z. *International Journal on Leadership*, 7(1), 44-49.

Naldi, L., Nilsson, P., Westlund, H., & Wixe, S. (2015). What is smart rural development?. *Journal of Rural Studies*, 40, 90-101.

NATO (2020): "Science & Technology Trends2020-2040". 11.12.2023 tarihinde https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf adresinden erişildi.

NATO Centre of Excellence Defence Against Terrorism (COE-DAT). SOF Roles in Crisis/CT Management Seminar, 6-8 July 2022.

NATO Centre of Excellence Defense Against Terrorism (COE-DAT). Crisis Management in Terrorism. Seminar Report, 09-10 December 2019, Ankara, Türkiye.

NATO Centre of Excellence Defense Against Terrorism (COE-DAT). Terrorism Experts Conference & Executive Level Defense Against Terrorism Seminar (TEC 2020), 3-4 November 2020, Ankara, Türkiye.

NATO Centre of Excellence Defense Against Terrorism (COE-DAT). Terrorism Experts Conference

& Executive Level Defence Against Terrorism Seminar (TEC 2021), 12-13 October 2021, Ankara, Türkiye.

Neumann, T., & Jones, B. (2024). PRISM: A Design Framework for Open-Source Foundation Model Safety. arXiv preprint arXiv:2406.10415.

Niinistö, S. (2024). Safer together strengthening Europe's Civilian and Military Preparedness and readiness. https://commission.europa.eu/document/download/5bb2881f-9e29-42f2-8b77-8739b19d047c_en?filename=2024_Niinisto-report_Book_VF.pdf

North Atlantic Treaty Organization. (2019). AJP-3 Allied Joint Doctrine for the Conduct of Operations, Edition C Version 1. https://www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

North Atlantic Treaty Organization. (2022a). NATO 2022 Strategic Concept. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

North Atlantic Treaty Organization. (2022b). AJP-01 Allied Joint Doctrine, Edition F Version 1. https://www.cimic-coe.org/resources/external-publications/ajp-01-edf-v1-f.pdf

North Atlantic Treaty Organization. (2023a). AJP-10.1 Allied Joint Doctrine for Information Operations, Edition A Version 1. https://nso.nato.int/nso/nsdd/main/standards?search=information%20operations

North Atlantic Treaty Organization. (2023b). AJP-10 Allied Joint Doctrine for Strategic Communications, Edition A Version 1. https://nso.nato.int/nso/nsdd/main/standards?search=strategic%20communications

Nunnally, J. C. (1978). *Psychometric theory*. (2nd Ed.). McGraw-Hill, New York.

Özcan, A.N. (13.01.2015). Avrupa Birliği'nin istihbarat örgütü kurma arayışı. *Milliyet Gazetesi*. https://www.milliyet.com.tr/yazarlar/nihat-ali-ozcan/avrupa-birligi-nin-istihbarat-orgutu-kurma-arayisi-1997738

Pavlova, E. (2020). Enhancing the organisational culture related to cyber security during the university digital transformation. *Information & Security*, 46(3), 239-249.

Pernik, P. (Edt.) (2022). *Cyberspace Strategic Outlook 2030 Horizon scanning and analysis*. NATO CCDCOE Publications. https://ccdcoe.org/uploads/2022/03/Horizon_Scanning_vol2_15032022.pdf

Polat, D. Ş. (2020, Şubat). NATO'nun yeni operasyon alanı: Siber uzay. *Güvenlik Bilimleri Dergisi*, 135-158.

Pöysti, T. (2018). Trust on digital administration and platforms. *Scandinavian Studies in Law*, 65, 321-363.

Prizzi, F. (2021). Cultural ıntelligence ed etnografia di guerra – il ruolo dell'antropologia nello studio dell'ınformation warfare di Al Shabaab. Edizioni Altravista.

Prizzi, F. (2023). *Kültürel istihbarat ve savaşın etnografisi*. Pankus Publishing House.

Prizzi, L. (2000). Le Operazioni di Sostegno della Pace 1982-1997 – il ruolo dell'Italia e del suo Esercito. Rivista Militare.

Qi, X., Zeng, Y., Xie, T., Chen, P. Y., Jia, R., Mittal, P., & Henderson, P. (2023). Fine-tuning aligned language models compromises safety, even when users do not intend to!. arXiv preprint arXiv:2310.03693.

