OAFLMUN’26

STUDY GUIDE

NATO

TABLE OF CONTENTS

I. **Letters……..**

1. Letter from the Secretary-General

2. Letter from the Under Secretary-General

3. Letter from the Academic Assistant

II. **Introduction to the Committee……...**

1. North Atlantic Treaty Organization (NATO)

2. History

3. Scope

III. Introduction to the Agenda Item……

1. The Integration of Artificial Intelligence in Modern Military Operations

1.1 Comprehensive Definition of Offensive Cyber AI Operations

1.1.1 Terrorist Networks

1.1.2 Hybrid Warfare

1.2 Predictive AI Targeting Systems

1.3 AI/ML Challenges for Target Recognition and Identification

2. Ethical and Operational Concerns for AI-Assisted and Autonomous Systems

IV. NATO's Strategic and Technological Framework……..

1. Cyberspace as an Operational Domain

1.1 Rules of Engagement in a Non-Kinetic Battlespace

1.2 Integration into Collective Defense Structures

2. NATO Cyber Defence Policy

2.1 Balance Between Collective Security and National Sovereignty

2.2 Early Cyber Defence Initiatives (Before 2010s)

3. Adoption of NATO AI Strategy (2021)

3.1 Emerging and Disruptive Technologies (EDTs)

3.2 NATO's Ethical and Policy Guidelines for AI

VI. Legal and Ethical Matters…….

1. Accountability and Responsibility

1.1 Appropriateness of Systems and Weapons According to Their Levels of Autonomy

1.1.1 Lethal Autonomous Weapons (LAWs)

1.1.2 Swarm Drones

2. Civil Liberties and Data Ethics

VII. Operational and Strategic Risks……...

1. Potential Civilian Harm and Collateral Damage

1.1 Risks of Misidentification in Targeting

1.2 Amplification of Civilian Exposure in Data-Based Operations

1.2.1 Civilian Data-Overload

2. Alliance Cohesion and Policy Divergence Among NATO Member States

VIII. Case Studies……

1. Case Studies of AI in Cyber Operations

1.1 NATO's Assistance for Cyber Efforts to Combat ISIS/DAESH

1.2 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

1.3 Allied Cyber Operations Centre (ACO) Coordination

2. Case Studies for Predictive AI Targeting Systems

2.1 NATO’s NEC (Network-Enabled Capability) Exerci

2.2 Defense Advanced Research Projects Agency (DARPA) Target Prediction Algorithms Development

3. Case Studies for Operational Risks

3.1 NSA Mass Surveillance Revelations (2013)

3.2 Cambridge Analytica Scandal (2018)

IX. Questions to be Addressed……...

X. Further Reading……..

XI. References……..

I. Letters

1. *Letter from the Secretary-General*

Dear Participants of OAFLMUN'26,

It is my pleasure to announce OAFLMUN'26. First and foremost, I would like to express my sincere gratitude to everyone who has given their utmost effort in organising this conference. As the Secretary-General of this conference, I am truly delighted and honoured to welcome you all. Our conference will be held at Özkent Akbilek Science High School from April 24th to April 26th.

Allow me to briefly introduce myself. My name is Ecrin İrem Gültop, and I am currently an 11th-grade student at Özkent Akbilek Science High School. I have been participating in Model United Nations conferences since December 2022. Throughout these experiences, I have witnessed genuine friendships, effective crisis management, proper approaches to diplomacy, and, undoubtedly, true leadership. Now, it is my turn to help a new generation of participants experience these remarkable opportunities.

The 2026 edition of OAFLMUN will host the following committees: NATO, HCC, UNWOMEN, JCC, UNSC, UNICEF, UNODC, and DISEC. I look forward to welcoming you all to an unforgettable conference experience where diplomacy, leadership, and collaboration will truly come to life.

Yours sincerely,

Ecrin İrem Gültop
Secretary-General of OAFLMUN'26

2. *Letter from the Under Secretary-General*

Dear Distinguished Delegates and Participants,

It is my great pleasure to welcome all of you to this edition of OAFLMUN'26, to the North Atlantic Treaty Organization Committee, as the Under Secretary-General. My name is İpek Dal, and I am a tenth-grade student at Ozel Buyuk Science High School. I am truly honoured to be part of this conference and to guide you through this intellectually engaging journey.

In this committee, you will have the opportunity to discuss highly relevant and evolving issues international security. Our agenda will focus on the implications of offensive cyber AI operations within the broader context of hybrid warfare, as well as the delicate balance between collective security and national sovereignty within NATO. These topics, while sometimes overlooked in everyday discussions, are becoming increasingly critical in shaping the future of global stability. As delegates, you will be responsible for addressing these challenges with thoughtful analysis, strategic thinking, and effective diplomacy. I would also like to express my gratitude to the person or people who made this possible. I would like to thank Ezgi Çimen, who was there whenever I needed help.

Finally, as delegates of the NATO Committee, I hope you have fun and make the most out of this experience. I hope that all of you will engage fully with the committee and really make the most out of the experience. I encourage each of you to read the study guide provided, as well as supplement that with further research. Please do not hesitate to contact me at ipekdal2424@gmail.com .

I look forward to seeing you all and witnessing your diplomacy in action.

Sincerely,

İpek Dal

Under Secretary-General of the NATO Committee

3. *Letter from the Academic Assistant*

Esteemed Delegates and Participants,

Welcome to OAFLMUN'26. I am Ezgi Çimen, a tenth-grade student at Mehmet Emin Resulzade Anatolian High School. I will be serving as your Academic Assistant for the committee throughout the conference. I am honored to write this letter to you all. I hope this conference brings you both joy and valuable experience. Through this conference, I believe you will expand your knowledge and deepen your curiosity about MUN conferences.

I would like to extend my special thanks to a few people. First, I am deeply grateful to İpek Dal. She is a wonderful friend and an incredible person, and I cherished every moment we worked together. I would also like to thank my dear friend Göknur Engin for supporting me during difficult times; through her, I found not only a mentor but also a lifelong sister. Taha, thank you for being by my side. Last but not least, I would like to thank my family, the person who influences me my dear mother, my biggest supporter my sister, my grandfather and Cem. I am sincerely thankful for their constant support in every aspect of my life, and I owe them a great deal.

I would also like to thank the delegates reading this guide. Without your participation, this guide would not exist. So, thank you to everyone I have mentioned, as well as those I may not have been able to name. With everyone's endless support, I have been able to write this letter.

I wish all my dear delegates a wonderful conference and fruitful debates. If you have any further questions, please feel free to contact me at ezgicimen10@gmail.com.

