Massachusetts Institute of Technology

Model United Nations Conference

Background Guide

Table of Contents

Letter from the Secretary General

Dear Delegates,

I am very excited to welcome you to Massachusetts Institute of Technology's 17th annual Model United Nations Conference - MITMUNC XVII! After months of planning, training and organizing, we hope this conference will be a new, challenging, and enriching experience for you.

With all the difficulties the world has experienced last year and is currently still experiencing, we still look forward to a brighter future. Building a sustainable future requires a lot of collaboration and effort and we are all hopeful to see that from you, the leaders of tomorrow.

This year, we decided to focus on technology and its impact on our societies and the whole world to test the pros and cons of technological advancement. Tech diplomacy is an important theme that defines MITMUNC XVII, especially with the prevalence of Artificial Intelligence. Technological advancements have paved the way for great and helpful solutions, yet they also opened up space for tech-abuse, which really makes us think, where are we heading? What's next? Dialogue, international relations and collaborations create the backbone of tech diplomacy and we are all looking forward to see your creativity spark during the conference to help implement tech diplomacy around the world, and fight technology-abuse that harms the international community.

Having experienced MITMUNC as a chair, then as a Secretary General, I am humbled and thrilled to guide MITMUNC into its best conference yet. Do not hesitate in contacting me or the secretariat team should you encounter any doubts along the way. I wish you the best of luck!

Sincerely,

Your Secretary General, Jad Abou Ali

For further inquiries, do not hesitate to contact us at sg-mitmunc@mit.edu.

MITMUNC XVII 2025

Letter from the Chairs

Dear Delegates,

Welcome to the 17th annual MIT Model United Nations Conference and to the International Court of Justice Committee! We're excited about the topics for this year and are truly looking forward to being your chairs.

I'm Rishika, a junior studying computer science and political science here at MIT. I have been part of our Model UN club for the last three year and have served as both a chair and secretariat member. In high school, I was involved with both MUN and Speech and Debate (Extemporaneous Speaking), with a focus on international current events. I think MUN is an amazing way to learn about the world around us and the challenges we face. I'm so excited to work with you all later this year.

My name is Lama Diriyeh, and I'm a sophomore at MIT studying Mechanical Engineering. I have been doing MUN since I was a freshman in high school. More than being an excellent space for practicing public speaking it also created a space of constructive discussions of relevant topics of global concern. Through organizing conferences, chairing committees, and being a delegate myself, I got the opportunity to meet exceptional people and form wonderful friendships. I hope you use this time to build long-lasting skills and strong relationships, and most importantly enjoy it to the most.

The two topics for this weekend address ongoing disputes in the Western Sahara and the use of cyber operations, specificially in warfare. We hope you'll use this weekend not only to learn more about these topics, but also to collaborate in creating lasting solutions.

Sincerely,

Your Chairs: Lama Diriyeh & Rishika Bansal

For further inquiries, do not hesitate to contact us at icj-2025@mit.edu.

MITMUNC XVII 2025

Committee Introduction

The World Court, officially known as the International Court of Justice (ICJ), emerged from the 1945 San Francisco Conference on International Organizations and began its mandate in April 1946. Established to resolve inter-state legal disputes, it operates through contentious cases—binding rulings on disputes between consenting member states—and advisory opinions for authorized UN organs.

Comprising 15 judges elected by the UN General Assembly and Security Council for nine-year terms, the ICJ abides by legal documents like the UN Charter, the Court's Statute, the Rule of the Court, and Practice Directions. Its jurisdiction covers disputes among UN member states while offering advisory opinions, exemplified in its counsel on Kosovo's statehood in 2011.

As the principal judicial organ of the UN, the ICJ settles disputes submitted by parties under its statute, excluding intervention in state matters. While all 193 UN member states adhere to the ICJ Statute, provisions exist for non-member entities. Unlike other UN bodies, the ICJ prioritizes resolving disputes based on international law rather than drafting resolutions, emphasizing the judges' adherence to international legal principles.

Functioning as the sole international court for inter-nation disputes, the ICJ has handled over 177 cases since 1949. Nevertheless, challenges persist in pursuing impartial justice globally. Criticisms of bias have arisen, exemplified by instances like the Nicaragua v. United States case, revealing limitations due to the Security Council's power to veto ICJ decisions. Furthermore, the ICJ faces hurdles in securing jurisdiction over contentious cases, relying heavily on the consent of conflicting parties for exercising its authority.

