## CONTENTS

Letter from the Chair ........................................................................................................... [3]

Topic A: ................................................................. [4]
  Introduction ...................................................................................................................... [4]
  History of the Topic...................................................................................................... [5]
  Current Status............................................................................................................... [7]
  Country Policy............................................................................................................. [12]
  Keywords...................................................................................................................... [13]
  Questions for Consideration.........................................................................................[14]

Topic B: ............................................................................................................................. [16]
  Introduction .................................................................................................................... [16]
  History of the Topic...................................................................................................... [16]
  Current Status............................................................................................................... [18]
  Country Policy............................................................................................................. [22]
  Keywords...................................................................................................................... [24]
  Questions for Consideration.........................................................................................[25]
Hello DISEC!

My name is Diego Negrón-Reichard and I am the chair for this year’s DISEC General Assembly Committee. It is such an honor to chair this committee four my fourth and last consecutive time alongside my amazing director, Lila Currie. I am a senior at the Woodrow Wilson School of Public and International Affairs, with minors in Entrepreneurship, Latin American Studies, and French. On campus, I was the captain of Princeton’s Model United Nations Team (PMUNT) for the past three years, and am now more recently involved with activism work when I formed the Princeton Advocates for Justice (PAJ) with several classmates. If any of these topics seem remotely interesting to you, please reach out! Model United Nations has been indispensable to my success as a student and as an individual in the professional work environment, and would encourage you all to keep developing the important skills MUN teaches us. Because this is my last year, it is certainly going to be the best, most demanding, and creative DISEC Committee yet. I am committed to delivering an exceptional committee experience, just as I am sure the room will be filled with only the most qualified and rigorous students.

The topics we will be discussing are certainly relevant: Cybersecurity in the 21st Century, and the Small Arms Trade in Latin America. The former, Topic A, requires solutions that are both far-reaching and impactful given the amount of people and parties involved. Because this is a policy arena on which the international community has been unable to reach consensus, I can only expect the debates and arguments presented to be unique and contentious. Delegates must be prepared to balance the interests of national governments, private corporations, and citizens in a discussion that will hinge on topics such as free speech, privacy, terrorism, and social media networks. And given the recent urgency of events, such as the 2017 Global Cyber Attack and the alleged intervention of Russia during the American presidential election, it is imperative the international community intervene.

On the other hand, Topic B focuses on a problem that has plagued developing countries for several centuries. The causes for the illicit trade of small arms in Latin America are plentiful, such as the presence of cartels, supply from developing nations, and systematic poverty. As such, any comprehensive (MUN buzzword) solution to the problem at hand must also consider all factions involved. I urge delegates to be creative in their solutions and to think how can the UN international body empower local actors to dissuade the perpetuation of the illegal trade. In the end, both Topic A and B demand careful attention and innovative delegates.

Sincerely,

Diego
TOPIC A: Cybersecurity in the 21st Century

Introduction

“Civil authorities in your area have reported that bodies of the dead are rising from their graves and attacking the living”. No, the DISEC body is not a crisis committee. However, that message was sent in the winter of 2013-2014 through the federal Emergency Alert System, exposing the vulnerabilities of the US' critical cyber infrastructure. As my fourth and last time chairing the DISEC committee, I am thrilled that we get to discuss such a relevant policy arena. I hope to see delegates arduously defend their country's stances on issues ranging from proactive cybersecurity to cyber hygiene. Because the policy questions we will attempt to answer cross-cut traditional country alliances, I wouldn’t be surprised to see new alliances emerge, and old ones break down (temporarily!).

The following background document is formatted in the following manner: it will first provide a brief history of cybersecurity as well as a technical introduction to “hacking”; and then a current situation section elaborates on the most recent cyberattacks, the most relevant national legislations, and the major policy discussions. The document ends with a brief section on country stances and a key words and questions portion.

History

You're sitting in your dorm, you look over a few last lines of codes, and click send. Soon after, the worm spreads over to 6,000 networked computers, clogging both university and government systems. This was the case of Robert T. Morris, a graduate student at Cornell University (this would never happen at Princeton, of course). It was a first on several accounts: it was one of the first time the “worm” virus, infamously known as the Morris worm in this scenario, was employed; it was the first time a cyber incident gained widespread media attention; and it was the account that resulted in the first felony conviction in the US under the 1986 Computer Fraud and Abuse Act (CFAA), an important piece of legislation which we’ll revisit[1].

The world of cybersecurity has exponentially developed since the 1988 Morris worm infected thousands of computers. The purpose of this section is to offer a brief historical account of the major computer
security breaches during the beginning of the 21st century. More recent events, such as the 2016 US Presidential election, will be covered under the “Current Issues” section of this Background Guide. However, for those delegates unfamiliar with the basics of cybersecurity, this section should be helpful to explain the different types of methods hackers use to infiltrate systems, as well as some classic examples of cyber intrusion.