Sincerely,

Ezgi Çimen

Academic Assistant of the NATO Committee

II. INTRODUCTION TO THE COMMITTEE

1. North Atlantic Treaty Organization (NATO)

The North Atlantic Treaty Organization (NATO) is an intergovernmental military and political alliance that was created in 1949, with the founders being the United States, Canada, and several Western European nations. The main purpose of the alliance was to provide collective security against the Soviet Union. NATO served as a deterrent to the Soviet Union's threat during the Cold War. Following the fall of the Warsaw Pact and the Soviet Union, the alliance persisted and took part in military operations in the Middle East, South Asia, Africa, and the Balkans. (NATO Organization, 2025)

2. History

The North Atlantic Treaty Organization (NATO) was established in 1949, shortly after World War II, when Europe was devastated and politically unstable. As tensions between the United States and the Soviet Union increased, the world entered an atrocious period, the Cold War. Many Western European countries were threatened by the spread of communism and the growing military power of the Soviet Union. In response, twelve countries, which are Belgium, Canada, Denmark, France, Iceland, Italy, Luxembourg, the Netherlands, Norway, Portugal, the United Kingdom, and the United States, signed the Washington Treaty on April 4, 1949, and created NATO as a collective defense alliance. The main idea behind NATO is that considering an attack made on a Member State is the same as considering an attack made on all the Member States, collectively, to NATO. This principle, known as Article 5, became the foundation of the alliance and aimed to prevent war through deterrence. During the Cold War, NATO mainly focused on defending the members against a possible Soviet invasion and maintaining military balance in Europe. After the Cold War ended in 1991 and the Soviet Union collapsed, NATO had to redefine its role. The alliance began addressing new emerging global challenges such as terrorism, ethnic conflicts, cyber threats, and regional instability. NATO expanded its membership to include countries from Central and Eastern Europe. The organization continues

to adapt to emerging security challenges and maintains its commitment to protecting the freedom and security of the member states.

3. Scope

The North Atlantic Treaty Organization (NATO)'s main purpose is to safeguard the freedom and security of all its members. Its essential principle is to sustain the safety of its member countries. This principle encourages cooperation among the members to bear the duty of safeguarding each other during any attack, risk, terrorism, etc., to maintain the peace in Europe and North America. NATO calls this cooperation collective defence.

III. INTRODUCTION TO THE AGENDA ITEM

1. The Integration of Artificial Intelligence in Modern Military Operations

As emerging technologies continue to reshape modern warfare, Artificial Intelligence (AI) has become increasingly integrated into NATO's military and cyber operations. AI/ML is increasingly used in various military domains and in support of various processes, e.g., Intelligence, Surveillance and Reconnaissance (ISR), Command and control (Observe/Orient/Decide/Act - OODA loop), or Targeting (e.g., Find, Fix, Track, Target, Engage, Assess – F2T2EA processes). In particular, AI/ML techniques provide advanced automated support for ISR data collection from heterogeneous sources, support to the PED (process, exploit, disseminate) process in terms of target detection/recognition/identification, multisensory data fusion and analytics from physics-based multimodality sensors and human-generated sources for intelligence production and situational understanding, as well as dynamic battle management and response. On the one hand, AI-based machine learning algorithms, assessment tools, and automated support systems offer opportunities to improve the efficiency and flexibility of NATO's operational framework. As the Alliance develops its defense capabilities, AI plays a key role in shaping future military strategies and doctrines. However, the Alliance must ensure it uses AI in a way that is consistent with its values.

On the other hand, the use of AI in military and cyber operations raises concerns about accountability and transparency. In short, while AI provides the conveniences and opportunities for NATO operations, the legal and ethical status of AI-based systems is still up for discussion.

1.1 Comprehensive Definition of Offensive Cyber AI Operations

Offensive Cyber AI Operations are the use of AI technologies to conduct proactive and targeted actions in cyberspace. The goal is to disrupt, degrade, manipulate, or gain unauthorized access to digital systems, networks, or data. These operations stand apart from traditional cyber operations because they employ AI-driven systems. These systems can recognize vulnerabilities, adjust to defenses, and perform cyber actions quickly and independently, without human oversight at every step. These operations may involve automated intrusion techniques or intelligent malware deployment. Shortly, Offensive Cyber AI Operations bring together the strategic objectives of offensive cyber warfare with the intelligent and adaptable capabilities of Artificial Intelligence.

Although Offensive Cyber AI Operations are currently not fully implemented against non-state actors, they will be in the near future. These operations are a deal because they use Artificial Intelligence to make decisions and take actions without a human being telling them what to do.

1.1.1 Terrorist Networks

Cyber operations are used in activities such as disrupting the communication networks of terrorist organizations (such as ISIS), dismantling their propaganda systems, and tracking their financial flows. In these operations, AI-powered analysis systems (e.g., pattern recognition, network mapping) are actively used. However, “fully autonomous AI (capable of launching attacks)” is neither widespread nor officially recognized.

Such operations are conducted in accordance with International Humanitarian Law (IHL) (particularly the law of armed conflict), NATO regulations, and the domestic laws of member

states. This is because the principles of proportionality and distinction must be strictly observed.

1.1.2 Hybrid Warfare

Within the framework of hybrid warfare, NATO relies more on the integration of artificial intelligence into offensive cyber operations. In modern conflict areas, cyber capabilities are used not only for defense but also for measures such as disruption, denial, and degradation of enemy systems. This is particularly crucial in operations targeting non-state actors, such as ISIS, where AI-supported tools make it easier to analyze data, map networks, and prioritize targets. This allows for the identification and dismantling of digital communication and propaganda infrastructures. However, such offensive capabilities are not conducted directly by NATO itself; instead, member states use their own cyber assets to do so, with NATO providing strategic coordination and guidance. International law, particularly the principles of proportionality and distinction, limits these operations, and AI remains primarily a decision-support tool. Human oversight is still essential.

1.2 Predictive AI Targeting Systems

Predictive AI targeting systems are advanced technologies that use artificial intelligence to analyze large datasets and anticipate potential threats before they fully emerge. Instead of only reacting to attacks, these systems aim to support proactive and preventive military strategies.

These systems operate by integrating data from multiple sources, including satellites, drones, surveillance systems, and digital communications. The AI processes this information to identify patterns, detect anomalies, and recognize behaviors that may indicate a future threat. For instance, repeated or unusual activity in a specific location, when compared with past incidents, may be flagged as a possible target. There are several key types of predictive AI targeting systems: *Pattern recognition systems* focus on analyzing historical data to identify recurring trends associated with threats. *Real-time surveillance systems* continuously monitor

live data and update risk assessments instantly. *Decision-support systems* assist human operators by providing target suggestions and risk evaluations, while leaving the final decision-making process to humans.

