Dear Delegates,

Welcome to the 2018 MIT Model United Nations Conference (MITMUNC)! We are pleased to welcome you to our committee, the European Union (EU). We, Jason Lu and Kendall Garner, will be your chairs for the course of this conference.

Jason is a freshman pursuing a degree in Computer Science and Engineering. He is participating in MUN for the first time. He enjoys to code and is also passionate about debating.

Kendall is a sophomore pursuing a degree in Electrical Engineering and Computer Science. He was a delegate of MUN in Indianapolis for four years and is passionate about languages.

The topics that we plan to debate in the IAEA include:

I. IoT Security and Regulation in the EU Market
II. EU Investments and Regulations in Autonomous/Electric Cars

The guide below is not designed to cover every aspect of the topics; rather, it is designed to give a brief overview of the broader questions of each topic. We hope that you can use this guide as a springboard for further research of your delegation’s positions. In preparation for the conference, each delegate will submit a single page position paper on each topic to mitmunc-eu@mit.edu.

We encourage you to take the time to read up on parliamentary procedures - however in the interest of time and fruitful debate, we will go over a few changes to our committee at the start of the conference.

If you have any questions, feel free to reach out to us at mitmunc-eu@mit.edu.

We wish you all the best in your preparations and look forward to seeing you at the conference!

Sincerely,

Jason Lu &
Kendall Garner

---

**Topic X: IoT Security and Regulation in the EU Market**

**Background:**
The Internet of Things (IoT) is “a cyber-physical ecosystem of interconnected sensors and actuators, which enable intelligent decision making.” This includes a wide range of devices, from smart home devices to complex network infrastructure. Across all device types, there are a few common trends: internet connectivity and sensor usage. With the advent of the Raspberry Pi and similar devices, as well as the popularization of “smart devices” in both the home and industry, IoT is becoming a popular and lucrative industry. In the EU, it is estimated that between 2013 and 2020, the number of IoT-connected devices will increase from 1.8 billion to almost 6 billion, and spending levels will increase from €307 billion to €1,181. To take advantage of the opportunity for growth and jobs, the EU has encouraged the development and research into IoT within the EU. At the same time, there is a need to ensure secure devices and infrastructure to reduce the risk of data leaks and cyber attacks.

**The Internet: from birth to the IoT era**

![Image of Internet evolution](image)

Since 2015, the EU has established multiple policies to encourage the growth of IoT in the European market. In 2015, the European Commission established the Alliance for Internet of

---

1 EINSA. “Baseline Security Recommendations for IoT”. 12
3 European Commission. “Advancing the Internet of Things in Europe.”
Things Innovation to work with major IoT stakeholders to help establish a competitive framework for the European market. As part of the Digital Single Market strategy, the EU hopes to build an IoT infrastructure based on three main principles: a single market for IoT, a “thriving IoT ecosystem,” and “human centered IoT.” To this end, the EU launched the IoT European Platform Initiative to conduct research and projects into IoT in Europe. Despite this, there remain challenges when implementing an IoT framework in the EU. Two major challenges that arise are the need for security and a set of common standards.

**Figure 21 Ranking of Main Business Demand Barriers (average score, 1 very low, 5 very high)**

<table>
<thead>
<tr>
<th>Security concerns</th>
<th>Lack of Interoperability and Standards</th>
<th>Need to Changing business processes</th>
<th>Proving the ROI of IoT investments</th>
<th>Funding the initial investments at the scale needed</th>
<th>Lack of Managerial support for IoT solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>4.2</td>
<td>3.6</td>
<td>3.6</td>
<td>3.2</td>
<td>3.1</td>
</tr>
</tbody>
</table>

Source IDC Elaboration – N of answers 32, average values

Figure 2: Concerns about IoT in the EU

Problems IoT

---

4 European Commision. “Advancing the Internet of Things in Europe.”
5 “Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination”, 57
Since an increasing number of devices are connected and used by a wider audience, the need for security and data protection is essential. The impact of security flaws in IoT have been highlighted in recent years with a few high-profile cyber attacks. The first is the Mirai botnet attack on the Dyn DNS provider, which impacted several major websites, such as Netflix, Spotify, and Amazon. This attack demonstrates the impact of general security flaws on a grand scale. Beyond botnets and DDOS attacks, IoT devices are also vulnerable to data leaks. An example was the Target data breach, which resulted in the theft of debit and credit account information of roughly 40 million people.6

One explanation for the number and scale of these attacks is that certain IoT devices are insecure if default settings are not updated. For example, the Mirai botnet utilized the fact that many devices were running outdated versions of Linux or still had the default username/password combination. However, not all vulnerabilities were caused by user carelessness. One possible explanation for why these devices were running outdated software was the fact that, in an attempt to save on costs, the manufacturer did not provide enough memory for regular updates.7 Ultimately, solutions to IoT security vulnerabilities can be categorized into two main steps: educating users about safety and ensuring strict standards for manufacturing.

