Al-Kashaf (Journal of Social Sciences) (Miscellaneous)
Volume: 05, No: 04. October – December 2025
ISSN: 2790-8798; E-ISSN: 2790-8801

Artificial Intelligence and Cyber Warfare as Emerging Threats to National Security in the Digital Age

Samreen Pervaiz *

** LL.M. Scholar, University of the Punjab, Lahore, Pakistan*

KEYWORDS

Artificial intelligence, Cyber Warfare, Cyberspace National Security.

ABSTRACT

Artificial intelligence has emerged as one of the most radical technologies in modern national security, defence, and governance of digital technology. In the digital world, cyberspace is no longer a medium of communication only; it is now a strategic space wherein states, non-state actors, criminal groups, and proxy networks are able to operate hostile movements without any physical borders being crossed. The main problem in this area is that AI-enabled cyber wars accelerate the speed, scope, anonymity, agency, self-sufficiency, and psychological effect of cyber operations, and the prevailing legal frameworks are unsure of how to deal with attribution, accountability, sovereignty, use of force, proportionality, due diligence, and state responsibility. This focused study specifically analyses how AI is changing cyber warfare and how AI is emerging as a new threat to national security through automated cyberattacks, AI-powered malware, adversarial machine learning, deepfakes, disinformation, ransomware, supply chain attacks, and how engineers are using AI to launch attacks against critical infrastructure. The methodology of this research is qualitative doctrinal legal research, based on international legal instruments, institutional reports, policy documents, and scholarly legal literature. The approach followed is analytical and comparative because the article investigates the principles of international law, cyber law, AI governance structures, and the principles of responsibility of the states. The hypothetical conclusion is that, based on the current international law, computer warfare is subject to this law, although it does not provide sufficient clarity in its operations to effectively apply this law to the current computer warfare. The article summarises that it should be stronger internationally, have more recognisable legal thresholds, be monitored by a human, presented by cyber attribution standards, passionate about critical infrastructure, and have AI-specific national security rules. This work adds to the legal literature by linking artificial intelligence, cyber warfare, and national security in a modern international law paradigm.

Introduction

Artificial intelligence (AI) has become a key attribute of contemporary security, defence, governance, and warfare. It is also finding more applications in processing large volumes of data, automating decision-making, detecting cyber threats, identifying vulnerabilities, and supporting military planning. Simultaneously, malicious actors are automating attacks, seasoning phishing, manipulating information, and creating deepfakes, as well as developing adaptive malicious tools. This dual significance provides AI as both a defence resource and a national security threat. In its Digital Defense Report 2025, Microsoft suggests that nation-state threat actors have turned to the application of AI to make their cyber and influence operations more scalable, targeted, and sophisticated, such as through synthetic media and automated influence campaigns (Microsoft, 2025).

The largest concern in the given area is the increasing gap between the evolution of technologies and the legal regulation of the sphere. Conventional international law was mostly formulated in the context of physical conflict, territorial aggression, and human-initiated and directed military action. Nevertheless, AI-based cyber warfare frequently transpires at the level of conventional armed conflict. It can consist of cyber espionage, data theft, infrastructure disruption, disinformation, electoral interference, ransomware, and malware placement without immediate physical destruction. This leads to legal ambiguity as to

*Corresponding Author: Samreen Pervaiz
Email Address: *samreenpervaiz478@gmail.com*

whether such acts constitute a violation of sovereignty and unlawful intervention, the use of force, or armed attacks.

This study specifically focuses on the role of AI in revolutionising cyber warfare and creating new threats to national security in the digital era. This study considers the application of AI in cyberattacks on critical infrastructure, military systems, elections, government agencies and their information systems, financial systems, healthcare systems, supply chains, and the information environment. It also examines the legal consequences of AI-enabled cyber warfare, especially in the context of attribution, state responsibility, proportionality, due diligence, meaningful human control, and accountability.

This study employs a qualitative and doctrinal methodology. This study examines primary and secondary legal texts, such as the United Nations Charter, the Draft Articles on State Responsibility prepared by the International Law Commission, international humanitarian law, legal studies of AI, journal reports of international organisations, and interface-specific instruments of AI governance. The analytical and comparative approach also characterises the study that evaluates the response of the current legal frameworks to the emergence of new cyber threats enabled by AI.