Such systems are increasingly relevant for organizations such as NATO, as they enhance situational awareness and enable faster, more informed responses. However, their use also raises important concerns regarding accuracy, potential bias in algorithms, and the issue of accountability if incorrect predictions lead to harmful outcomes.

In summary, predictive AI targeting systems represent a significant shift toward more anticipatory forms of defense. While they offer clear strategic advantages, their implementation must be carefully managed to ensure ethical and responsible use.

1.2.1 AI/ML (Machine Learning) Challenges for Target Recognition and Identification

Although automatic target recognition is a well-established research field, important challenges remain, as highlighted by recent studies on AI-enabled detection and identification systems. While AI and machine learning perform strongly when classifying targets with clear and well-defined signatures, their accuracy can decrease in more complex and dynamic environments, which limits effective situational awareness.

A key issue is the need for high-quality and diverse datasets. AI systems rely on large amounts of labelled data, but in military contexts, such data is often limited or incomplete. For example, studies within NATO research programs have emphasized that insufficient or unbalanced datasets can significantly reduce classification accuracy. To address this, researchers increasingly use synthetic data generated through advanced 3D modeling and simulation. Evidence shows that combining real and synthetic data, along with transfer learning, improves model performance and generalization.

Challenges also arise in detecting small objects in aerial imagery, such as distinguishing drones from birds. This has been observed in multiple real-world operations, where surveillance systems struggled to correctly identify low-signature aerial objects. As a result, techniques like super-resolution are required to enhance image quality and improve detection reliability.

In addition, combining data from multiple sources remains complex. Effective multimodal data fusion depends on selecting the appropriate level of integration (pixel, feature, or decision level). For instance, intelligence operations often combine satellite imagery, sensor data, and human reports; however, inconsistencies between these sources can lead to conflicting assessments.

Another critical concern is uncertainty. AI predictions are not always fully reliable, which makes it essential to measure and manage uncertainty in classification results. Past cases have shown that over-reliance on AI-based predictions can lead to misidentification of targets, raising ethical and operational risks. Although methods such as hard and soft data fusion – integrating sensor-based and human-generated information – have advanced, ensuring accurate and trustworthy intelligence for decision-making remains a significant challenge.

2. Ethical and Operational Concerns for AI-Assisted and Autonomous Systems

Artificial intelligence (AI) is one of the main drivers for innovation within different industries, and autonomous systems have attracted a lot of attention recently. Autonomous systems that rely on AI (Artificial Intelligence) today exist in many different domains, including self-driving cars, autonomous drones, robotics, and smart personal assistants (e.g., Alexa and Google Home) that can all independently complete tasks without humans physically or directly controlling the system. However, for autonomous systems to increase in performance, there are still several difficulties and issues that need to be solved, mainly related to how the system processes different kinds of data generated from multiple sources of information in real-time, and how to ensure that autonomous actions completed by the system will always be safe and successful. This challenge is particularly significant when it comes to the integration of AI systems into autonomous vehicles such as self-driving cars, which will require making tough decisions extending beyond data collected historically. Challenges also include how to manage the large amounts of data generated from a variety of sources and having assurances regarding the quality of this data, as well as how to integrate and process different data streams appropriately.

IV. NATO's Strategic and Technological Framework

1. Cyberspace as an Operational Domain

In recent years, NATO has recognized cyberspace as an operational domain, on a par with land, air, space, and sea. Cyberspace is composed of digital systems, including the internet, computer systems, embedded computers, and networked devices ('IoT') that support increasingly complex operations in all domains. They enable communication, information sharing, logistics coordination, and the planning and direction of armed forces. Cyber space, however, is a highly threatened environment as States and Non-State Actors seek to steal, manipulate, or destroy information, disable critical functions of governments and companies, and disrupt ways of life. The characteristics of the cyber space operational environment—Stateless, Anonymous, Dynamic— present significant challenges to the deterrence, defense, and response of cyber threats. But NATO has taken a cyber-centric approach to enhancing cyber capabilities, improving the cyber resilience of its stakeholders, and fostering a culture where cyber is integrated into all aspects of military planning. This approach includes deterring, defending against, and deciding how to respond to cyber threats.

1.1 Rules of Engagement in a Non-Kinetic Battlespace

Formulating rules of engagement (ROE) in cyberspace has unique characteristics due in large part to the non-kinetic and potentially transformative nature of cyber operations, even those conducted in support of conventional operations. In essence, ROE in cyberspace differ from those in the traditional domain, not only due to differences in how harm is inflicted and observed but also as a result of the distinct, potentially far-reaching strategic, societal and operational consequences of cyber activities. The application of NATO's collective defense commitment, Article 5, in light of contemporary cyber threats is still evolving and is particularly predicated on a clear and mutual understanding regarding what constitutes an armed attack in cyberspace. Challenges such as those associated with the capability to attribute authorship for cyber attacks add complexity to the challenge of formulating meaningful, yet

flexible rules of engagement, for both offensive and defensive cyber operations. Rules of engagement in cyber must reflect principles of proportionality, necessity, and legitimacy in application, and they must be operational rules that consistently meet the requirements of lawfulness under both NATO and international law. Further, cyber responses must be proportionate to any given cyber threat, with due consideration of the potential consequences to both the targeted adversary and Third Parties affected by the conflict. Of particular concern are those scenarios in which limited information exists regarding the very situation where restraint is least desired, and the risk of escalation is greatest.

Accordingly, the NATO Alliance must respond to growing challenges in cyberspace by establishing a more stable and defensive Cyber Rules of Engagement Framework in order to maintain safe and effective conduct of cyber operations.

1.2 Integration into Collective Defense Structures

The integration of cyberspace into NATO's defence and deterrence is one of the main developments in NATO's security and defence policy. Cyber threats can affect several Allies at the same time, thereby requiring a common response at the speed of information. The Alliance therefore strongly encourages Allies to build strong national cyber defences, enhance shared capabilities and mechanisms for information and best practice sharing, in order to foster collective resilience. With many cyber threats originating abroad, it is critical that Allies are able to share and analyse information and agree on a common response at speed and scale. Moreover, with cyber defence a core part of NATO's collective defence, a major cyber attack could, in certain circumstances, trigger a collective defence response, which in turn requires high levels of interoperability, information and intelligence sharing, and even trust between Allies. On a broader level, NATO cooperates with partners, industry, as well as global organisations, to tackle the cyber threats of today and tomorrow. In achieving integrated defence and deterrence, NATO engages in distributed training, joint planning and operations, as well as common doctrines, processes, and standards to ensure cyber defence is treated on par with other defence domains.

