MEF SCHOOLS MODEL UNITED NATIONS 2026

“Achieving SDGs (Sustainable Development Goals) in line with the 2030 United Nations agenda."

Committee: United Nations General Assembly Sixth Committee (Legal)
Agenda Item: Updating International Legal Principles Applicable to State Conduct in Cyberspace
Student Officer: Ceylin Deniz, Lara Genç

Position: Deputy Chairs

Introduction

The use of the internet has been increasing exponentially worldwide, not just the number of people who use it, but the means we utilize it too. Within a short period of time, the internet became an essential part of our daily lives. Today, anyone can perform day to day business, satisfy their socialisation and entertainment needs, perform professional work, execute financial transactions, and organise governmental interactions via the internet.

Inevitably this progressing range of usage requires national involvement and precise state conduct as internet usage is now widened from abstract cyberspace into real life matters; abusive use of internet, data security, AI, cyber crimes, copyright issues, transaction security, the issue of protecting minors, and national security issues have become integral points of discussion that need solutions. Today all around the world millions suffered at least once from wrongdoing, faced with tangible or intangible damages incurred through the internet. Many countries are faced with national security threats via hacking attempts or espionage.

Given the actual and potential damages and risks on people, private companies, and on the states, taking urgent legal measures turns into one of the utmost domestic and international issues. In this context, it is crucial to update and clarify how current international legal principles apply to state conduct in digital spaces in order to promote responsible state action in cyberspace and maintain international stability, transparency, and accountability. Ensuring that the legal mechanisms reflect the realities of modern cyber operations is essential in safeguarding and enhancing international peace and security on the digital world.

Definition of Significant Terms

Cyberspace:
The internet seen as an imaginary, notional setting in which there are no limits and people can socialize, communicate, network, and learn information regarding any subject (Cambridge Dictionary, Oxford Languages Dictionary)

State Conduct:
The expectations and rules for behaviour regarding the actions of a government, the conduct of a sovereign state (The Law Dictionary)

Distributed Denial of Service (DDOS) Attacks:
An attack in which multiple machines operate together in order to attack one specific target (Cybersecurity and Infrastructure Security Agency)

State Responsibility:
A cardinal principle of international law that holds a state accountable in the case that it has committed "internationally wrongful acts”.

Information and Communication Technologies (ICT):
An umbrella term encompassing all categories of technology utilized for the storing, gathering, transmitting, or processing of information (National Institute of Standards and Technology Glossary)

Cyber Operation:
Actions that are taken in order to target an adversary's information through influence and disruption while ensuring the protection of one's own (Air Force Institute of Technology)

Malicious Cyber Activity:
Any unauthorized cyberspace activities with intentions of disrupting, damaging, or gaining illegal access to various network, data, or computer systems, while also seeking to compromise the confidentiality and/or security of physical or virtual infrastructure. (National Institute of Standards and Technology Glossary)

Detailed Background of the Issue

The Growing Role of Cyberspace in State Activities:

Over time, cyberspace has become an essential part of our lives, playing a key role in politics, economics, security systems, military systems, educational institutions, critical infrastructure systems and many more. Information and Communication Technologies (ICTs) are now essential for the management of critical infrastructure, financial systems, military operations, healthcare services, and democratic processes. Because of this, many countries are utilizing cyberspace to carry out their national security, political, and economic interests.

This growing dependence has also increased governments' exposure to cyber threats. Cyber operations such as hacking, phishing attacks, ransomware, malware, and Distributed Denial Of Service (DDOS) attacks can disrupt vital services, compromise sensitive data, interfere with elections, and harm national security. Regulation and accountability are especially difficult because, in contrast to traditional military operations, cyber operations are usually concealed, hard to identify, and often carried out in ways that remain ambiguous under existing legal frameworks.

These potential risks create the need to update the already existing legal principles in accordance to the emerging technologies and applications of cyberspace. With new technology developing such as artificial intelligence, it's important to keep the related legislation up to date to combat possible threats. Around 177 countries worldwide have adopted comprehensive cybersecurity laws, however it's also important to maintain unison and establish international legal principles on the topic.