The available literature indicates that cyberspace has become an accepted area of national and international security. NATO considers cyberspace as an operating domain, and at the 2024 Washington Summit, allies agreed to set up the NATO Integrated Cyber Defence Centre to improve network protection, situational awareness, and the implementation of cyberspace as an operating domain during peacetime, crisis, and conflict (NATO, 2024). Tallinn Manual 2.0 is also a valuable scholarly source because it analyses the applicability of international law to cyber operations, including those that fall under the threshold of an armed conflict (Schmitt, 2017). However, the Tallinn Manual is not a treaty and does not entirely address the more recent issues created by AI, autonomous cyber tools, and adversarial machine learning.

The gravity of the cyber threats posed by AI is also validated in recent institutional literature. As one of the key security risks significant in its own right, it is proposed by NIST adversarial machine learning, including attacks that manipulate AI training data, inputs, model behaviour, privacy, and generative AI outputs (Vassilev et al., 2025). The ICRC has realised that modern armed conflicts are raising new issues with international humanitarian law as armed conflicts are increasingly cyber operations, information operations, autonomous systems, and artificial intelligence-assisted military decision-making (International Committee of the Red Cross [ICRC], 2024). These developments indicate that AI-enabled cyber warfare is no longer merely a technical and policy matter of cybersecurity; it is a legal, strategic, humanitarian, and national security issue.

AI, Cyber Warfare, and National Security

AI is a term used to systems which can perform functions which typically require human intelligence, such as learning, prediction, classification, pattern recognition, decision-making, and automation. AI can be employed in the cyber realm to use defensive to identify malware, detect abnormal network behaviour, examine threat intelligence, and assist incident response. However, the same capabilities can be used in an offensive manner to identify vulnerabilities, generate malicious codes, create phishing messages, impersonate trusted persons, and conduct massive information operations.

This directly impacts national security, as modern states rely on digital systems to govern, defend, finance, communicate, provide healthcare, transport, and administer the state. Such systems may not need invasive physical actions to be affected by a cyberattack, but they can cause detrimental effects to the social fabric of people, economic stability and life of civilians, and sovereignty of states. For example, an artificial intelligence-based attack on a hospital system might postpone emergency services, tamper with patient information, or shut down necessary services. The Oxford Statement on Cyber Operations against Healthcare declares

that international law is applicable to state cyber operations and that such operations by states violating this rule have severe adverse effects on essential medical services in other states (Oxford Institute for Ethics, Law and Armed Conflict, 2020).

AI as a Dual-Use Technology in Cyber Warfare

AI is a dual-use technology in the sense that it can be utilised in both lawful and criminal ways. On the one hand, AI enhances cyber defence by detecting malware, abnormal network behaviour, analysing threat intelligence, and improving incident response. Conversely, hostile nations, proxy groups, terrorists, and cybercriminals can use the same technology to automate the hacking process, craft more convincing phishing prompts, bypass security software, influence mass media, and accelerate cyberattacks.

This two-fold use poses a grave question of legality and policy. By constraining AI development to a significant extent, states can undermine both innovation and national cyber defence. However, when AI systems are not properly regulated, they can be abused for cyber warfare and electronic blackmail. This regulatory issue is reflected in the European Union AI Act, which came into force on 1 August 2024 and adopts a risk-based framework for responsible AI development and deployment (European Commission, 2024).

The legal significance of the dual-use issue is that intelligence sources in cyber warfare could be domestic companies, open-source projects, research entities, cloud service providers, or software-type companies. This makes it harder to keep track of who is doing what and who is held responsible when harmful cyber operations are involved, as they may involve a blend of state agencies, commercial contractors, developers, server or cloud providers and non-government actors. Thus, any type of cyber warfare facilitated by AI cannot be controlled solely through military laws. It must also have a cybersecurity law, corporate responsibility, export controls, technology governance, and international cooperation.

AI and the Transformation of the Cyberattack Lifecycle

AI reinforces virtually all phases of the cyberattack lifecycle. During reconnaissance, AI can scan vast networks, collect open-source information, identify vulnerable systems, and map organisational structures. The weaponisation stage can be aided by AI to create malicious code or select the most effective approach to attack. During the delivery phase, generative AI can generate individualised phishing email messages, synthetic voices, artificial videos, and fake messages. During the exploitation phase, AI can fit the environment of the target in terms of security. The evasion stage is where AI can alter malware behaviour to evade detection.