Another major concern in the EU regarding the IoT device market is competition and data usage. A common scenario for IoT devices would be as follows: an IoT device records data, sends the data to a cloud service to be processed, and the user is then able to view the data. While this sounds logical, one concern is that the cloud service and the device itself are traditionally provided by the same vendor. In this scenario, called a “vendor lock-in”, the user may be forced to only use the vendor’s cloud service and would be unable to use competing services. Similarly, this issue also

6 For more examples of IoT security issues, see “Baseline Security Recommendations for IoT” pages 100-102
7 Jack Wallen. “Five nightmarish attacks that show the risks of IoT security”
arises when multiple intelligent devices communicate directly with each other—for example, a series of devices used to manage a home. A user may want to have devices to control lighting, temperature and other devices; however, these devices traditionally only communicate between each other if provided by the same vendor. As a result, if a user wishes to control multiple devices simultaneously, then it may become necessary to buy all products from the same vendor.8

Possible Solutions

One proposal put forward to prevent flaws in IoT devices would be to require inspections of devices before being sold in the European market. Set forth in the “Cybersecurity Act”, there would be “Conformity Assessment Bodies” whose responsibilities would be to serve as a “third-party body independent of the organisation or the ICT products or services it assesses”.9 They would assess that the products would meet EU specifications while remaining impartial to the product or service they review. However, there are some concerns faced by this current mechanism. With the wide variety and types of IoT devices offered, there arise questions about whether there should be some universal standard for devices, or whether devices should be considered by type. Furthermore, there is concern that these current definitions are too vague, and fail to consider different scales of services and products.10 Additionally, a problem faced by companies in the EU market is that certain member states may have different certification mechanisms for devices. What this means in practice is that a company may be required to go through multiple tests in different member states before being able to market their product.11

Another landmark regulation impacting security is the General Data Protection Regulation (GDPR). Similar to the Cybersecurity Act, the GDPR establishes that a company may be required to

---

8 European Commission. “Advancing the Internet of Things in Europe.”
9 European Commission. “Proposition…on ENISA, Annex.”
10 AIOTI. “AIOTI position on the EU Cybersecurity Act Proposal”, 2-5
11 European Commission. “Proposition… on ENISA”
carry out an assessment of new technology usage in regards to personal data. As a new innovation, this “new technology” would include IoT devices. Furthermore, companies using IoT devices to collect data would be required to inform their clients of this data collection as well as receive proper consent. In the event of a breach, the company would be given a limited amount of time to report the leak. Failure to abide to these terms could result in hefty fines.\textsuperscript{12}

Topics to Consider

The question of IoT security and regulation in the EU requires complex, multifaceted solutions. You should consider how IoT devices should be regulated, as well as who should regulate them. Should policies be decided by the national government, or should there be a general policy in the EU that applies for every member state? Should international policies and standards for IoT devices transcend the EU? How should these standards be taken in a larger, global context? Could there be standards at different levels of organization, and if so, how would these standards interact? Would the standards be the same for every device, or would there be varying standards for different types of devices? How should quality assessments be conducted for IoT products? Would they be managed by national governments, third-party organizations, or some other mechanism? How would these assessments and regulations play out between member states? What role would industry leaders play in these assessments? What should the response be for vulnerabilities and cyber attacks involving IoT devices, and how could the risk of these events be reduced?

In addition to the regulation of IoT devices, you may want to consider its role in the European market. Should the EU continue to advocate for IoT progress? How do you ensure adequate regulations while not harming the European market? What research should be conducted regarding IoT in the European market, and how should they be funded? What is the best approach

\textsuperscript{12}“GDPR”. Official Journal of the European Union. If you wish to read more about GDPR without perusing the whole document, you may also want to visit https://eugdpr.org/
for educating people about IoT security? There are many questions to consider when discussing IoT in the EU. Some of them are more immediately obvious, while other questions may only seem tangentially related. Ultimately, it would be difficult to develop a solution that addresses every question; however, a good solution is one which is able to tackle the nuances of IoT security while making compromises as necessary.

Works Cited


EU Investments/Regulations in Autonomous Cars

Background:

In recent years, countries have been investing more in autonomous and electric vehicles. While fully autonomous vehicles are new, many parts of autonomy have started development long ago. Adaptive cruise control and parallel park assist were both introduced in 2006. Automatic emergency braking was available in 2008 and lane keeping technology was introduced in 2014. In our current world, we look towards changing partial autonomy to full autonomy where the driver does not have to give any input at all. These vehicles will be safer and more friendly towards the environment: autonomous vehicles could improve travel time by as much as 40 percent, recover 80 billion hours lost to congestion, and reduce fuel consumption by up to 40 percent. However, there will also have to be regulations. The EU must take a stance on how to regulate these vehicles while also maintaining leadership in autonomous vehicle technologies. According to the EUObserver, the current commission is asking citizens about their opinions on self-driving cars. In their survey, they state that "the objective is to allow all Europeans to benefit from safer traffic, less polluting vehicles and more advanced technological solutions, while supporting the competitiveness of the EU industry."