In 2000, the ILOVEYOU worm infected millions of computers within hours of its release. Like 1988, this worm was constructed by a student for his senior thesis. While the first incidents were perpetrated by students exploring their computational capacities, future attacks take on a much more notorious tone. In 2001, Microsoft is the victim of a new type of hack, known as denial-of-services attacks (DNS), in which the paths that take users to Microsoft’s websites are corrupted. The Microsoft episode is important for it marks a shift in the private sector’s role in cyber security: rather than play a bystander role, Bill Gates announced that his company would secure its products and services, kicking off a massive internal training campaign[2]. There are also examples of companies gaining unauthorized access to their competitors’ trade secrets – releasing the Watergates on a whole new set of legal questions to be considered. The Microsoft breach also introduces a key component to be discussed later: human error. While hackers are certainly developing highly complex devices, many of the major cyberattacks could have been avoided were it not for human error[3].

While the private sector started to gain an ever-more important role in cybersecurity, another actor, specifically relevant to the DISEC body, emerged: the nation state. In 2004, North Korea claimed to have trained over 500 hackers to crack neighboring countries’ systems[4]. Governments were now seriously concerned with the threat of cyberwarfare, perpetrated either by individuals or state-sponsored entities. Although governments have been victims of cyber attacks in the past, the frequency with which these intrusions happened have increased significantly during the 21st century. For example, on May 17th Estonia recovers from a massive denial of service attack. Even the United Nations was a victim, after Turkish hacker Kerem125 hacked the UN website. On 2008, 20 Chinese hackers claimed to have gained access to the Pentagon’s website.

The main takeaway from this section should be clear by now: cybersecurity encompasses a wide variety of scenarios and actors. As such, any solution to the current problems will require innovative thinkers that are
able to manage numerous interest groups. Before moving on to a discussion of the major current policy issues, below is an outline of the most common type of cybersecurity attacks:

- **Malware**: refers to various types of harmful software, such as viruses or ransomware. It requires that the user actually download the software, either by downloading a document from online (don’t worry PMUNC should be a safe source), or accepting a pop up on your screen. Once the malware is installed, it can cause damage on your systems through a variety of means, such as collecting keyboard history or taking control of your machine.

- **Phishing**: it is the process by which hackers encourage you to install malware into your systems. Because hackers know you would never accept a random invitation, they might instead send emails that look like they come from familiar sources with the intent of getting you to click on an infected document. As briefly mentioned, there is an ample amount of room for human error.

- **SQL (pronounced “sequel”) Injection Attack**: A structured query language, or SQL, is a computer programming language generally used to communicate with databases. An injection attack seeks to specifically target these servers – something that is potentially problematic if the databases hold private information.

- **Denial of Service (DoS)** – hackers flood their victim’s websites with more traffic than they’re built to handle to the point that the services provided are no longer available to the intended users. Sometimes, in a scenario known as Distributed Denial of Service (DDoS), multiple computers are involved, making it even more difficult to deal with the intrusion.

- **Session Hijacking**: hackers can hijack “sessions”, which refers to the transactions your computer engages with multiple servers around the world when you request information. These sessions have a unique ID that hackers can gain access to and “take on your identity”

There are several other types of cybersecurity attacks. Nevertheless, the most relevant point for our committee is that delegates are aware of the diversity and complexity of these potential attacks. A good delegate will know the basics of these intrusions (you need no more than what was outlined here). A great delegate will know the specific responses to these attacks. DISEC is by definition a “technical” committee, and showing strong knowledge is always a plus.[5] Now that you know the history and basics of cybersecurity, let’s move on to the core of this committee.
Current Situation

Do you know what duo-authentication is? I’d hope so, we are millennials after all! However, our parents would most likely not be familiar with the concept. This generational knowledge gap is just one of the many interesting and complicated policy arenas that this committee should be ready to discuss. This section is structured in the following format: I will first go over the most current events related to cyber security; I will then dive into the appropriate national legislation of key countries to highlight how different countries’ legal systems support or deter cybersecurity; and lastly, we will go over the major topics that are currently being discussed in the realm of cybersecurity.

We remember two particular things from 2016: Donald Trump became president of the United States, and Russia interfered in the U.S. election process. These two events are indisputable facts that have shifted and framed many of the international policy discussions. Back in October 2016, the US government publicly recognized that it was “confident” the Russian government hacked the Democratic National Committee (DNC) and its politically affiliated organizations[6]. While the American intelligence agencies acknowledged that the hack led to the release of thousands of sensitive emails that contained damaging information on the DNC and the party candidate Hillary Clinton, it did not go as far as to state Russia was attempting to bolster Trump’s chances[7]. However, one month later, the CIA briefed US senators and informed them that Russia was in fact meddling to help Trump win the presidency. How did they come to this conclusion? Russia had not only hacked the DNC, but had done the same thing to the GOP and several of its political affiliates, but had not released them to the public. Additionally, there is evidence to show the Russians had developed “troll farms” to spread negative publicity on Clinton.