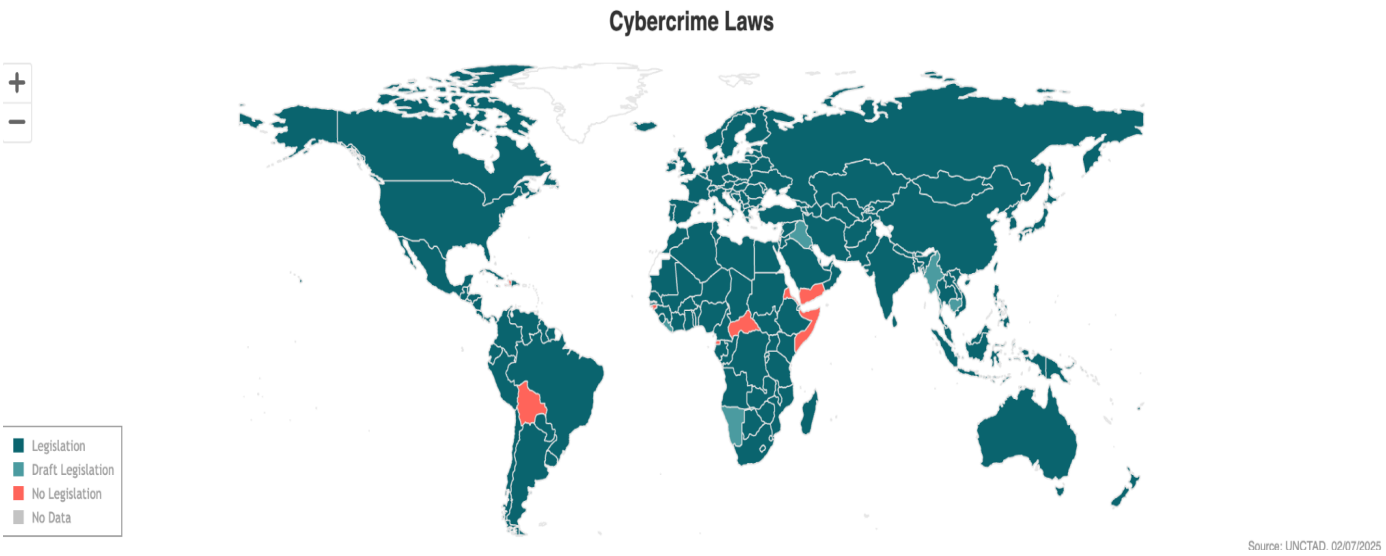

Figure 1: UN Trade and Development (UNCTAD), Cybercrime Legislation Worldwide

The Presence of Malicious Intentions In Cyberspace:

With the usage of cyberspace, both state as well as non-state actors have consistently utilized cyber operations that endanger digital systems, gather sensitive information, disrupt important services, or manipulate environments of information. These activities usually border on the line between traditional espionage and wrongful conduct, especially since many do not inflict any physical damage, yet cause significant economic, political, and security consequences.

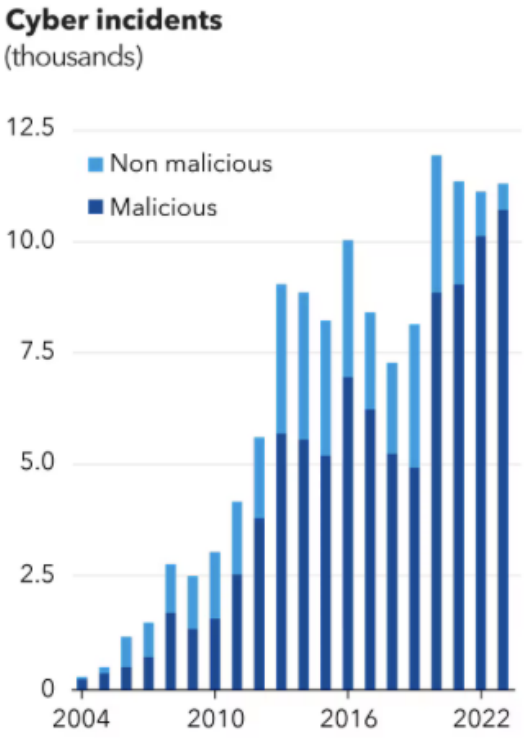

Figure 2: Number of cyber incidents spanning from 2004 to 2022

One example of such cyber activities occurred in 2015 when Ukraine's power grids were hacked through the usage of Russian-led cyber attacks. This heavily damaged Ukraine's infrastructure and targeted regional power distribution companies, which caused several power outages in the region. Dissimilar to conventional operations, cyber activities generally take place below the threshold of armed conflict and might not cause immediate physical damage. This complicates their definition in terms of existing international legal categories and principles.

