DUMUNC XL

Background Guide

United Nations Commission on Science and Technology for Development

Chairs

Table of Contents

Letter from the Dais **3**

Topic A: The Role of Technology in Medicine: Balancing Innovation and Cybersecurity **4**

A.1 - Introduction **4**

A.2 - Background and Significance **4**

A.2.i - Artificial Intelligence **4**

A.2.ii - Smart Medical Devices **5**

A.3 - Risks and Implications **5**

A.3.i - Artificial Intelligence **6**

A.3.ii - Smart Medical Devices **6**

A.4 - Questions to Consider **7**

Additional Committee Information **8**

Additional Sources and Reading **9**

Letter from the Dais

Dear Delegates,

It is our pleasure to welcome you to DUMUNC 2024! We're honored to serve as the chairs of DUMUNC's Commission on Science and Technology for Development, and we look forward to working with you all.

The CSTD was created to provide "a forum where countries can raise critical challenges and explore opportunities presented by rapid technological development." Technology is advancing at a faster pace than ever before, and each new innovation brings with it a host of questions:How can nations protect healthcare infrastructure from cyberattacks while encouraging the development of cutting-edge medical solutions? What role should international cooperation play in setting cybersecurity standards for AI and medical devices? The nature of these problems is evolving literally from day to day, and so we encourage you to come to the committee having thoroughly researched their history, and previous/proposed solutions, as well as their intersection with your country's policy concerns. We hope this background guide will be helpful to you as you dive into the nuances of these issues.

If you have any questions or concerns as you're preparing for this committee, please feel free to reach out to any of us. Once again, welcome to the CSTD — we can't wait to meet you, and we're excited to see what solutions you'll bring to the table! Welcome to UNCSTD at DUMUNC 2025!

Sincerely,

Ashley Deleon
aed52@duke.edu

Tyler Walley
tjw38@duke.edu

Topic A: The Role of Technology in Medicine: Balancing Innovation and Cybersecurity

A.1 - Introduction

"A life saving medical device can also become a weapon." While this may seem like a contradiction, it is an increasingly relevant issue as technology continues to play a larger role in modern healthcare.

The twenty-first century has witnessed groundbreaking advancements in technology, transforming not only how we live and work but also how we approach medicine. Artificial Intelligence (AI) and other smart technology are revolutionizing medicine. AI assists doctors in diagnosing diseases and personalizing treatments, while smart medical devices like insulin pumps and robotic surgery systems enhance patient care. However, with this innovation comes a serious threat: cyberattacks on medical technology.

This committee will explore the critical questions: How can nations maximize the benefits of AI and smart medical devices while ensuring strong cybersecurity protections? How can the international community ensure that technology in healthcare remains a tool for saving lives, and not a vulnerability?

A.2 - Background and Significance

The healthcare industry has experienced a significant transformation in recent decades, largely fueled by the integration of technology. Technology has become an integral part of the healthcare system. To understand the scope of its impact, it is important to examine several key areas where innovation is reshaping the field.

A.2.i - Artificial Intelligence

One of the most transformative technologies in modern medicine is AI. AI is revolutionizing various facets of healthcare, including diagnostics, and patient care. Algorithms powered by AI can analyze complex medical images, such as X-rays and MRIs, predict patient outcomes, and generate personalized treatment plans based on extensive datasets. Notable AI systems like IBM

Watson Health and Google DeepMind are already demonstrating promising results, assisting doctors in diagnosing diseases such as cancer and eye conditions with greater speed than traditional methods.

Building on these advancements, robotic surgery has emerged as a significant breakthrough in healthcare. Several hospitals have begun using robot-assisted surgeries to reduce human error and enhance precision. One notable example is the da Vinci Surgical System, which allows surgeons to control instruments with great accuracy. The system, "translates [the] surgeon's hand movements at the console in real time, bending and rotating the instruments while performing the procedure…[It also] delivers highly magnified, 3D high-definition views of the surgical area."[1] With such increased precision, the likelihood of a successful outcome is significantly improved.

A.2.ii - Smart Medical Devices

In tandem with AI, smart medical devices are becoming an integral part of patient care. These devices allow for continuous, real-time monitoring of patients and enable remote care. Examples include insulin pumps for managing diabetes and pacemakers for regulating heart rhythms. Such devices are revolutionizing healthcare by offering patients the convenience of home-based care while reducing hospital stays. They also enable more personalized treatment adjustments based on real-time data.

Despite these advancements, the growing interconnectivity of medical devices also raises significant security concerns. If not properly secured, these devices can become vulnerable to cyberattacks. As healthcare becomes more digitized, ensuring the safety and security of these devices is critical to protecting patient wellbeing.

A.3 - Risks and Implications

While technology promises great benefits for healthcare, its rapid integration into the sector is not without significant challenges. As these systems become increasingly interconnected the complexity of these systems has increased exponentially. This technological evolution has

[1] Intuitive, "Da Vinci Robotic-Assisted Surgery," Intuitive.com, 2025.

outpaced the development of cybersecurity frameworks, leaving systems vulnerable to a growing array of threats. Healthcare has become one of the most targeted sectors for cyberattacks.[2]

A.3.i - Artificial Intelligence

Adversarial attacks on AI systems pose a severe threat to healthcare reliability. These attacks involve altering the input data that AI systems rely on, causing them to produce incorrect or dangerous results. For instance, AI-driven diagnostic tools used for medical imaging could be manipulated to misdiagnose serious conditions. Even seemingly small modifications to medical images can trick AI algorithms into making fatal errors. This creates the risk of life-threatening misdiagnoses that could lead to delayed treatments or inappropriate medical interventions.