Raja, D. S. (2016). Bridging the disability divide through digital technologies. *Background paper for the World Development report*, 1-35.

Ranchordás, S. (2022). The digitization of government and digital exclusion: setting the scene. In *The Rule of Law in Cyberspace* (pp. 125-148). Cham: Springer International Publishing.

RAND Corporation. (2021). Select RAND Research on the information environment: 2014-2020. https://doi.org/10.7249/CPA614-4.

Re: Russia. (2024, December 25). Time and money. https://e-vid.ru/tv-i-kino/251224/yaschik-dlya-deda-v-rossii-televidenie-teryaet-auditoriyu

Röttger, P., & Vedres, B. (2020). The information environment and its effects on individuals and groups. Oxford Internet Institute, University of Oxford. https://royalsociety.org/-/media/policy/projects/online-information-environment/oie-the-information-environment.PDF

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, 23(15), 1-20.

Scharre, Paul (2020): *İnsansız ordular-katil robotlar, otonom silahlar ve makine savaşları*. (K. A. Çetinalp, Çev.). İstanbul: Kronik Kitap.

Schmid, S., Riebe, T., & Reuter, C. (2022). Dual-use and trustworthy? A mixed methods analysis of AI diffusion between civilian and defense R&D. *Science and engineering ethics*, 28(2), 12.

Searle, J. R. (1996). *The construction of social reality*. London: Penguin Books.

Seger, E., Dreksler, N., Moulange, R., Dardaman, E., Schuett, J., Wei, K., ... & Gupta, A. (2023). Open-sourcing highly capable foundation models: An evaluation of risks, benefits, and alternative methods for pursuing open-source objectives. arXiv preprint arXiv:2311.09227.

Selva, G. P. (2018, June 21). U.S. must act now to maintain military technological advantage, Vice Chairman says. (J. Garamone, Interviewer)

Simons, G. (2021). Iran and Russia as objects and subjects of Western psychological operations and ınformation warfare. *Journal of Iran and Central Eurasia Studies*, 4(1), 109-127.

Simons, G. (2022). "Inevitable" and "Imminent" Invasions: The Logic Behind Western Media War Stories. *Journal of International Analytics*, 13(2), 43-58.

Singer, Peter Warren (2015): *Robotik savaş-21. yüzyıldaki robotik*. Devrim M. Erdemir ve T. Erdem Erdemir, Çev.). Ankara: Buzdağı Yayınevi.

Smeets, M. (2023). The challenges of military adaptation to the cyber domain: a case study of the Netherlands. *Small Wars & Insurgencies*, 34(7), 1343-1362. https://doi.org/10.1080/09592318.2023.2233159.

Statewatch. EU INTCEN. https://www.statewatch.org/media/documents/news/2016/may/eu-intcen-factsheet.pdf

Statista Research Department. (2024, November 4). From which forums, blogs, social media, and messengers do you usually read news, information reports? https://www.statista.com/statistics/1102127/russia-most-popular-social-media-for-news/

Stopkillerrobots.org (a): Problems with autonomous weapons. 29 Mart 2024 tarihinde https://www.stopkillerrobots.org/stop-killer-robots/facts-about-autonomous-weapons/ adresinden erişildi.

Stopkillerrobots.org (b): Spokes Persons. 29 Mart 2024 tarihinde https://www.stopkillerrobots.org/spokespersons/ adresinden erişildi.

Stopkillerrobots.org (c): Vision and Values. 29 Mart 2024 tarihinde https://www.stopkillerrobots.org/vision-and-values/ adresinden erişildi.

Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Proceeding of the 6th Global Summit on Education*, 1-14.

Tabachnick, B. G. ve Fidell, L. S. (2012). *Using multivariate statistics*. New Jersey: Pearson Education.

Taban, H. & Aydilek, E. (2023). Dijital Çağda İstihbarat Analizi. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 39-67.

TASS. (2024, April 24). In Russia, the number of authors in social media reached a record 69 million in March. https://tass.ru/obschestvo/20633509.

Tekerek, M., & Tekerek, A. (2013). A research on students' information security awareness. *Online Submission*, 2(3), 61-70.

The Association of Professional Users of Social Networks and Messengers. (2024, December 7). Users spend 10 times more time on VKontakte than on Instagram, Facebook, Likee and Twitter. https://appsim.ru/polzovateli-provodyat-v-vkontakte-v-10-raz-bolshe-vremeni-chem-v-instagram-facebook-likee-i-twitter/

Türkiye Siber Güvenlik Kümelenmesi (2023). Hakkımızda. https://siberkume.org.tr/hakkimizda.