The legal issue is that attacks powered by AI might take place quicker than both the legal and institutional mechanisms to respond to them. Conventional legal procedures involve investigation, gathering of evidence, attribution, legal evaluation, and state adjudication. However, artificial intelligence-driven cyber actions might result in harm before the affected state detects the intruder. This poses a serious loophole in terms of the pace of technological change and legal fallout.

Emerging AI-Enabled Cyber Threats to National Security

AI-Powered Malware and Automated Intrusions

AI-enabled malware can be considered the most severe source of security threats to a nation. Classic malware tends to adhere to hardcoded instructions. However, AI-enhanced malware can evolve to fit the environment, elude detection, find useful data, and alter attack patterns. Military databases and defence communication systems, financial institutions, public-sector networks, and critical infrastructure can become targets of such malware.

In the context of the law, AI-enhanced malware makes foreseeability and responsibility more problematic. If a state deploys an AI-

enabled cyber tool that spreads beyond its intended target, harms civilian infrastructure, or even disables essential services, it should not avoid its responsibility by stating that the system acted unpredictably. Under the International Law Commission's Draft Articles on State Responsibility, every internationally wrongful act by a state entails international responsibility (International Law Commission, 2001).

Deepfakes, Cognitive Warfare, and Democratic Destabilisation

One of the significant threats to national security is AI-generated deepfakes which may lead to a lack of trust in institutions. Deepfakes can consist of fake video and audio, created speeches and or fake military announcements, forged diplomatic messages, or engineered evidence. A deepfake message using a presidential, military leader, minister, judge, diplomat, etc., in a situation involving tense political or military circumstances could lead to panic, diplomatic conflict, or military miscalculations.

The threat of deepfakes is not limited to misinformation. They can be used as a means of cognitive warfare, which aims to manipulate perception, emotion, decision-making, and public trust. AI-based disinformation can also be used to undermine democratic institutions through the dissemination of fake news items, voter manipulation, or the inculcation of election distrust.

Adversarial Machine Learning

The systems based on AI are not merely a weapon of cyber warfare; they are a target as well. Adversarial machine learning is a type of attack that can manipulate AI systems, training data, inputs, outputs, or model behaviour. NIST lists key types of adversarial machine learning attacks, such as evasion attacks, poisoning attacks, privacy attacks, prompt injection attacks, and indirect prompt injection attacks, against generative AI systems (Vassilev et al., 2025).

This threat is of particular importance to the national security since governments grow more dependent upon AI systems in the areas of five functions of the national security information system: border protection, biometric identification, intelligence analysis, surveillance, fraud detection, cyber defence and military decision support. In case an opponent succeeds in corrupting these systems, the state can then make erroneous judgements due to false information. To illustrate, an AI threat detection system can fail to detect a real attack, legal person can be falsely charged, or can suggest a disproportionate response.

The legal issue is that adversarial machine learning transforms cyber warfare as the network attack, by changing the attack into the decision-making process. This presents an enhanced variant of the vulnerability of national security since the state might lose faith in the reliability of their own security systems.

Attacks on Critical Infrastructure and Civilian Harm

The first focus of AI-generated cyber warfare is the critical infrastructure. Hospitals, water systems, energy grids, telecommunications networks, financial systems, airports, seaports and emergency services are known to be vital in the lives of the people. An operation against such systems using cyber can result in severe civilian damage without the use of bombs, missiles, or a physical invasion.

ICRC has realised that cyber operations, information operations, autonomous systems, and AI supported military decision-making pose significant challenges to the protection of civilians under the provisions of the international humanitarian law (ICRC, 2024). On legal grounds, the field of attack in civilian infrastructure may breach the concept of distinction, proportionality, and precautions when conducting attack in armed conflict. Even not in case of armed conflict such operations can be in force of sovereignty, due diligence duties, human rights and domestic criminal law. When AI can be used to target a wider audience or disrupt in a faster and more efficient manner, states need to conduct more stringent legal due diligence prior affixal deployment of cyber capabilities.