This MUN committee is highly challenging, but we will make sure it’s also an exceptional learning opportunity.

Topic A: Western Sahara

I. Introduction

The Western Sahara lies in the western most region of the Sahara. It has borders mostly with Morocco to the North, slightly with Algeria to the Northeast and mainly with Mauritania to the South and East. It has two main regions Río de Oro, the southern two thirds of the region, and Saguia el-Hamra the northern third. Geographically it is mostly a desert with important resources including iron and potash ore, as well as a large reserve of phosphate near Bu Craa. [6]

Fig. 1. United Nations, Map No. 3175 Rev. 4, Oct. 2012 [4]

II. History

A. Pre-Colonization

The region had established trading ties with Europe by the 4th century BCE. It had contact with the Romans, and was later occupied by the Ṣanhajāh Amazigh, who later were dominated by Muslims around 1000 CE. Portuguese and Spanish colonial discoveries and claims over the region were limited, however, in 1884, The Spanish Society of Africanists and Colonists established treaties with the local population in the coastal region of Río de Oro. Spain then claimed protectorate over the coastal region. Their colonial expansion was impeded by the French colonial expansion in Mauritania and the establishment of Semara between 1898-1902 by Sheikh Mā' al-'Aynayn. Nevertheless, the Spanish rule over the region expanded until it had complete control of the Western Sahara by 1934. [6]

B. During and Post Spanish Colonization

In 1957, newly independent Morocco claimed authority over the territory, and its military was repelled by the Spanish troops. A year later, Spain declared both Río de Oro and Saguia el-Hamra one Spanish province: Spanish Sahara. Joining the conflict, Mauritania, also newly independent, claimed authority over the region in 1960. To complicate the situation, the phosphate reserves near Bu Craa were discovered in 1963, making the territory not only strategic geographically but also a resourceful profitable territory. [6]

By the 1970s, The Polisario Front (Popular Front for the Liberation of Saguia el-Hamra and Río de Oro), a guerrilla insurgency, was established by the indigenous Sahrawi people. Consequently in 1975, Spain declared it will withdraw from the area and partitioned the Western Sahara between Morocco and Mauritania even though the World Court (ICJ) declared both their claims to the territory tenuous. Morocco was given the northern two thirds -with the phosphate reserves- and Mauritania the remaining southern third. The Polisario Front became based in Algeria, which supported the Sahrawis' right to independence and sovereignty. Fighting ensued between the Polisario Front and both countries and in 1976, the Front declared a government in exile of the Saharan Arab Democratic Republic (SADR). [6]

By 1979, Mauritania left the conflict and established a peace agreement with the Polisario Front, but Morocco simply took control of their portion of the Western Sahara and fortified the region. [6]

In 1988 the UN proposed a solution to the conflict allowing the Sahrawi people to decide who they would prefer to be ruled by: the Polisario Front, or Morocco in a referendum conducted by the UN. After both parties accepted the referendum and agreed on a cease-fire in 1991, Morocco moved tens of thousands of "settlers" into the territory and requested the UN assess their voting rights before the referendum is conducted. A process which dragged on into the early 2000s with Morocco continuously expanding its rule and infrastructure in the region. [6]

Despite these setbacks as well as Algeria's diminished material capacity of support for the Polisario Front (though its diplomatic support remained unwavering), it continued its diplomatic effort for self-determination. In 2001, the new Moroccan King declared Morocco will no longer agree to a referendum in Western Sahara. UN peace efforts continued with renewing the peacekeeping forces in the region and proposing new resolutions which got rejected by Morocco. In 2007, Morocco suggested a plan that includes autonomy within the Moroccan state, but no referendum, which was rejected by the Polisario Front. After the fighting ensued again between the parties in 2020, the US became the first country to recognize Moroccan sovereignty over the region in exchange for normalization of ties with Israel, and in 2023 Israel followed in exchange for an embassy. [6]

III. International Actions

As mentioned in the previous section, the UN had several proposed resolutions and negotiation efforts mostly with no fruitful results. Since 1963 the UN has listed Western Sahara as a Non-Self-Governing Territory awaiting decolonization.[4] In 1974, the ICJ published its advisory opinion on the Western Sahara in response to two questions:

I. "Was Western Sahara (Rio de Oro and Sakiet El Hamra) at the time of colonization by Spain a territory belonging to no one (terra nullius)?"