2. NATO Cyber Defence Policy

Cyber defence has become an important aspect of NATO's collective security and has even become an operational domain alongside land, air, and sea. NATO is committed to an active Cyber Defence, and its new Cyber Defence Policy reaffirms the alliance's role in this field and its commitment to defence against cyber attacks. The policy emphasizes the importance of collective defence under Article 5, which would be invoked in the case of a significant cyber attack. NATO will focus on building and maintaining cyber defence capabilities that are compatible with those of its partners, enhancing interoperability, increasing cooperation between governments, international organizations, and industry to foster greater resilience in the face of significant cyber threats against the critical information infrastructure of its nations. NATO's defence in cyberspace is defensive but dynamic, employing the latest technologies and innovations, such as AI and machine learning, to detect and deter cyber threats. Additionally, all NATO operations in cyberspace are conducted in accordance with international law and in respect for state and regional security, including sovereignty and proportionality.

NATO's Cooperative Cyber Defence Centre of Excellence in Estonia conducts strategic research and development, as well as practical training, aimed at improving the cyber defence capabilities of all nations, enabling them to deal with the rapidly evolving threats in the cyber domain.

2.1 Balance Between Collective Security and National Sovereignty

Collective security is a fundamental principle of NATO, which requires extensive cooperation and integration among its member nations. This increased cooperation, however, can be at odds with the pursuit of national sovereignty, particularly in cyber affairs. While Article 5 of the North Atlantic Treaty binds NATO member nations together in mutual defence, there is evidence that nations are reluctant to fully activate collective behaviour in the face of cyber threats. According to the European Union Agency for Cybersecurity (ENISA), cyber-attacks against critical information infrastructures have been on the rise, demanding a common

European, if not even global, defence strategy among nations. However, the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) has demonstrated that intelligence-sharing between NATO nations is very limited, due to the risk of revealing national vulnerabilities and core strategic assets.

Our analysis also reveals that nationally controlled Cyber Incident Response Programmes typically offer the fastest response in the first year, with responses that improve over time through multilateral cooperation. As a result, a trade-off typically exists between efficiency and national control, prompting some to argue that efficiency should be the guiding principle. Yet, as a consensus-based, voluntary coalition, NATO does not subscribe to this view, instead choosing a model that accommodates varying degrees of sovereignty over individual assets, while maximising collective situational awareness and security through data- and exercise-sharing. This balanced approach is essential to securing the cooperation of individual member states and meeting alliance objectives, and reflects a nuanced appreciation for the importance of strategic autonomy.

2.2 Early Cyber Defence Initiatives (Before 2010s)

Before the 2010s, NATO slowly began to acknowledge cyberspace as a strategic area of concern. In the early 2000s, its efforts focused on defensive cybersecurity to protect its networks. Initially, its cyber defence efforts were restricted to its own communication and information systems. However, as it became increasingly reliant on digital networks to facilitate its military planning, coordination, and intelligence sharing, these very networks became potential targets for cyberattacks. Accordingly, the Alliance invested in cybersecurity measures to defend its information systems and technologies.

It was a cyberwar against Estonia in 2007 that made the world realize the enormous scale of the impact that a cyber attack could have on a country’s critical information infrastructure (CII), including sectors like banks, mass media, public services, and governance. While NATO itself was not a target of the attack, the conflict highlighted serious concerns for the security of the Alliance’s member countries and showcased the challenges that security forces and

governments might face in addressing threats in cyberspace. NATO therefore proceeded quickly to develop an articulated cyber defence policy and strategy.

One of the key results of this period was the establishment in 2008 of the Cooperative Cyber Defence Centre of Excellence in Tallinn. In addition to this, NATO adopted its first Cyber Defence Policy in 2008, laying out the protection of its critical information systems, effective management of cyber incidents, and cooperation between nations as its core goals. During this period, NATO was generally responsible for cyber defence at the national level, with a supporting and coordinating role.

Although the cyber defence efforts undertaken before the 2010s were relatively limited in scope, they laid an important foundation for the recognition of cyberspace as an operational domain by NATO in the 2010s. These efforts helped shape the Alliance's overall cyber defence strategy and laid the groundwork for subsequent innovation in this field.

3. Adoption of NATO AI Strategy (2021)

In 2021, NATO adopted a NATO Artificial Intelligence Strategy, marking a significant step towards ensuring the Alliance remains at the forefront of 21st-century technological evolution. Global competition is increasingly playing out in the technological sphere, and NATO recognizes that artificial intelligence (AI) will play an important role in future security and defense. The Strategy seeks to ensure that NATO and its member countries stay ahead of the curve with regard to AI, while also maximizing interoperability, resilience, and deterrence and defense among Allies. AI must be harnessed for military planning, intelligence, logistics, and decision-making. At the same time, the Strategy underscores the importance of protecting democratic societies and values as AI is harnessed for defence. In short, the Strategy seeks to ensure that technology remains genuinely a force for good. NATO must remain the world's preeminent leader in AI, while setting the global gold standard for the responsible use of this powerful emerging technology.

3.1 Emerging and Disruptive Technologies (EDTs)

Emerging and Disruptive Technologies (EDTs) play a crucial role in NATO's Artificial Intelligence Strategy. Emerging and Disruptive Technologies have the potential to transform how future security challenges will be addressed. EDTs comprise a diverse array of technological advancements. In developing the AI Strategy, NATO considered technologies such as artificial intelligence, autonomous systems, big data, and quantum computing, as well as new applications of biotechnology and next-generation communications technologies. The key potential benefits of EDTs for situational awareness and strategic decision-making include accelerated analysis of large amounts of data and increased precision and efficiency of military operations. However, EDTs also present opportunities and threats that have not previously existed. For example, they could increase cyber threats and create even greater dependence on technology while also enabling potential adversaries to develop similar capabilities.

NATO is not only looking at opportunities to benefit from EDTs but is also working to create a conducive innovation ecosystem, encourage cooperation and interoperability, and support technology development among its member countries. NATO recognizes that Emerging and Disruptive Technologies are not simply tools to be employed by the Alliance; rather, they are strategic assets that will set the parameters for the future security landscape and will determine the global balance of power in war and peace.