Supply Chain Attacks, Cloud Infrastructure, and Systemic Risk

The risk of supply chain attacks is also bolstered by AI-enabled cyber warfare. Current digital platforms rely on software vendors, cloud providers, service providers of third-party services, the data centres, application programming interfaces and exterior contractors. When one of the characters involved in the attack compromises one of the trusted suppliers, the attack can extend to the various organisations and government systems. Such attacks may be aided by AI discovering weak dependencies, software patterns, and automating exploitation.

This is a critical issue, because it is now vital that the systems owned by governments are supplemented with digital infrastructure owned privately. Systems imperative to state security may be controlled by cloud providers, software companies, cybersecurity firms, telecom operators, and data processors. The legal aspect of this is that national cyber defence necessitates the cooperation between public and private sectors. States cannot safeguard national security by merely regulating government agencies. They need to place reasonable cybersecurity responsibilities on critical non-government actors and respect innovation and privacy and commercial freedom.

Cyber Espionage, Data Weaponisation, and Strategic Intelligence

Cyber espionage has always been a part of a state practice, yet AI adds additional strategic value to it. The large quantities of stolen information, behaviour patterns, prediction of institutional vulnerability, and transformation of raw data into intelligence can be analysed by the AI. This implies that data theft can no longer be just a privacy or confidentiality problem but can develop into a national security problem.

AI, Ransomware and State Crime Dynamics

Ransomware is an often-considered cybercrime but as an AI-enabled cyber warfare can also become a matter of national security. Criminal organizations can also apply AI to detect lucrative targets, generate convincing phishing messages, automate the negotiation process, evade detection, as well as accelerate intrusion. When hospitals, energy companies, transport systems, or public institutions, or even defence contractors, are the target of ransomware, the impacts become strategic.

Autonomous Cyber Defence and Escalation Risk

AI is being applied in more ways than just to commit cyber offence; it can also be used to apply cyber defence. Automated cyber defence systems are able to identify threats, cut traffic and isolate infected machines as well as respond to attacks more swiftly than human teams. This is helpful since cyber operations are frequently used at machine velocity. Nevertheless, autonomous cyber defence may introduce the risk of escalation in case systems have overly aggressive responses, and the human factor of reviewing such responses is inadequate.

International Legal Framework Governing AI-Enabled Cyber Warfare

Use of Force and Armed Attack

The Charter of the United Nations is the cornerstone of the international political system of laws. Article 2(4) does not allow any state to employ force against the territorial integrity or political autonomy of another state, but Article 51 recognises the natural right of self-defence in the event of armed assault by another state (United Nations, 1945).

The most important legal issue is the possibility of an AI-driven cyber operation to constitute a use of force or an armed attack. The best method is the effects-based method. According to this interpretation, the jurisdiction to classify a cyber operation should be based on the impact of the cyber operation and not the weapon or method utilized. In the event that an AI-powered cyberattack, which causes fatalities, physical damages, structural failures or other effects that can be compared to a conventional military force, it can be considered a use of force or an armed attack.

Nonetheless, the area of legal uncertainty is present in cases where cyber operations result

in significant non-physical damages. To use the example that successful cybercriminals can cause devastating effects to national security without causing physical damages. The current international law does not offer a universally applicable standard of such harm. This is where the malicious players would practice in the grey zone, which is near to an actual warfare.

Sovereignty, Non-Intervention, and Due Diligence

The use of AI in cyber operations can be considered to be a violation of sovereignty in any case where AI is used to interfere with the territory, infrastructure, or otherwise governmental functioning of a particular state. Cyber operations against military infrastructures, elections databases, public administration networks, and even judicial systems and emergency services can be included. Sovereignty goes beyond physical boundaries not only by the capacity of the state to undertake certain vital governmental functions without outside interference.

The Law of non-intervention applies as well. Cyber operation could violate this principle when it forcefully interferes in the matters that are within the domestic jurisdiction of another state, in such cases as elections, political decision-making, public order, national defence, or constitutional processes. Deepfakes produced by AI, as well as an individual disinformation, can abuse this principle when they are utilised to control democratic procedures or destabilise social institutions.