II. "What were the legal ties between this territory and the Kingdom of Morocco and the Mauritanian entity?"

The answer to I was negative, and the answer to the II in brief was that evidence supports the existence of legal ties of allegiance between the Sultan of Morocco and some of the local tribes, as well as the existence of similar ties between the Mauritanian entity and the territory of Western Sahara. The court concluded, however, that there is no evidence to any territorial sovereignty between the territory of Western Sahara and the Kingdom of Morocco or the Mauritanian entity. [5]

IV. Countries' Positions

As mentioned previously the US recognizes Moroccan sovereignty over the region, a declaration that was rejected by the UN, EU, and the African Union (AU). Several European countries including Spain and Germany strongly opposed the proclamation and lobbied with other EU members preventing the EU from following the US's proclamation. The African Union which recognizes the SADR as a member state supports the Sahrawi people's right to self-determination and urged Morocco to respect colonial borders (border that existed at the time of independence). [1]

V. Projections and Implications

The people of the Western Sahara are obviously heavily affected by the issue, economically, and politically. This conflict has been ongoing for over 60 years and has affected the diplomatic relations and cooperation between involved countries. The natural reserves in the Western Sahara especially the phosphate reserves are crucial to global food supply chains, and the rekindled conflict could disrupt the extraction and processing. [2]

VI. Conclusion

It is essential to consider current resolutions on the table as well as the demands and claims of both parties in forming a resolution and to keep the rights of the people of Western Sahara at the forefront of the efforts to resolve the issue. Understanding past resolutions and why they didn't succeed, as well as countries' positions and their development over time will also be important in the process.

VII. Questions to be Addressed

- How can the UN address the human rights problems in the Western Sahara and the refugee camps for Sahrawi people in Algeria?
- What is the most viable, just resolution to the conflict given the current situation that would grant the Sahrawi people their right to self-determination?
- How can the international community, including the UN, EU, AU, and others contribute to the advancement of a resolution to the conflict?

VIII. Bibliography

1. Chograni, Houda. "The Polisario Front, Morocco, and the Western Sahara Conflict." *Arab Center Washington DC*, 8 July 2021, arabcenterdc.org/resource/the-polisario-front-morocco-and-the-western-sahara-conflict/.
2. Sun, Esther. "What Does the Western Sahara Conflict Mean for Africa?" *Council on Foreign Relations*, Council on Foreign Relations, www.cfr.org/in-brief/what-does-western-sahara-conflict-mean-africa. Accessed 9 Jan. 2025.
3. "Western Sahara Profile." *BBC News*, BBC, 28 Oct. 2024, www.bbc.com/news/world-africa-14115273.
4. "Western Sahara | The United Nations and Decolonization." *United Nations*, United Nations, www.un.org/dppa/decolonization/en/nsgt/western-sahara. Accessed 9 Jan. 2025.
5. *Western Sahara*, www.icj-cij.org/case/61. Accessed 9 Jan. 2025.
6. "Western Sahara." *Encyclopædia Britannica*, Encyclopædia Britannica, inc., 21 Dec. 2024, www.britannica.com/place/Western-Sahara.

Topic B: Legality of the Threat and Use of Cyberwarfare and Operations

I. Introduction

Over the last two decades, state-sponsored cyber operations have slowly become a more prominent military and government strategy. Cyber operations can be defined as activities in cyberspace that are intended to project power through the application of force (CSRC Content Editor). This may include employing capabilities to "manipulate, deny, disrupt, degrade, or destroy targeted computers, information systems, or networks" (Hanson et al. 1). State-sponsored cyberoperations are those specifically perpetrated by a state or state-affiliated actor.