Cyberspace is not dependent on physical borders and operates transnationally, as seen in the Russian cyberattack against Ukraine in 2015. Digital frameworks and infrastructure often belong to private establishments and frequently span multiple jurisdictions at once. Cyber activities can be employed remotely, routing through multiple states, and implemented by utilizing extensive systems without the knowledge or consent of their owners. This makes it difficult when determining the origin of the operation, the legal jurisdiction that applies, and which state, if there are any, bears responsibility for wrongful conduct, which can cause legal issues in the long run.

Global Recognition of Cyberspace In Terms of International Law:

In the case where international law is applied to cyberspace, the existing principles of international law raise unanswered legal queries, especially those regarding national sovereignty, non-intervention, use of force, and state responsibility. Since most principles of international law were developed in regards to physical borders and territories, complexities arise when such principles are utilized in the context of cyberspace, which doesn't necessarily have any physical borders or limitations.

In most situations, states have varying ideas on how and when these principles apply to cyberspace and cyber activities, particularly where the harm caused is indirect or non-physical. These differing understandings result in legal ambiguities and uncertainties in the global system.

Overall, concerns on the issue of state behaviour in cyberspace have led to frequent meetings and discussions in the United Nations (UN), especially in terms of international peace and security. These discussions illustrate the acknowledgement that cyber operations can have grave consequences in regards to stability, mutual trust between states, and the preservation of civil infrastructure.

Although there is ongoing and consistent dialogue as well as communication between states, the legal definition of cyberspace and its regards to international law continues to be a subject of debate among many Member States.

Timeline of Key Events

1991-1998	The internet is rapidly recognized and used, digital communication technologies/platforms start to reshape state governance, military activities, and economy.

2004	The European Union Agency for Cybersecurity (ENISA) is established
2004-2005	The United Nations General Assembly deploys the first Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, showcasing the first formal UN attempt to investigate cyberspace and state conduct in cyberspace.
2009	The second Group of Governmental Experts (GGE) is established to continue the efforts of the first.
2011	The third Group of Governmental Experts (GGE) is formed for further investigation and examination
2012-2013	The third GGE has a meeting to confirm that international law is indeed relevant and applicable to cyberspace, marking the first acknowledgement of cyberspace in terms of international law applicability.
2015	The fourth GGE is established, soon affirming that the UN Charter applies to state conduct in cyberspace and introducing norms regarding the issue.
2016	The General Data Protection Regulation (GDPR) is introduced by the EU.
2016-2017	The fifth GGE is created, yet it fails to reach an agreement on key legal issues, illustrating the division between states regarding cyberspace in legal contexts.
2019-2021	The United Nations Open-Ended Working Group (OEWG) on ICTs is established, and it thereafter reaffirms that international law is applicable to state conduct in cyberspace, operating from 2019 to 2021.
2022	The second OEWG is established.
2025	The second OEWG disbands and ceases its operations.
2025	The permanent UN ICT body, the Global Mechanism on Developments in the Field of ICTs in the Context of International Security and Advancing Responsible State Behaviour is established.

Major Countries and Organizations Involved

United States:

As one of the most influential states in cyberspace, the United States plays a central role in discussions on updating the international legal principles. As a global economic power and a leader in digital innovation, hosting major internet platforms and artificial intelligence companies, the United States has developed extensive regulations regarding cyberspace at both the federal and state levels.

On May 6, 2024 the United States released their “International Cyberspace & Digital Policy Strategy ”. The integration of cybersecurity with sustainable development and technological innovation, a safe and inclusive cyberspace based on international law (including international human rights law), and a comprehensive policy approach utilizing diplomatic and international tools across the digital ecosystem are the three guiding principles of this strategy paper released.

Recently, it has been announced that the US government is preparing a new cyberspace strategy and new legislation that’s aimed to be released in January 2026, which will be concentrating on six key components intended to combat growing cybersecurity risks due to deficiencies of the existing federal regulations.