3.2 NATO's Ethical and Policy Guidelines for AI

NATO's Ethical and Policy Guidelines for AI are key components of the AI Strategy developed by the Alliance. These guidelines must guide the development and use of AI responsibly. Above all, AI should be used lawfully and in conformity with relevant International Norms and Standards, whether common to the North Atlantic Community or established under accepted International Law, including International Humanitarian Law and respecting Universal Human Rights. In addition to these core principles, the use of AI at NATO must also be governed by a set of additional requirements. Notably, AI must remain under meaningful Human Control. Decisions made by AI systems must be explainable and traceable, and the system must be

reliable, with outcomes that can be safely predicted. Furthermore, care must be exercised to mitigate any unforeseen effects of the use of AI, including potential biases that may be embedded into algorithms and the increased risk of escalation. In adopting these principles, NATO aims to instill public confidence in the use of AI among not only its member countries but also globally as technologies continue to evolve, and the line between beneficial use and unethical application becomes increasingly tenuous. As AI takes root in every domain of conflict, NATO is not only reinforcing its military prowess but also validating its legitimacy and credibility.

V. Legal and Ethical Matters

2. Accountability and Responsibility

2.1 Appropriateness of Systems and Weapons According to Their Levels of Autonomy

Different levels of autonomy not only offer various advantages such as speed, efficiency, and data processing, but they also raise concerns about operational control and reliability. Human-in-the-loop systems require a human operator to approve decisions before an action is conducted. These systems are often used for situations that involve sensitive decisions, such as target identification or the use of force. Because in making these decisions, there must be a direct human judgment. Human-on-the-loop systems allow artificial intelligence to perform more independently while a human supervises the process and intervenes if necessary. These systems can be seen as a balance between efficiency and human oversight. Lastly, human-out-of-the-loop systems are capable of making decisions without human supervision once they are activated. While such systems may provide significant operational speed and automation, they also raise concerns regarding control, reliability, and the potential risks of unintended outcomes. Therefore, discussions within alliances often focus on which levels of autonomy are appropriate for different operations and how to ensure that they follow the legal and ethical standards and International Humanitarian Law (IHL).

2.1.1 Lethal Autonomous Weapons (LAWs)

Lethal Autonomous Weapons are weapon systems that do not require, based on the autonomy level, human control, human supervision, or human judgment. These systems can operate in air, land, sea, and space, potentially in communication-denied environments where human control is impossible. There are three types of LAWs, which are being human-out-of-the-loop, human-on-the-loop, and human-in-the-loop, in other words, meaningful human control weapons. Human-out-of-the-loop weapons are not being monitored or supervised by a human being, which raises concerns regarding security. All the targeting and decisions are being made by the weapon itself. Human-on-the-loop weapons are being supervised by a human being regularly in order to prevent operational and targeting accidents that may occur. However, the weapon is still based on Artificial Intelligence, and critical decisions are being made by it, which may affect vulnerable lives both socially and economically. Human-in-the-loop weapons are being used by a human being, and human judgment plays a crucial role in conducting an attack. These kinds of weapons cannot be strictly used without the approval of a human being for critical actions such as shooting and targeting. Target can be detected by AI, and shooting must be monitored by a human. If the weapon causes damage or takes a victim's life, the operator who monitors that weapon would be held accountable for the lives of the vulnerable.

In conclusion, often called "killer robots" these systems raise major ethical, legal, and security concerns, with various examples of the above, with international debates ongoing regarding whether to regulate or ban their use in modern warfare. However, if the weapon causes damage, the detection of the responsible parties may be strenuous.

2.1.2 Swarm Drones

Swarm drones are a highly advanced category of autonomous weapons systems, in which multiple unmanned aerial units operate through decentralized coordination and algorithmic decision-making. These systems rely on artificial intelligence, sensor fusion, and real-time data exchange to function as a cohesive network rather than as individual platforms. For instance, NATO has emphasized the integration of autonomous systems in exercises such as *NATO's*

Robotic Experimentation and Prototyping with Maritime Unmanned Systems (REPMUS), where allied forces tested coordinated unmanned platforms in real operational scenarios. Similarly, the U.S. Department of Defense's "swarm strategy" demonstrations, including the Perdix micro-drone program, showed how large numbers of drones can collaboratively adapt to changing environments without direct human control.

This collective behavior increases operational efficiency, adaptability, and resilience in conflict zones. However, their level of autonomy raises significant concerns regarding their appropriateness under international humanitarian law and established principles of armed conflict. NATO policy discussions have repeatedly underlined the importance of "meaningful human control" over autonomous systems, so that the risks posed by systems that can independently select and engage targets. In a swarm context, ensuring distinction between civilian and military targets becomes more difficult, especially in dense urban environments. In addition, the rapid speed and scale at which swarm drones can act may reduce the possibility of timely human intervention. Real-world conflicts, such as the use of loitering munitions and coordinated drone attacks in the Nagorno-Karabakh conflict (2020), provide evidence of how semi-autonomous systems can already overwhelm traditional defenses and increase the risk of escalation.

Therefore, despite their strategic and tactical advantages, the deployment of swarm drones necessitates strong regulatory frameworks, clear command responsibility, and strict adherence to NATO's emerging standards on autonomy in weapons systems. To ensure that these technologies are used legally and morally, it is still important to make sure that there is accountability, openness, and human oversight.

VI. Operational and Strategic Risks

1. Potential Civilian Harm and Collateral Damage

NATO's adoption of artificial intelligence (AI) and machine learning for its future military operations will be a sensitive issue due to the risks of civilian harm and collateral damage. Improved accuracy and speed are key benefits offered by modern technologies, yet they

increase complexity, making it even harder for militaries to distinguish between targets and to avoid harming civilians. Future surveillance, targeting, and decision-making on strikes are more likely to be automated or semi-automated, limiting the time available to weigh the consequences of a strike. Moreover, the use of AI increases the risk that accountability for any harm caused will be lost in a 'black box'. The use of AI in military operations must thus be carefully managed to preserve the gains of technological innovation while fulfilling NATO's obligations under international humanitarian law. Ensuring civilian protection and avoiding harm must remain a top priority.

1.1 Risks of Misidentification in Targeting

The risk of misidentification in targeting in AI-powered systems is perhaps the most critical of all AI risks in the military domain. The extent to which AI systems can accurately identify targets depends greatly on the data they have been trained on, how this data has been labelled, and utilized to develop decision-making processes. The risk of biased or incomplete training datasets is well-documented in the literature. In addition, incorrect pre-training of algorithms can affect the reliability with which a system identifies objects or situations as targetable. This risk is particularly pronounced in dynamic battlefield environments where civilians can exhibit behaviors and engage in activities that might suggest to an AI-powered targeting system that they pose a threat. Also, it is critical to remember that the enemy will attempt to deceive AI systems by pretending to be civilians or by manipulating AI datasets. Validation of AI-driven targeting decisions is therefore imperative, and this validation should always be conducted by humans who have the ability to question, challenge, and undo decisions made by the AI system. NATO must be particularly concerned about the potential for increased civilian casualties, as well as a breach of the principles embedded in the Protection of Civilians agenda, if AI-powered targeting systems are introduced into military operations without corresponding measures to validate targeting decisions.