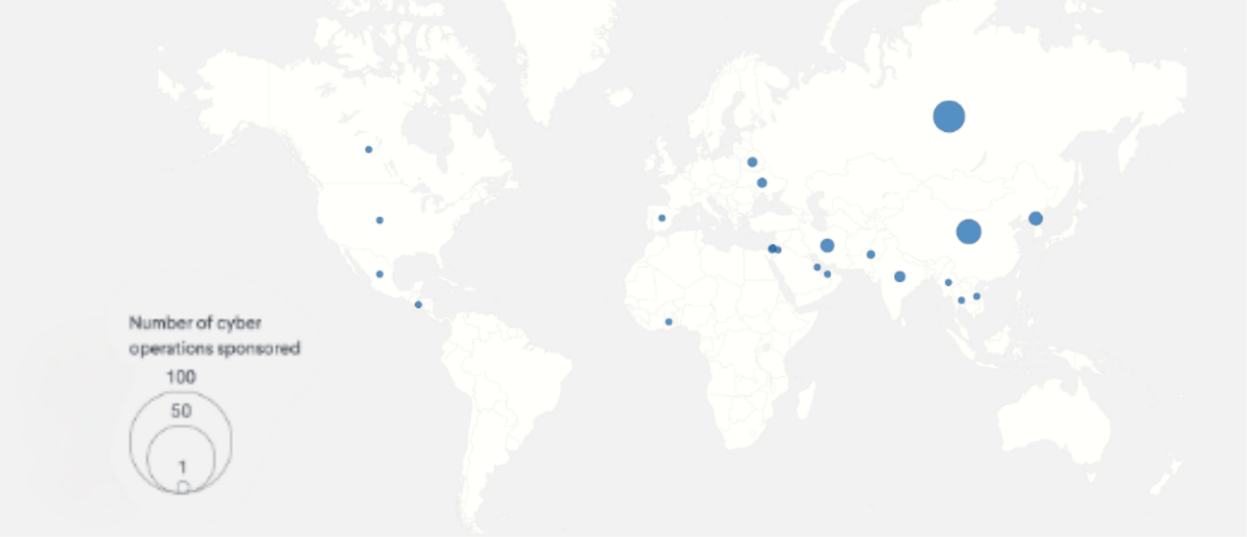

Figure 2. *Number of cyber operations sponsored by each state in 2023*

The number of cyber offensives undertaken by states has increased dramatically in this century, from nineteen in 2005 to 124 in 2023. Some of the most notable cyber operations have been the Georgia operation (2008), Stuxnet (2010), WannaCry (2017), NotPetya (2017), SolarWinds (2020), and Salt Typhoon (2024). All of these were responsible for millions of dollars worth of damage in the form of stolen information or impaired infrastructure. In the last five years, the number of yearly cyber

operations has remained relatively constant at 125, with a brief spike in 2022 at the onset of the Russia-Ukraine war (Council on Foreign Relations). These operations range in nature and may include ransomware attacks, information-theft and cyber espionage, disinformation campaigns, critical infrastructure attacks (via worms or malware), and distributed denial-of-service attacks (DDoS). Although the form and function of cyber operations vary greatly, the perpetrators do not. Nearly 80% of all suspected cyber operations since 2005 have been carried out by one of four states: China, Iran, North Korea, or Russia (Council on Foreign Relations).

Some of the aforementioned cyber operations fall under the subcategory of cyberwarfare. Cyberwarfare refers to any cyber operations that are conducted through military means in order to achieve military objectives (Schmitt 564). The most recent example of cyberwarfare is within the Russia-Ukraine war, where both countries have used their cyber capabilities to target the security of information and infrastructure in the other (*Significant Cyber Incidents | CSIS*).

Although both cyberwarfare and state-sponsored cyberoperations can severely and significantly hurt opposing governments and civilians, there are currently very few international laws explicitly addressing their use. The General Assembly has requested an **advisory opinion** on applying existing international law to cyberwarfare and cyber operations.

II. History

A. Cyber Operations Supporting Geopolitical Goals

The first recorded cyber operation occurred just days after the ARPANET, the precursor to the modern internet, was launched in 1969. Researcher Bob Thomas created a program called Creeper that could move across ARPANET's network, leaving a message that read: "I'm the creeper, catch me if you can" (Kemper). This harmless experiment laid the groundwork for future, more dangerous, cyber operations. In 2007, Estonia experienced one of the first large-scale cyberattacks. Following a political dispute with Russia over the relocation of a Soviet-era war memorial, Estonia's digital infrastructure was hit by massive denial-of-service (DDoS) attacks that crippled banks, government agencies, and media websites (Council on Foreign Relations). This attack highlighted the vulnerabilities of highly networked

societies and was the first time a state threatened another through primarily cyber operations. Since then, states have increasingly relied on their cyber capabilities to affect their geopolitical goals.

The 2010 Stuxnet worm was a landmark event in state-sponsored cyber operations. Allegedly developed by the United States and Israel, Stuxnet was designed to sabotage Iran's nuclear facilities by targeting its industrial control systems (Sanger). This was the first instance of malware engineered to cause physical damage to critical infrastructure, signaling a shift from cyber espionage to direct offensive tactics. Most recently, the Salt Typhoon hack targeted the global financial sector in November 2024. The hack caused billions of dollars in losses and disrupted financial markets worldwide using advanced cryptographic techniques (Miller et al.). As technology continues to evolve, and global networks become more interconnected, state-sponsored cyber operations may become both more intricate and impactful.