---

13 Boston Consulting Group “Revolution Vs. Regulations…”
Much of the driverless car development in Europe has been recent. Prior to 2015, EUObserver finds that “official commission documents rarely mentioned self-driving cars or autonomous or automated vehicles.” In October, the EU established a High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the European Union. It consisted of economy, industry, and transport ministers from 12 EU countries, representatives from the car industry, and representatives of civil society. This Gear 2030 group was convened to facilitate discussion on how to promote competitiveness and growth in the automotive sector -- not to discuss if autonomous vehicles should be adopted. Also, Gear 2030 was founded because many believed that leadership in autonomous vehicle technologies would create new global market opportunities for Europe and its automobile industry.\textsuperscript{14}

Since most of the conversation has been regarding when, not if, autonomous vehicles will take over, European automakers have already started testing in recent years. According to the Boston Consulting Group, the European automaker Audi has already presented its highly autonomous A7 model in 2015, which has “high-driving capability,” and is being tested in Las Vegas and San Francisco. BMW has also tested its autonomous 2 Series. Volvo and Swedish government bodies have launched the “Drive Me” initiative in which 100 autonomous vehicles drive around public roadways in everyday conditions in the city of Gothenburg. The Netherlands have also worked towards introducing a driverless taxi for universities.\textsuperscript{15} As of now, 21 countries across the EU have agreed to collaborate on large scale autonomous vehicle tests.\textsuperscript{16}

\textbf{Key Issues:}

\textbf{Liability}

\begin{itemize}
  \item \textsuperscript{14} EU Observer “How the EU Commission...”
  \item \textsuperscript{15} Boston Consulting Group “Revolution in the Driver’s Seat…”
  \item \textsuperscript{16} Forbes “Europe to Be…”
As an emerging technology, driverless cars will not be able to operate completely autonomously, so drivers must take partial control of vehicle navigation. In the case of an accident, should the EU take measures against automakers for a technical malfunction? Or should the EU allow automakers to push the blame onto the owner of vehicles?\(^\text{17}\)

As of now, there are many risks that are not covered by existing EU legislation. If current rules remain, there will be a shift in liability transfer, hurting the consumer. The EU must decide if liability of the driver should decrease as the technology becomes more prevalent. When Autonomous vehicles are rolled out to the world, there much not be legal uncertainty. Possible reasons for the driverless car to take blame would be: software failure, network failure, and hacking. Autonomous

\(^{17}\) Boston Consulting Group “Revolution Vs. Regulation…”
vehicles give hackers the window of opportunity to strike remotely, and the EU needs to take precautions against that.

**Current Solutions/Regulations:**

The C-ITS Final report states that as long as the driver remains in control of the vehicle, no changes to liability are necessary. However, this will need to be revised as autonomous vehicles improve. The Product Liability Directive (PLD) for the EU has a harmonized framework that believes that the producer of a defective product must compensate for personal injuries and damage to private property. The Motor Insurance Directive (MID) has a more fractured framework as different states have adopted different liability systems. The Netherlands has a semi-strict liability system while France is very strict. The UK has a no strict liability regime based on negligence rules. In a public consultation, people believed that autonomous vehicles should be insured for liability to victims of accidents the same way as drivers. People were unsure if MID should clarify their policies with the development of autonomous vehicles.  

**Moral Problems:**

The EU must regulate how manufacturers decide moral responses as it can affect the lives of many. An example problem of this would be the classic trolley problem: should an autonomous vehicle reroute itself to kill less people? Much of the debates over this have led to the discussion over the value of a person, in which the car would save a person of higher status. Surveys have shown that most people would spare young people over old people, employed over unemployed, and even dogs over criminals; however, is this really what these driverless cars should opt to do?

---

18 European Parliament Research Service “A common EU approach to Liability…”

19 The Guardian “Who should AI kill in a driverless…”
**Possible Solutions:**

One of the solutions to these moral problems is to allow the driver to intervene in such a scenario. However, given that humans will have to rarely intervene, their decisions at such critical moments may not be of good judgement. Another solution is to just try and slam on the brakes, as it is probably the most optimal solution since it is precise (as compared to swerving).

**Mandating Autonomy in New Vehicles:**

All autonomous vehicles would be able to operate better if all other cars were also autonomous. Consulting firms believe that it would take lawmakers about five years to consider the safety and economic benefits of autonomous cars before taking a step forward. How should the EU enforce autonomy in new vehicles? What can be done for the people who cannot afford such new vehicles?

**Conclusion:**

The EU committee must recognize that the rise of autonomous vehicles will require new regulations to maintain the safety of citizens. Current legislation is not up to date, so the EU must redefine liability for motor vehicles. In the case of an accident, should the EU enforce the automaker to take blame for a technical malfunction? Next, the EU must decide if they should impose regulations on how automakers solve moral problems. Should a driverless car be able to reroute itself to kill less people? Who would take blame for the death of someone caused by the intention to prevent the loss of more lives? And finally, when those problems are solved, the EU must figure out how it can bring autonomous cars to everyone, even those who cannot afford it, as it will make these cars much more safe.
Works Cited


**Helpful Links:**

More information on current EU positions on AVs