1.2 Amplification of Civilian Exposure in Data-Based Operations

Artificial intelligence and machine learning algorithms are being leveraged to significantly enhance the capabilities of militaries in planning, execution, and assessment of operations. As militaries rely increasingly on processing large datasets for actionable intelligence, there is a growing risk of increased exposure of civilians to harm. Surveillance systems, with both static and roving sensors, and biometric data collected and maintained in databases, can potentially include information related to civilians. Similarly, data collected in real-time to inform decision-making can inadvertently include information of military relevance that affects civilians. Moreover, in operations where both combatants and civilians are included in data collection, there is a risk of civilians being involved in hostilities indirectly. There is also a potential for civilians to be wrongly identified, surveilled, or targeted based on incorrect interpretations of data. With greater connectivity of data systems, there is also an increased risk of cyberattacks and misuse of civilian data by states and non-state actors alike. NATO must incorporate stronger data governance practices, prioritize civilian data protection, and ensure that privacy and security protections are embedded into all AI-enabled operations and processes. This can be achieved by implementing practices of data minimization and fostering an environment in which the use of excessive or invasive data practices is discouraged.

1.2.1 Civilian Data-Overload

Civilian data-overload. Modern armed forces are increasingly relying on data from a variety of civilian sources, from satellites and drones to Facebook posts and credit card transactions. This information is fed into sophisticated AI systems designed to analyse it all as quickly as possible. In theory, this can lead to dramatically improved situational awareness, allowing soldiers and their commanders to make far better decisions than they would with legacy tools and techniques. In practice, the large amounts of noise contained in civilian data can greatly increase the chances of the AI making mistakes – even going so far as to mistake a civilian for a legitimate target. The pressure to make timely decisions within a fast-paced battlefield environment only adds to the risk of disaster. But the problems with relying on civilian data don’t stop there: there are serious ethical concerns around surveillance and the potential invasion of civilians’ privacy and human rights. NATO, therefore, needs to invest in better data

filtering and algorithms, as well as clear rules on which data should be collected and used for military purposes.

2. Alliance Cohesion and Policy Divergence Among NATO Member States

The challenge of alliance management is well established in the literature on NATO and, indeed, any intergovernmental organisation. Keeping an alliance of mostly democratic nations on the same page has always been hard. As technologies related to Artificial Intelligence (AI) mature and grow in significance within the security environment, challenges associated with AI are putting additional pressure on member states to either speak with one voice or suffer adverse effects for not doing so. Some will progress at different rates related to capabilities and commitments to utilising such systems, whilst others—whether domestically, regionally, or globally – will pose different positions or a set of positions regarding the very same technologies (e.g., weapons/AI in the realm of Defence and Security). Naturally, all this affects, or could affect, current or future shared practices at the operational level. Those diverging practices would in turn very likely impact overall interoperability – always a principal objective for the Alliance. Differences, furthermore, in their respective national frameworks for regulating matters related to the development and use of AI (e.g., in both peacetime and, of particular note, warfare), could make for uneven treatment of individuals – whether military or civilian – related to Alliance Command Structures (both current and future), and when exercising US/NATO commander responsibilities. Issues relating to their interpretations and understanding of applicable international norms and law at both the strategic and tactical levels – as these impinge upon (or are affected by) new evolving military technologies and their respective developmental trajectory – have, consequently, to be addressed on an Alliance-wide basis to preserve unity within Alliance structures.

Harmony, consensus, and cooperation can, thus, serve as the operational arm for, and the guiding light to NATO's quest for unified policies, for consistent and coherent interpretations of what national leaders consider the application of norms and law in respect of issues directly affecting their security (and, ultimately, that of the West) in the AI Age. By having aligned policies and agreed positions – pertaining not only military and technological applications, but

also encompassing related policy/ decision-making within the defence enterprise at large (covering Security/ Strategic Studies, industry, start-ups and all relevant other stakeholders) – the Alliance is able, nay obliged, to better address future problems arising out of technology, whilst establishing standards and cooperating on norms within defence and security to sustain their cohesion. Enhanced cooperation, framed by the interdisciplinary methodologies applicable in the AI field – encompassing robust academic/ research investment, with efforts directed towards mapping out areas to focus on in shared US/ EUAlliance investment for the longer-term – is consequently vital, particularly when it comes to fostering collaboration when it comes to governance and the adoption of best-practices as regards the ethical implications that are now, or may in the future be raised, by growing use and associated increasing complexity of emerging technologies such as those represented by AI.

VII. Case Studies

1. Case Studies of AI in Cyber Operations

1.1 NATO's Assistance for Cyber Efforts to Combat ISIS/DAESH

Islamic State of Iraq and the Levant, also known as ISIS or DAESH, has posed a massive threat to global stability through online propaganda, digital radicalization, encrypted communication networks, and cyber-enabled financing methods. In response, NATO has improved intelligence-sharing mechanisms among Allies, strengthened cyber defense programs, and supported strategic communications initiatives to undermine terrorist networks in the digital sphere. By recognizing cyberspace as a domain of operations and an integral part of collective defense, NATO seeks to increase the resilience of Allied critical infrastructure and military networks against terrorism-based cyber activities. This assistance is mostly focused on coordination, training, and technical capacity-building rather than direct offensive cyber operations.

1.2 NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

The NATO Cooperative Cyber Defence Centre of Excellence is a unique military coalition of 20 NATO countries working together to strengthen cyber defence capabilities among NATO Allies. The Centre was established in 2008, following the 2007 cyberattacks perpetrated against Estonia. The Centre conducts world-class scientific research, organises large-scale practical exercises, including the world's most advanced live-fire cyber defence exercise Locked Shields, and develops manuals for legal assessment of cyber warfare. Notably, the Tallinn Manual is the first comprehensive work to examine the application of International Humanitarian Law and other parts of international law to cyberspace from an academic and legal perspective.

1.3 Allied Cyber Operations Centre (ACO) Coordination

Allied Command Operations (ACO) is responsible for conducting all NATO Military operations, including cyber operations through the Allied Cyber Operations Centre. The Centre provides Situational Awareness, planning support, and coordination for cyber operations across all NATO militaries. It also coordinates with National cyber assets to provide the capability to synchronise cyber effects to defence plans in the land, air, and maritime operations areas. Cyber elements are also incorporated into major NATO military exercises such as large-scale amphibious assaults, as seen in Exercise Trident Juncture.