United Kingdom:

Since the UK has left the EU in 2020, all sorts of cyberspace regulations have been at the national level in the country. But as a member of most of the international agreements and pacts, the UK has also started some important initiatives like Internet Watch Foundation (IWF), and the national regulations of the UK are in accordance with and comply with EU regulations.

Not long ago on November 12, 2025, The UK Cyber Security and Resilience (Network and Information Systems) Bill was introduced to Parliament by the country’s department of Science, Innovation and Technology. Addressing the flaws, deficiencies, and breaches in the UK's present cybersecurity laws (the Network and Information Systems (NIS) Regulations, 2018) is one of the bill's main objectives, as both the number and the depth of cyberthreats and attacks are increasing.

China:

With the Cybersecurity Law (2017), Data Security Law, and Personal Information Protection Law (2021), China has a state-centered cyber legal framework that focuses mainly on national security and sovereignty.

The Cybersecurity Law of China was enacted in 2017 with the primary goal of enhancing cybersecurity, data localization, and protection for national security. With the emerging technologies, the law has been updated on October 28, 2025, for the first time since 2017 , with the aim of strengthening state support for AI development and raising compliance standards for critical infrastructure and network operators.

European Union (EU):

In a number of areas, the EU has been actively working to improve cybersecurity and data and communication security. It's been the EU's long standing goal to strengthen cooperation, resilience, and a rules-based international order in cyberspace and they have taken many steps in order to achieve this goal.

One of the most important digital laws in the EU, the General Data Protection Regulation (GDPR) was introduced in 2016 and has been in use since May 2018, providing a single, unified framework for data protection. In addition to strengthening cybersecurity and breach management requirements, it seeks to standardize data protection regulations within the EU, protect the privacy and personal data of EU citizens, and make compliance easier for businesses operating abroad.

Apart from GDPR, the EU has taken multiple measurements such as the EU Cyberspace Strategy, The Network and Information Systems Directive (NIS Directive), and the EU Cybersecurity Act that have had/has a significant impact on the issue.

ENISA:

ENISA, the European Union Agency for Cybersecurity, supports EU member states, companies, and institutions by strengthening the EU's cybersecurity framework and supporting the prevention and response to cyberattacks. ENISA offers fundamental cybersecurity to European citizens, supports the private companies and authorities by strengthening cybersecurity, guaranteeing reliable ICT goods and services and improving the cyber policies.

ECSO:

The European Cyber Security Organization (ECSO) is a self-financed, non-profit public-private federation based in Belgium that was founded in 2016 and includes more than 250 members from the field of cybersecurity. It acts as a vital contractual partner of the European Commission, encouraging public-private collaboration to strengthen Europe's cybersecurity resilience and strategic autonomy.

Previous Attempts to Solve the Issue

UN Group of Governmental Experts (GGE) Report, 2021:

The UN Group of Governmental Experts (GGE) report, created under the General Assembly resolution 73/266, emphasizes on responsible state conduct in cyberspace within the framework of international security. The work done for this report being conducted partly during the COVID-19 pandemic, underlined the world's increasing reliance on digital technology and highlighted the necessity of using information and communication technologies (ICTs) responsibly to reduce threats to global peace and security.

The report highlights and adds upon previous GGE reports from 2010, 2013, and 2015, acknowledging that state behavior in cyberspace is subject to current international law standards.

While emphasizing that an open, secure, and peaceful cyberspace, respecting sovereignty, human rights, and sustainable development is in the shared interest of all states, the report also mentions international cooperation, capacity-building, and the participation of non-state actors.

The EU Cybersecurity Act (CSA), 2019:

By giving ENISA a permanent mandate and creating a voluntary EU-wide cybersecurity certification framework for ICT products and services, the EU Cybersecurity Act (Regulation (EU) 2019/881) aims to improve cybersecurity and trust throughout the European Union. The Act also aims to improve overall cyber resilience while reducing the division in the EU's internal market. It also promotes cooperation among member states and offers technical assistance to EU institutions.