Another concept of importance is due diligence. It implies that states must not wittingly permit their land, infrastructure or electronic networks to be utilized in activities that are known to have severe harmful impacts on other states. Despite the controversy surrounding due diligence in cyberspace, it is growing in importance due to the frequent use of a third-party infrastructure in cyberspace. The UN Open-Ended Working Group on security of and in the use of ICTs kept stressing on responsible behaviour of the states and the application of the international law in the cyberspace (United Nations Open-Ended Working Group, 2025).

State Responsibility and Attribution

The legal control over AI-supported cyber warfare focuses on state responsibility. An internationally wrongful act under the Draft Articles of the International Law Commission can be found when the conduct is attributable to a state and the conduct amounts to a breach of an international obligation (International Law Commission, 2001).

Cyberspace makes attribution challenging as attackers can wrap themselves in the proxy groups, compromised systems, falsely implied technical indicators, anonymisation tools, third-party servers and AI-generated identities. Attribution is even more difficult because AI tends to produce deceptive patterns, imitate the tricks of other players, and raise false-flag members. This poses a grave threat of under-response and over-response. When attribution becomes too small, those states that are responsible might escape liability. When attribution is excessively hasty the innocent states are accused.

International Humanitarian Law and Civilian Protection

The international humanitarian law is relevant when the use of AI-enabled cyber operations takes place in times of armed conflict. The important principles include distinction, proportionality, military necessity, precautions and humanity. The parties should differentiate military targets and civilian members. They should also not be attacked in such a way that it causes the death of an excessive number of civilians in proportion to the expected military value.

Special challenges are posed by cyber operations due to the fact that civilian and military systems tend to be interconnected. An attack on a military communication network can extend into civilian use of the internet, hospitals, banking networks or even emergency response procedures. AI is riskier, as automated systems might be unable to comprehend fully the civilian

ramifications. Thus, commanders and legal advisers should make sure that AI-assisted cyber operations will not be beyond the human control, legal examination, and safeguarding.

The challenges identified in the work of contemporary IHL challenge by the ICRC, as outlined in the above challenges issues, raise important questions to civilian protection particularly when the issues identified by the ICRC cut across digital operations and AI-assisted military decisions (ICRC, 2024).

Human Rights Implications of AI-Enabled Cyber Warfare

The human rights are also impacted by AI-enabled cyber warfare. The privacy, freedom of expression, political participation, equality, and due process may be compromised by cyber surveillance, data manipulation, and internet shutdowns, disinformation campaigns, biometric targeting, and automated monitoring. Strong powers of cyber defence may be necessary by states but such powers must be accountable through legality, necessity, proportionality, judicial supervision and democratic accountability.

The Council of Europe Framework Convention on Artificial Intelligence is notable in that it has made the connection between AI governance and human rights, democracy, and the rule of law. It was drafted to be signed on September 5, 2024, and is reported by the Council of Europe to be the first legally binding international agreement in this area (Council of Europe, 2024). The legal argument is that national security cannot be invoked as the general excuse to unchecked surveillance, censorship or arbitrary digital control.

Comparative and Institutional Responses

The international and regional institutions started responding to AI and cyber threats, but their actions are still inadequate. In an effort to enhance protection, situational awareness and cyber coordination, NATO has enhanced cyber defence by considering cyberspace an operational domain and establishing the NATO Integrated Cyber Defence Centre (NATO, 2024).

The AI Act has been adopted by the European Union, which comes into force on August 1, 2024. It establishes a risk-based system to control AI and put more strict responsibilities on the high-risk AI systems. Another example where AI governance has been linked to human rights, democracy, and the rule of law is in the Council of Europe approach which is also treaty-based (Council of Europe, 2024).

These advancements demonstrate that AI regulations are shifting out of the framework of an ethical discussion to one of legal regulation. Nevertheless, such systems are not yet capable of adequately responding to AI-driven cyber warfare. The first gap is that the use of AI in civilian, criminal, intelligence, and military activities neither legally nor practically intersect nowadays. Thus, further regulation needs to deal with dual-use character of AI in a much more straightforward manner.

Regulatory Gaps and Critical Analysis

The first major gap is the attribution gap. Attribution by international law is a precursor to establishing state responsibility, whereas AI compounds these attribution challenges through heightened opportunities of anonymity, misrepresentation and use of a false flag. With no attribution, a victim state will not identify the actor responsible with clarity with demand of reparations or any other lawful action.