B. Russia-Ukraine and Broader Cyberwarfare

The Russia-Ukraine conflict has become a critical case study in the evolution of cyberwarfare, demonstrating how cyber operations can be integrated into traditional military strategies. The 2008 Russia-Georgia war provided an early glimpse into Russia's approach, as Georgia's government websites were struck by cyberattacks just before Russian military forces entered the country (Council on Foreign Relations). These DDoS attacks disrupted communication and weakened Georgia's ability to respond, marking one of the first clear examples of hybrid warfare, where cyber operations were used in conjunction with physical military actions to further military goals.

In the current Russia-Ukraine conflict, which has been called the first true cyberwar and has brought into question how current international laws apply to this relatively new sphere, Russian forces have repeatedly used misinformation campaigns, intelligence operations, and infrastructure attacks to support their military strategy against Ukraine (*Significant Cyber Incidents | CSIS*). In 2015, Russia allegedly launched a cyberattack that temporarily knocked out parts of Ukraine's power grid—the first known cyberattack to cause a power outage. This set a precedent for the use of cyber tools to cause

widespread societal and infrastructure damage. Ukraine has launched counter cyber-offensives as well, mostly in the sphere of intelligence-gathering and disinformation (*Significant Cyber Incidents | CSIS*).

The Middle East has also emerged as a critical battleground for cyberwarfare, with countries like Iran and Israel actively developing and deploying cyber capabilities. In 2020, Iranian hackers targeted Israeli water treatment facilities, attempting to increase chlorine levels to dangerous limits (Council on Foreign Relations). Israel responded with cyberattacks that temporarily shut down Iran's port systems (Bergman and Halbfinger). Saudi Arabia has also been the target of cyberattacks, most notably the 2012 Shamoon virus attack perpetrated by Iran, which crippled the Saudi national oil company, Saudi Aramco (Council on Foreign Relations).

As Iran, Israel, and other regional powers invest more heavily in cyber capabilities, the Middle East has become a hotbed of cyber conflict. These cyber operations are often covert, making attribution difficult, but they carry significant strategic implications. In the context of broader geopolitical tensions, cyberwarfare in the Middle East is being used to supplement conventional military strategies, sabotage critical infrastructure, and exert pressure on adversaries without escalating to direct armed conflict.

III. International Actions

The United Nations has addressed the issue of cyberwarfare through various forums, with the UN Group of Governmental Experts (GGE), International Committee of the Red Cross (ICRC), UN General Assembly, and the final UN Open-Ended Working Group (UNOEG) affirming that international law, including the UN Charter and International Humanitarian Law (IHL), applies to cyberspace (Press and information team of the Delegation to the UN in New York). IHL is the set of rules that lay out what can and cannot be done in an armed conflict. These rules are primarily derived from the four Geneva Conventions of 1949, although additional provisions may be found in the Additional Protocols of 1977, etc. ("What Is International Humanitarian Law Factsheet"). However, the application of IHL to cyber operations remains complex. Questions such as what constitutes an

"armed attack", how state sovereignty expands into cyberspace, and measurement of impact remain largely unaddressed.

The Tallinn Manual 2.0, a non-binding document, offers guidance on applying IHL to cyber operations, but it lacks formal international legal authority. It states that cyber attacks must rise to the level of an armed conflict (or be part of an armed conflict) to be regulated by IHL (Schmitt Rule 80(3)). For instance, the 2007 cyberattacks on Estonia, causing $1 million in damage, were not considered to fall under IHL, while the 2008 cyber operations between Georgia and Russia were regulated by IHL as they were conducted in furtherance of an existing conflict (Echr). The GGE report also suggests that the Law of Armed Conflict, Law of State Responsibility, and the UN Charter more broadly should be applied to cyber operations (Hsu and Murray).

IV. Countries' Positions

States like the United States, Russia, and China have expressed support for certain IHL principles in relation to cyber operations, though there remains significant disagreement over issues such as attribution, sovereignty, and the use of force in cyberspace. Russia has repeatedly advocated for a new legal instrument to help apply IHL to cyberspace, largely due to their ongoing usage of cyber operations for military and geopolitical gain (Lumiste). Iran has published a declaration on its position on applications of international law to cyberspace, but notably made no mention of IHL (Schmitt and Schmitt). States who have suffered extensively from cyberattacks, such as Ukraine and EU member states, have underlined their support of the UN framework of responsible state behavior in cyberspace ("Ukraine: 3rd Cyber Dialogue With the European Union Takes Place in Brussels").