The EU Cyber Resilience Act (CRA), 2024:

The EU Cyber Resilience Act (CRA), established December 2024, was designed to improve and enhance the cybersecurity of hardware and software products with digital components by creating mandatory security requirements. In order to improve overall cyber resilience in the EU and make it easier for consumers and businesses to find safe digital products, the act requires the manufacturers to create, produce, and maintain products securely, address vulnerabilities, and provide regular updates regarding their products.

Alternative Solutions

- In order to address the legal ambiguities in relation to state conduct in cyberspace, delegates should examine various attempts and solutions differing in scope. The approaches that should be taken to illustrate this issue should take into account the different perspectives of Member States, especially in regards to diverging views on clarifications of existing laws, developments of new standards, or the strengthening of present mechanisms. Overall, delegates should keep in mind the pathways addressed in United Nations assemblies and forums while developing solutions that define legal clarity, predictability, security, and stability in cyberspace.

- A possible solution method would be to establish a voluntary legal dialogue forum and/or platform in order to provide room for consistent legal discussions on cyberspace, enabling Member States to present their differing views while revisiting interpretations as technologies continue to improve. This would promote communication as well as cooperation through a procedural approach, aligning with the 17th Sustainable Development Goal, “Partnerships for the Goals”.

- Additionally, many developing states are faced with challenges in fully involving themselves in discussions regarding the issue at hand due to limited legal as well as institutional capacity, causing them to be unable to express their own views or perspectives. To combat this, capacity-building measures or initiatives focusing on international cyberspace law could assist these states in comprehending and articulating legal positions in relation to state conduct in cyberspace. These measures and/or

initiatives could include UN-supervised legal training programs, workshops, and expert knowledge exchanges, without the breach of national sovereignty.

- Another alternative solution could be the implementation of confidence-building and transparency mechanisms between states. Voluntary bilateral or multilateral agreements could be made that regard commitments between member states to notify other nations in cases of important/significant cyber incidents with possible cross-border impacts. Such intelligence-sharing could enable predictability and reduce miscalculation risks, allowing states to better prepare themselves for malicious intentions enacted through cyberspace. It is important to note that state involvement in such transparency approaches should be voluntary to not infringe on national sovereignty, state confidentiality, or domestic security.

- Lastly, it would be effective to develop an international, unbiased framework that highlights shared perspectives of lawful and wrongful state conduct in cyberspace, outlining the details and implications of the specifics. This framework should be non-binding, and rather than impose legal implications, it should contribute to the evolution of international law in the context of state conduct in cyberspace.

Useful Links

https://ccdcoe.org/library/publications/overview-of-un-oewg-developments-continuation-of-discussions-on-how-international-law-applies-in-cyberspace/
https://dig.watch/cyber-norms
https://www.coespu.org/articles/can-international-law-be-applied-cyberspace
https://www.unodc.org/unodc/cybercrime/convention/home.html
https://dig.watch/resource/oewg-report-2021-2025
https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf
https://www.unoda.org/en/our-work/emerging-challenges/developments-field-information-and-telecommunications

Bibliography

1. Council of the European Union. *Council Conclusions on Cybersecurity.* Council of the European Union, 2024, data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf. Accessed 30 Dec. 2025
2. United States Department of State. "Building Digital Solidarity: The United States International Cyberspace and Digital Policy Strategy." *U.S. Department of State*, n.d., www.state.gov/building-digital-solidarity-the-united-states-international-cyberspace-and-digital-policy-strategy/. Accessed 30 Dec. 2025
3. Sayegh, Emil. "Trump Administration Prepares New Cybersecurity Strategy for 2026." *Forbes*, 21 Dec. 2025,