As AI continues to play a critical role in diagnostics and decision-making, the consequences of AI manipulation could be devastating for patient care.

A.3.ii - Smart Medical Devices

The proliferation of smart medical devices, such as pacemakers and wearable health monitors, has significantly improved healthcare accessibility. However, this increased interconnectivity also introduces critical security vulnerabilities. Many of these devices lack proper encryption and robust security measures, making them prime targets for cyberattacks, including hacking, ransomware, and data breaches.

Research has demonstrated that smart medical devices are highly susceptible to cyber threats. Malicious actors can exploit these vulnerabilities to steal sensitive patient data, demand ransom, or even engage in blackmail. More alarmingly, compromised devices can serve as gateways to broader hospital networks, potentially jeopardizing entire healthcare systems. A notable example is the 2017 WannaCry ransomware attack, which impacted over 200,000 computers worldwide, including medical devices in several UK hospitals.[3] The attack disrupted radiology equipment and other critical systems, highlighting the devastating consequences of such cyber intrusions.

---

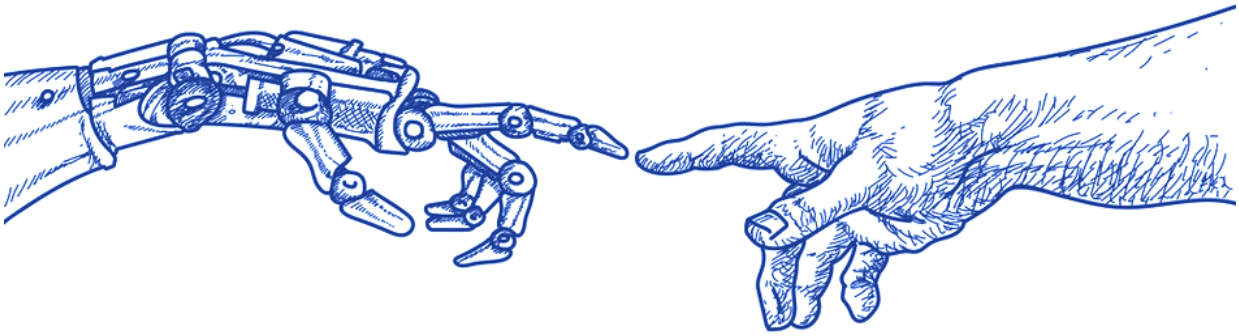
[2] Vibhu Mishra, "Cyberattacks on Healthcare: A Global Threat That Can't Be Ignored | UN News," United Nations, November 8, 2024.

[3] Sam Bocetta, "6 Medical Devices Hackers like to Target and Why," GlobalSign, January 12, 2023.

The security weaknesses in healthcare technology present not only financial and privacy risks but also life-threatening dangers. In extreme cases, cyberterrorists could disable life-saving medical technologies, putting patient lives at risk. As technological advancements continue to outpace security policies, the urgent question remains: how can we ensure these critical systems remain protected from cyber threats?"

A.4 - Questions to Consider

- How can we foster innovation in medical technology while ensuring that cybersecurity is not compromised?
- What role should global enforcement mechanisms play in securing healthcare technology against cyber threats, and how can they be implemented effectively?
- Given the rapid pace of technological advancement, what international standards should be established to regulate the use of AI and smart devices in healthcare, and how can they balance innovation with security?
- Should manufacturers of smart medical devices be held legally responsible if their products are hacked, and what steps should governments take to ensure cybersecurity compliance within the industry?
- How can international cooperation shape standards for securing AI-powered medical systems, and what specific elements should these standards include to protect both patients and healthcare providers?
- In the face of evolving threats, how should international standards for cybersecurity in healthcare technology evolve to address both emerging risks and the need for innovation?



Additional Committee Information

Position Papers

- In order to be eligible for awards, a **one-page** single-spaced position paper is due the night before DUMUNC (11:59 PM EST on April 4th), outlining your delegation's position on 1 of the topics outlined. You may choose the topic and style. We would prefer them as PDFs.
- Position papers should be emailed to aed52@duke.edu AND netid with the email title "[WHO] Delegation Name," i.e., "[WHO] USA"

Preferences of the Dais

- Do **not** prewrite any resolutions, amendments, or other materials before the first committee session.
- Conduct all **committee work within committee time and spaces** to ensure equitable access to policymaking for all parties involved.
- Be respectful to your fellow delegates and the activity of Model United Nations as a whole. Stay attentive, respectfully engage with your peers, and ensure that you are fighting for your interests well.

Notes on Procedure

- We understand that as a General Assembly, some delegates may be new to Model United Nations and may need procedural assistance or reminders. Do not hesitate to tell us (e.g. passing a note) if you need a moment to catch up on procedure!
- Accordingly, to the more experienced delegates of the committee: be ready and willing to assist your less experienced peers with procedure! The chairs will look favorably upon being a team player and non-exploitative! :)

Additional Sources and Reading

Bocetta, Sam. “6 Medical Devices Hackers like to Target and Why.” GlobalSign, January 12, 2023. https://www.globalsign.com/en/blog/medical-devices-hackers-target

Intuitive. “Da Vinci Robotic-Assisted Surgery.” Intuitive.com, 2025. https://www.intuitive.com/en-us/patients/da-vinci-robotic-surgery/about-the-systems#:~:text=The%20da%20Vinci%20surgical%20system,she%20guides%20via%20a%20console

Mishra, Vibhu. “Cyberattacks on Healthcare: A Global Threat That Can’t Be Ignored | UN News.” United Nations, November 8, 2024. https://news.un.org/en/story/2024/11/1156751#:~:text=The%20digital%20transformation%20of%20healthcare,Health%20Service%20Executive%20(HSE)