V. Projections and Implications

Cyberwarfare has the ability to affect severe and immediate economic, social, and infrastructural damage to another state. With ongoing offensive uses of cyber operations against Ukraine, and past instances against nearly every country with a well-developed cyber architecture,

cyberattacks not only cost states billions of dollars every year, but have the potential to completely shift the geopolitical landscape.

VI. Conclusion

The regulation of cyber operations and cyberwarfare has become increasingly necessary both because of the frequency and intensity of cyberattacks. Whether through applying existing international laws or creating a new mechanism for regulation, the international community must establish clear frameworks to address the legal and ethical challenges posed by cyber operations. The current ambiguity surrounding the application of international law to cyberspace creates risks for states and civilians alike, as cyberattacks can easily escalate conflicts without appropriate standards in place.

VII. Questions to be Addressed

- When does a cyber operation constitute an "armed attack"?
- Beyond physical damage, how should damage relegated within cyberspace (such as data theft or network disruption) be addressed?
- How should state sovereignty within cyberspace be measured, especially with regard to transnational networks or information-flow?
- Based on the above questions, when and how does international humanitarian law, the law of armed conflict, and the UN Charter apply to cyberwarfare and operations?

VIII. Bibliography

BBC News. "Ransomware Cyber-attack: Who Has Been Hardest Hit?" *BBC News*, 15 May 2017, www.bbc.com/news/world-39919249.

Bergman, Ronen, and David Halbfinger. "Israel Hack of Iran Port Is Latest Salvo in Exchange of Cyberattacks." *The New York Times*, 19 May 2020, www.nytimes.com/2020/05/19/world/middleeast/israel-iran-cyberattacks.html.

Clark, Sam. "Winter Is Coming. So Are Russia's Elite Hackers." *POLITICO*, 22 Nov. 2024, www.politico.eu/article/russia-hackers-europe-winter-energy-infrastructure-moscow-gas-hike-digital.

Council on Foreign Relations. "Cyber Operations Tracker." *Council on Foreign Relations*, www.cfr.org/cyber-operations.

CSRC Content Editor. *Offensive Cyberspace Operations (OCO) - Glossary | CSRC*. csrc.nist.gov/glossary/term/offensive_cyberspace_operations.

Echr. *HUDOC - European Court of Human Rights*. hudoc.echr.coe.int/fre?i=001-224473.

Hsu, Kimberly, and Craig Murray. *China and International Law in Cyberspace*. US-China Economic and Security Review Commission, 6 May 2014, www.uscc.gov/sites/default/files/Research/China%20International%20Law%20in%20Cyberspace.pdf.

Kemper, Kathy. "'I'm the Creeper; Catch Me If You Can!'" *The Hill*, 18 May 2011, thehill.com/blogs/pundits-blog/technology/91595-im-the-creeper-catch-me-if-you-can.

Lumiste, Liina. "There and Back Again? Russia's Quest for Regulating War in Cyberspace." *Polish Yearbook of International Law*, vol. XLIII, 2023, pp. 239–60, doi:10.24425/PYIL.2024.152300.

Miller, Maggie, et al. "We Need to Talk About Salt Typhoon." *Politico*, 12 Dec. 2024, www.politico.com/newsletters/national-security-daily/2024/12/12/we-need-to-talk-about-salt-typhoon-00183727.

Press and information team of the Delegation to the UN in New York. "EU Statement – UN Open-Ended Working Group on ICT: International Law." *EEAS*, www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-international-law-2_en?s=63.

Sanger, David. "Obama Order Sped up Wave of Cyberattacks Against Iran." *The New York Times*, 1 June 2012, www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all&_r=0.

Schmitt, Michael N., and Michael N. Schmitt. "Noteworthy Releases of International Cyber Law Positions—PART II: Iran." *Lieber Institute West Point*, 6 Sept. 2024, lieber.westpoint.edu/iran-international-cyber-law-positions.

Significant Cyber Incidents | CSIS. www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

"Ukraine: 3rd Cyber Dialogue With the European Union Takes Place in Brussels." *Shaping Europe's Digital Future*, 15 July 2024, digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels.

US Department of Justice Office of Public Affairs. *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions*. 13 July 2022, www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

"What Is International Humanitarian Law Factsheet." *ICRC Advisory Service*, International Committee of the Red Cross, July 2004, www.icrc.org/sites/default/files/document/file_list/what-is-ihl-factsheet.pdf.