www.forbes.com/sites/emilsayegh/2025/12/21/trump-administration-prepares-new-cybersecurity-strategy-for-2026/. Accessed 31 Dec. 2025
4. United States Department of State. *United States International Cyberspace and Digital Strategy.* U.S. Department of State, 15 May 2024, www.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf. Accessed 30 Dec. 2025
5. Timmons, Joe, et al. "Reform of the UK's Cybersecurity Regime: What to Expect." *White & Case*, www.whitecase.com/insight-alert/reform-uks-cybersecurity-regime-incoming. Accessed 30 Dec. 2025
6. Chin, Kyle. "Cybersecurity Laws and Regulations in the UK." *UpGuard*, www.upguard.com/blog/cybersecurity-laws-regulations-uk. Accessed 31 Dec. 2025
7. LawInfoChina. "Cybersecurity Law of the People's Republic of China." *LawInfoChina*, www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3. Accessed 31 Dec. 2025
8. China Briefing."China Amends Its Cybersecurity Law." *China Briefing*, www.china-briefing.com/news/china-cybersecurity-law-amendment/. Accessed 31 Dec. 2025
9. Sen, Kaushik. "Cybersecurity Regulations in the European Union." *UpGuard*, www.upguard.com/blog/cybersecurity-regulations-in-the-european-union. Accessed 1 Jan. 2026
10. European Union Agency for Cybersecurity (ENISA). *ENISA – The EU Agency for Cybersecurity*, www.enisa.europa.eu/. Accessed 1 Jan. 2026
11. European Cyber Security Organisation (ECSO). *European Cyber Security Organisation*, ecs-org.eu/. Accessed 1 Jan. 2026
12. European Union. "The EU Cybersecurity Act." *EUR-Lex*, eur-lex.europa.eu/EN/legal-content/summary/the-eu-cybersecurity-act.html . Accessed 1 Jan. 2026
13. United Nations. *Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations Digital Library, digitallibrary.un.org/record/3934214?ln=en&v=pdf. Accessed 1 Jan. 2026
14. European Commission. "Cyber Resilience Act." *European Commission Digital Strategy*, digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act. Accessed 1 Jan. 2026
15. United Nations Conference on Trade and Development. "Cybercrime Legislation Worldwide." *UNCTAD*, unctad.org/page/cybercrime-legislation-worldwide. Accessed 1 Jan. 2026
16. United Nations. *Article 4. Conduct of Organs of a State*. *Materials on the Responsibility of States for Internationally Wrongful Acts*, Part One: Chapter II, United Nations Legislative Series, 2nd ed., 2023, legal.un.org/legislativeseries/pdfs/chapters/book25/english/book25_part1_ch2_art4.pdf.
17. Tiirmaa-Klaar, Heli. *The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body*. Cyberstability Paper Series, The Hague Centre for Strategic Studies & Global Commission on the Stability of Cyberspace, Dec. 2021, https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

18. *AFIT / Graduate School of Engineering & Management*, www.afit.edu/EN/programs.cfm?a=view&D=13. Accessed 2 Jan. 2026.
19. *Cyber-Attack against Ukrainian Critical Infrastructure | CISA*, www.cisa.gov/uscert/ics/alerts/IR-ALERT-H-16-056-01. Accessed 1 Jan. 2026.
20. "Cyberspace: Definition and Implications." *CCDCOE*, ccdcoe.org/library/publications/cyberspace-definition-and-implications/. Accessed 1 Jan. 2026.
21. Editor, CSRC Content. "Information and Communications Technology (ICT) - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/information_and_communications_technology. Accessed 1 Jan. 2026.
22. Editor, CSRC Content. "Malicious Cyber Activity - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/malicious_cyber_activity. Accessed 1 Jan. 2026.
23. "Global Financial Stability Is at Risk Due to Cyber Threats, the IMF Warns. Here's What Needs to Happen." *World Economic Forum*, www.weforum.org/stories/2024/05/financial-sector-cyber-attack-threat-imf-cybersecurity/ . Accessed 1 Jan. 2026.
24. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security :" *United Nations*, United Nations, digitallibrary.un.org/record/799853?ln=en&v=pdf. Accessed 1 Jan. 2026.
25. *The Sixth United Nations GGE and International Law in Cyberspace*, www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/. Accessed 2 Jan. 2026.
26. Staff, TLD. "Professional Conduct." *The Law Dictionary*, The Law Dictionary, 27 Mar. 2017, thelawdictionary.org/professional-conduct/#:~:text=Definition%20and%20Citations:,state%20and%20local%20bar%20associations.
27. "State Responsibility." *State Responsibility | How Does Law Protect in War? - Online Casebook*, casebook.icrc.org/a_to_z/glossary/state-responsibility. Accessed 1 Jan. 2026.
28. *Understanding Denial-of-Service Attacks | Cisa*, www.cisa.gov/news-events/news/understanding-denial-service-attacks. Accessed 2 Jan. 2026.