In the ACO model, coordination is central, but action is decentralized, allowing Allies to defend themselves while collectively defending each other. While strategic coordination of cyber defence efforts across nations with different capabilities, legal frameworks,s and technological development is a difficult undertaking, NATO has recognized the utility of cyberspace as an operational domain (officially in 2016) and is working to achieve the necessary interoperability and information sharing across the Alliance. The Allied Cyber Operations Centre at NATO will play a similar role as a key source and recipient of information, operating within the constraints of NATO's principles of collective defence and with appropriate political oversight.

2. Case Studies for Predictive AI Targeting Systems

2.1 NATO's NEC (Network-Enabled Capability) Exercises

NATO's Network Enabled Capability (NEC) is an emerging framework for enhancing Operational Effectiveness (OE) through the interconnectedness of sensors, decision-makers, and weapon systems within a pervasive network environment. NEC Training Exercises are conducted to test the Allied Force's information superiority capabilities to gain Situational Awareness, make timely decisions, and to effectively coordinate and conduct a combined military operation across land, air, maritime, and cyber dimensions.

One such example is the annual Coalition Warrior Interoperability Exercise (CWIX) conducted by NATO for the purpose of evaluating interoperability between the communication and information systems of its member countries and their partners. CWIX, which was held for the last time in 2012 and is not going to be held in the future, involved thousands of experts from around 30 countries. Hundreds of systems were tested annually at the exercise, which made it one of the world's largest interoperability exercises. The scientific and operational assessment results demonstrate that network-enabled solutions reduce decision time significantly and improve the accuracy of shared information. The outcome is known as the "common operational picture," helping commanders to make timely and appropriate decisions in response to changing battle space conditions.

NATO is also conducting efforts to create NATO Federated Mission Networking (FMN) based on lessons learned in Afghanistan. The goal of FMN is to develop an interoperable networking infrastructure based on common communication standards. While formal NATO testing is still ongoing, assessments carried out by NATO to evaluate the overall interoperability of current national communication systems based on FMN principles have shown positive outcomes and tangible benefits in terms of increased success of missions and reduction of operational risks, particularly in joint and coalition environments.

However, those who employ NEC also face a series of challenges. Increasingly complex interconnected systems offer more targets for the cyber threat, generate greater volumes of data that must be correctly interpreted, and are frequently incompatible with older systems. Analysis conducted by NATO's CCSS found that data overload can often impede rather than support the decision-making process. Thus, even as NEC exercises dramatically increase the coordination and efficiency potential of Military Planning, those who plan military operations must also invest in solid cybersecurity measures, develop institutional protocols to govern the flow of information, and run periodic training exercises to stay on top of rapidly evolving threats.

In summary, NATO NEC tests demonstrate that network-enabled operations can deliver significant military benefits; meanwhile, they have clearly highlighted the need for effective management of technology in order to achieve resilience, security, and success.

2.2 Defense Advanced Research Projects Agency (DARPA) Target Prediction Algorithms Development

The Defense Advanced Research Projects Agency (DARPA) has pursued the development of advanced target prediction algorithms that improve speed, accuracy, and performance for military decision-making. The algorithms employ techniques from artificial intelligence and machine learning to process large datasets of information, identify patterns or correlations, and make predictions regarding future targets or threats to the warfighter. While current target tracking and engaging systems rely on significant amounts of operator input, DARPA's target prediction algorithms aim to enable targets to be identified and prioritized with partial or no human oversight.

DARPA's Mosaic Warfare concept aims to transform the way military units organize and employ distributed networks of small, smart systems. Studies show that such distributed systems, informed by AI, can significantly improve targeting accuracy while significantly reducing response time. Reports from current DARPA programs – such as the agency's work using machine learning to detect and track boats from satellite imagery – show that the

approach can achieve higher detection rates than traditionally trained analysts. Researchers are exploring how these predictive systems can process mountains of data to filter out information irrelevant to the warfighter and to prioritize the most critical details for a human to decide.

In addition to these efforts, DARPA has initiated several programs aimed at developing explainable artificial intelligence (XAI), which seeks to develop systems that provide authoritative explanations of their results to enhance trust and accountability. Experience shows that operators are more likely to accept the output of AI tools if they can understand the basis for the prediction.

Despite the significant advances achieved with the algorithms developed under DARPA's Target Prediction (TP) effort, numerous challenges remain. Science and the defense technical community have addressed the potential for bias in algorithms and data-driven systems, as well as the risks associated with adversarial examples that can cause AI systems to fail by manipulating the input to the system. Recent conflicts have highlighted failures of sophisticated targeting systems when data is lacking or misleading. Consequently, even with the increased operational capability that the best available target prediction algorithms can provide, the algorithms must be tested, employed, and managed by trained personnel, and obey all applicable law, custom, and standards of ethics and humanitarian law.

DARPA’s results show promise that using artificial intelligence for target prediction could revolutionize warfare by bringing greater precision and efficiency to the battlefield, but also underscore the need for improved reliability, explainability, and responsible use of the technology.

3. Case Studies for Operational Risks

3.1 NSA Mass Surveillance Revelations (2013)

The NSA mass surveillance revelations were a series of disclosures made in 2013 by Edward Snowden, a former contractor for the National Security Agency (NSA). The revelations described the scope of NSA's surveillance efforts, which had been collecting phone metadata and massive amounts of communications records from around the world from a variety of sources, often with assistance from large technology companies through programs like PRISM and the use of malware through programs like XKeyscore. The revelations sparked a global debate over issues of privacy, cybersecurity, and surveillance, and led to numerous calls for reform. The events represented a significant shift in the conversation around how to balance security efforts and individual rights.

From a more scientific viewpoint, the revelations provided important insight into the scope and capabilities of systems using data for intelligence. In studies of cybersecurity and data science, analyzing metadata has again and again revealed sufficient information to determine behavioural patterns of individuals, their social networks, as well as forecasts on their future behaviour with high accuracy. For instance, by analyzing the call metadata of mobile phones without ever having accessed the communication contents, patterns of regular activities and personal relationships could be delineated with an accuracy of more than 90 per cent. Numerous studies have published their findings in journals and academic proceedings following the Snowden revelations, exemplifying the power big data analytics has in the domain of intelligence.

Secret documents also reveal strengths and weaknesses of mass surveillance, touting its value in catching terrorists early but also suggesting it hasn't stopped any major attacks. That assessment is based on their own experience, as well as independent reviews from parliamentary and academic oversight groups, which have found sparse evidence that bulk collection of data played a decisive role in foiling terrorism.

The leak has also highlighted serious concerns with respect to data security and data governance. The breach appears to have been effected by a single insider - the disclosure of classified data raises significant concerns regarding the effectiveness of an organization's internal controls, including accountability and oversight. The illicitly disclosed information has

also sparked an international rift, particularly between the US and allied governments, after reports suggested that surveillance targeted at foreign government officials and organisations had taken place.