The second gap is the threshold gap. The international law lacks clear guidelines as to the point when serious non-physical cyber injury is a use of force or armed assault. The political, economic, psychological and institutional damage may be caused by AI-enabled operations without a tangible destroyed macro-environment. By enabling aggressors to stay below the legal bar of traditional warfare.

The third gap is the accountability break. Programmers, individual businesses, commanders, intelligence, cloud, and autonomous systems might be involved in AI-enabled cyber operations. Current legislation lacks a precise allocation of the responsibility in

case AI systems cause unintended or disproportional harm.

The fourth gap is the human control gap. AI has the potential to eliminate the important human role in cyber operations, more so where autonomous systems are used to detect and respond to threats in real-time. This is an issue of necessity, proportionality, precaution and command responsibility.

The fifth gap is critical infrastructure gap. In most instances, national security systems are owned or operated by commercial entities and as such, a public/ private legal coordination is therefore necessary. With no clear responsibilities it assumes on the part of the crucial private actors, the concept of national cyber resilience is still a half-baked concept.

Conclusion

AI-enabled cyber warfare has transformed modern security threats into faster, more autonomous, and highly complex forms of conflict. AI technologies such as automated cyberattacks, deepfakes, ransomware, cyber espionage, and attacks on critical infrastructure can destabilize states without traditional military force. Although existing international law, including the UN Charter, state responsibility, international humanitarian law, and human rights law, applies to cyber operations, these frameworks were not specifically designed for autonomous AI systems. Major legal gaps therefore remain regarding attribution, accountability, human control, and the legal thresholds of cyber operations. The study concludes that stronger international cooperation, effective AI governance, and meaningful human oversight are essential to protect national security and international stability in the digital era.

Recommendations

States should adopt AI-specific cybersecurity laws to regulate threats such as AI-generated malware, deepfakes, automated ransomware, and cyber deception. International law should also provide clearer standards on when AI-enabled cyber operations amount to unlawful intervention, use of force, or armed attack.

Governments must strengthen cyber attribution mechanisms and ensure meaningful human oversight in AI-related military and cybersecurity operations. Critical infrastructure, including hospitals, banking systems, and energy networks, should receive stronger legal and technical protection against AI-assisted cyberattacks.

International cooperation between states, regional organizations, and technology companies should be enhanced through information sharing, joint cyber responses, and harmonized legal frameworks. At the same time, cybersecurity measures must remain consistent with human rights, privacy, and democratic principles.

Finally, states should work toward a binding international framework governing AI-enabled cyber warfare, particularly regarding attribution, accountability, civilian protection, proportionality, and responsible state behaviour in cyberspace.

REFERENCES

Council of Europe. (2024). *The framework convention on artificial intelligence and human rights, democracy and the rule of law*. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

European Union Agency for Cybersecurity. (2025). *ENISA threat landscape 2025*. https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf

International Committee of the Red Cross. (2024). *International humanitarian law and the challenges of contemporary armed conflicts*. https://www.icrc.org/en/report/2024-icrc-report-ihl-challenges

International Law Commission. (2001). *Draft articles on responsibility of states for internationally wrongful acts*. United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Microsoft. (2025). *Microsoft Digital Defense Report 2025*. https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

Oxford Institute for Ethics, Law and Armed Conflict. (2020). *Oxford statement on the international law protections against cyber operations targeting the health-care sector*. University of Oxford. https://law.yale.edu/sites/default/files/documents/pdf/Faculty/circulation_oxfordstatement_internationallawprotections_cyberoperations_healthcare.pdf

United Nations. (1945). *Charter of the United Nations*. https://www.un.org/en/about-us/un-charter/full-text

United Nations Open-Ended Working Group. (2025). *Final report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025*. United Nations. https://digitallibrary.un.org/record/4084927

Vassilev, A., Oprea, A., Fordyce, A., & Anderson, H. (2025). *Adversarial machine learning: A taxonomy and terminology of attacks and mitigations* (NIST AI 100-2e2025). National Institute of Standards and Technology. https://csrc.nist.gov/pubs/ai/100/2/e2025/final

NATO. (2024, July 10). *Washington Summit Declaration*. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/washington-summit-declaration

NATO. (2024, July 30). *Cyber defence*. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

European Commission. (2024, August 1). *AI Act enters into force*. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.