United Nations Development Programme. (2020). Human development report 2020: The next frontier-Human development and the Anthropocene. United Nations. Retrieved from https://hdr.undp.org/en/2020-report.

Ünal, A. N., & Ergen, A. (2018). Siber uzayda yeterince güvenli davranıyor muyuz? İstanbul ilinde yürütülen nicel bir araştırma. *Manisa Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 16(2), 191-216.

Vičič, J., & Harknet, R. (2024). Identification-imitation-amplication: understanding divisive influence campaigns through cyberspace. *Intelligence and National Security*, 39(5), 897-914. https://doi.org/10.1080/0268427.2023.2300933.

Wang, Y., & Chen, D. (2018). Rising sino-US competition in artificial intelligence. *China Quarterly of International Strategic Studies*, 4(2), 241-258.

Welby, B. and Hui Yan Tan. (2022). Designing and delivering public services in the digital age, *OECD Going Digital Toolkit Notes*, 22, Paris: OECD Publishing. https://doi.org/10.1787/e056ef99-en

Western, J. (2005). *Selling intervention and war: The presidency, the media, and the American public*.

JHU Press.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment?. *Computers in Human Behavior*, 84, 375-382.

Yılmaz, B. A. (2020). Siber terörizm ve değişen istihbarat anlayışı. *Anadolu Strateji Dergisi*, 1(1), 65-82.

Yılmaz, S. (2022). Anka Enstitüsü. http://ankaenstitusu.com/akilli-istihbarat/

Yiğit, M. F., & Seferoğlu, S. S. (2019). Öğrencilerin siber güvenlik davranışlarının beş faktör kişilik özellikleri ve çeşitli diğer değişkenlere göre incelenmesi. *Mersin Üniversitesi Eğitim Fakültesi Dergisi*, 15(1), 186-215.

Zissis, D., & Lekkas, D. (2011). Securing e-government and e-voting with an open cloud computing architecture. *Government Information Quarterly*, 28(2), 239-251.

Zoja, L. (2017). *Paranoia-the madness that makes history*. London and New York: Routledge.

Zollmann, F. (2017). *Media, propaganda and the politics of intervention*. Peter Lang.

FOTOĞRAFLAR / *PHOTOGRAPHS*


ULUÇ ÖZÜLKER
CHRISTOPHER FARRANDS


PERSPECTIVE
POLAND – EUROPE - NATO
I. GEOPOLITICAL CONTEXT– STRATEGIC POSITION
*NATO/ UE border
*Border neighborhood Belarus, Ukraine, Baltic States
Polish -Belarusian border
Polish -Ukrainian border
II. NATO MILITARY PRESENCE IN POLAND
III. The Importance of Poland on NATO's Eastern Flank
IV. Polish support for Ukraine
V. The consequences of war in Ukraine for Poland / polish foreign policy
North Atlantic Treaty Organization (NATO)
NWEGEO
İSTANBUL
BEYKENT ÜNİVERSİTESİ
BEYKENT ÜNİVERSİTESİ


1. OTURUM
2. OTURUM
3. OTURUM
4. OTURUM
5. OTURUM
6. OTURUM


Geri Dönüşü...
MASAÜSTÜ
1. OTURUM
2. OTURUM
3. OTURUM
4. OTURUM
5. OTURUM
6. OTURUM
Yeni klasör

İSTANBUL BEYKENT ÜNİVERSİTESİ

Ayazağa - Maslak Yerleşkesi
Ayazağa - Sarıyer / İST. Faks: 0 (212) 289 64 90

Beylikdüzü Yerleşkesi
Beykent - Büyükçekmece / İST. Faks: 0 (212) 872 28 30

Hadımköy Yerleşkesi
Akçaburgaz Mevkii - Esenyurt/İST

Taksim Yerleşkesi
Sıraselviler - Beyoğlu / İST. Faks: 0(212) 243 02 78

İstanbul Beykent Üniversitesi Çağrı Merkezi
beykent.edu.tr-info@beykent.edu.tr
444 1997

/BeykentUnv /BeykentUnv /BeykentUnv /BeykentUnv /İstanbul Beykent Üniversitesi