The 2013 NSA mass surveillance revelations provide a critical case study of the potential of large-scale data-driven intelligence systems. The revelations expose both the capability to gain situational awareness at unprecedented scale through advanced analytics, and the corresponding need for greater transparency, accountability, and legal oversight of such capabilities.

3.2 Cambridge Analytica Scandal (2018)

The Cambridge Analytica scandal refers to the misuse of personal data from millions of Facebook users by the political consulting firm Cambridge Analytica. The data was harvested by a third party using a Facebook app, and then used to create “psychographic profiles” of users to be used in political advertising – notably during the 2016 United States presidential election.

Several scientific studies in data science and political communication research have shown the potential of such microtargeting practices to change people’s voting behavior. In this research, the researchers used the OCEAN model for personality traits and found some astonishing results: digital traces like Facebook likes can predict a large set of personality characteristics very well. However, several empirical studies and reports by regulatory bodies indicate that the overall impact of microtargeting in the last elections is still unclear and hard to measure.

The scandal revealed serious shortcomings in data governance, user consent, and the accountability of platforms. Big data and algorithmic profiling, which are already widely used for commercial purposes, have now also been used to mount political influence operations. The case study is therefore a significant example of the risks of data exploitation in the absence of adequate data protection laws, transparency, and ethics rules.

VIII. Questions to be Addressed

1. How can the North Atlantic Treaty Organization ensure “meaningful human control” over AI-assisted and autonomous military systems while maintaining operational efficiency and speed?

2. To what extent should predictive AI targeting systems be trusted in high-risk military operations, and what red lines should be implemented to minimize misidentification and civilian harm?

3. How can NATO balance the strategic advantages of offensive cyber AI operations with the legal obligations under international humanitarian law and the protection of civilian data?

4. What regulatory frameworks should be established to govern the development and deployment of lethal autonomous weapons (LAWs) and swarm drone technologies within NATO member states?

5. How can NATO address policy divergence and differing national regulations among its member states regarding the use of artificial intelligence in military operations?

6. In what ways can NATO strengthen accountability and transparency in AI-driven decision-making processes, particularly in cases of unintended consequences or collateral damage?

7. How should NATO cooperate with international organizations and non-member states to establish global norms and ethical standards for the military use of artificial intelligence?

IX. Further Reading

North Atlantic Treaty Organization Science and Technology Organization. (2020). Benefits and challenges of AI/ML in support of intelligence. *https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-IST-190/MP-IST-190-09.pdf*

International Committee of the Red Cross. (2019). Artificial intelligence and machine learning in armed conflict: A human-centred approach. *https://www.icrc.org/en/document/artificial-intelligence-and-machine-learning-armed-conflict-human-centred-approach*

Defense Advanced Research Projects Agency. (n.d.). Explainable artificial intelligence (XAI) program. *https://www.darpa.mil/program/explainable-artificial-intelligence*

Amer, K., & Noujaim, J. (Directors). (2019). The Great Hack [Documentary]. Netflix. *https://www.netflix.com/title/80117542*

<PRIVATE_PERSON>. (n.d.). AI in autonomous systems. Wiley Online Library. *https://onlinelibrary.wiley.com/doi/abs/10.1002/9781394355471.ch12*

<PRIVATE_PERSON>. (2023). Public policy challenges, regulations, oversight, technical, and ethical considerations for autonomous systems: A survey. IEEE. *https://ieeexplore.ieee.org/abstract/document/10063171/*

North Atlantic Treaty Organization Science and Technology Organization. (n.d.). A novel swarm defense end-to-end system for autonomous drone detection, tracking, and neutralization. *https://www.sto.nato.int/document/a-novel-swarm-defense-end-to-end-system-for-autonomous-drone-detection-tracking-and-neutralization/*

North Atlantic Treaty Organization. (2021). Artificial Intelligence Strategy.

International Committee of the Red Cross. (2019). Artificial Intelligence and Machine Learning in Armed Conflict: Implications for Protection.

Defense Advanced Research Projects Agency. (2020). Explainable Artificial Intelligence (XAI) Program Overview.

United Nations Institute for Disarmament Research. (2021). The Weaponization of Increasingly Autonomous Technologies.

European Union Agency for Cybersecurity. (2022). Cybersecurity and AI: Challenges and Opportunities.

NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence.

World Economic Forum. (2020). Global Risks Report: Cybersecurity and AI Risks.

RAND Corporation. (2020). Artificial Intelligence in Military Operations: Risks and Opportunities.

The Great Hack. (2019). The Great Hack [Documentary].

X. References

North Atlantic Treaty Organization. (2016, July 9). Warsaw Summit Communiqué. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2016/07/09/warsaw-summit-communique

nato.int

North Atlantic Treaty Organization. (n.d.). Relations with Iraq. https://www.nato.int/en/what-we-do/partnerships-and-cooperation/relations-with-iraq

United Nations Office for Disarmament Affairs. (n.d.). Lethal autonomous weapon systems. https://disarmament.unoda.org/en/our-work/emerging-challenges/lethal-autonomous-weapon-systems

North Atlantic Treaty Organization. (2016). Warsaw Summit Communiqué. https://www.nato.int

North Atlantic Treaty Organization. (2021). Artificial Intelligence Strategy. https://www.nato.int

North Atlantic Treaty Organization. (2022). NATO 2022 Strategic Concept. https://www.nato.int

International Committee of the Red Cross. (2019). Artificial Intelligence and Machine Learning in Armed Conflict. https://www.icrc.org

United Nations Office for Disarmament Affairs. (2020). Lethal Autonomous Weapon Systems. https://disarmament.unoda.org

NATO Cooperative Cyber Defence Centre of Excellence. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press.

Defense Advanced Research Projects Agency. (2020). Explainable Artificial Intelligence (XAI) Program. https://www.darpa.mil

European Union Agency for Cybersecurity. (2022). Cybersecurity Threat Landscape Report. https://www.enisa.europa.eu

Organisation for Economic Co-operation and Development. (2019). OECD Principles on Artificial Intelligence. https://www.oecd.org

World Economic Forum. (2020). The Global Risks Report 2020. https://www.weforum.org

RAND Corporation. (2020). The Role of Artificial Intelligence in Future Warfare. https://www.rand.org

Cambridge University Press. (2018). Ethics of Artificial Intelligence and Robotics.

Stanford University. (2021). Artificial Intelligence Index Report. https://aiindex.stanford.edu

United Nations. (1949). Geneva Conventions.

United Nations. (1977). Additional Protocols to the Geneva Conventions.