The 2016 US election raises several important points. First, it is a clear example of state-sponsored cyber intrusion. While Russia has not acknowledged its involvement, intelligence agencies around the world are confident in their assessments. Second, this event highlights the difficulty involved in pinpointing the perpetrator of an attack, and the appropriate measures to retaliate once an identity has been confirmed. The United States has recently approved new sanctions against the Russian government – but, are these sanctions
warranted? And are they even effective at curtailing Russian influence? In a case of known state-sponsored cyber intrusions, should the victim respond alone, or should there be a mechanism by which nations can coalesce and punish the perpetrator? Finally, this issue points to one of the fundamental problems of cybersecurity: currently, the benefits of conducting a cyber attack far outweigh the potential costs. As such, delegates, how can we make it so the costs will outweigh the benefits?

If you think 2016 was full of drama, let’s move on to 2017. In the first six months of 2017, not only have we seen the standard corporate breaches, but we’ve been witness to state-sponsored ransomware, more campaign hacking, and leaks of important spy tools.

A group called Shadow Brokers successfully retrieved particularly significant NSA tools. Specifically, in April the group stole a tool known as EternalBlue that works by exploiting bugs in Windows[8]. The incident revived an important debate surrounding the exploitation of bugs in commercial products for intelligence-gathering. If the NSA knew that there was a bug in a series of Windows products, shouldn’t they be required to report that to the company? Or, does the prospect of effortlessly collecting intelligence outweigh that responsibility? Regardless, the NSA’s tool was used in two future ransomware attacks in 2017.

On May 12, a ransomware called WannaCry rapidly infected hundreds of thousands of users around the globe, including public utilities and large corporations. Particularly troublesome was the fact that the attack crippled the National Health Service hospitals and facilities in the United Kingdom[9]. Ultimately, the ransomware had significant flaws that security experts used as a kill switch to render the attack neutral. Intelligence agencies concluded that the attack was product of a North Korean government project that aimed to cause chaos and generate revenue. Interestingly enough, the WannaCry ransomware benefited from the EternalBlue exploit. Even though Microsoft had already patched up the bug, numerous firms had not updated their systems by the time of the incident.

A month after WannaCry, enter Petya: a ransomware that had a similar composition as WannaCry and infected multiple countries. While the infected networks included US pharmaceutical Merck, Russian oil giant Rosnoft, and Danish shipping company Maersk, researchers believe that the ransomware actually masked a cyberattack against Ukraine. For example, the cyberattack hit Ukraine infrastructure particularly hard, disrupting
public services, central bank operations, and airports. Ukraine has been the victim of a series of cyber assaults, largely believed to be perpetrated by Russia[10].

Interventions in elections and related sensitive material continued in 2017. For example, 198 million voter records were exposed following a major discovery by Chris Vickery[11]. Vickery showed that a whole database of private voter information held by a company called Deep Root Analytics was essentially publicly accessible. While misconfiguration is not a malicious hack in itself, it is an all too common cybersecurity risk for firms and governments. Another example of election intervention is when now French president Emmanuel Macron’s campaign was hacked two days before the general election[12]. Contrary to the Clinton camp back in 2016, the Macron campaign was prepared for such an attack and the impact was minimal. Researchers have found evidence that the campaign was targeted by a Russian-government-linked group called Fancy Bear back in March. The perpetrator of the most recent attack is unknown.

By the time of the publication of this background document, I am confident we will witness even more global cyberattacks. Thus, the main takeaway from this section should be to understand the dangerous nature of cyberattacks and have a strong grasp of the current global situations. The following section will go over relevant national legislation that could serve as a beacon for international policy development.

**Relevant National Legislation**

It is important to look at how nations understand cybersecurity and how their respective legal systems accommodate for new developments in the field. As such, I will provide a quick summary of different regulatory environments that are pertinent to our discussion.

In the United States, the most relevant piece of “legislation” is no legislation at all. In fact, it’s a general framework developed by a government agency to help guide the private and public sector in all matters related to cybersecurity. Titled the 2014 National Institute of Standards and Technology (NIST) Cybersecurity Framework, the lengthy document was a signature piece of the Obama administration. The NIST Cybersecurity Framework takes on a risk-based approach for organizations to detect, mitigate, and respond to cyber threats. Not only does it contain provisions to ensure cybersecurity measures are business friendly (low-cost), it also emphasizes the importance of civil liberties, such as the right to privacy. Finally, there is one crucial component
of the framework that is worth highlighting: rather than developing new cybersecurity standards and risk management processes, the Framework considers a variety of existing standards and allows for sufficient flexibility for future developments. In essence, it provides a common language for all interested parties to organize their systems.

In the United Kingdom, similar to the US, there has been an emphasis on voluntary standards to enhance Critical National Infrastructure protection. Specifically, the 2011 UK Cyber Security Strategy lays out specific standards for government contractors, and the Centre for protection of National Infrastructure calls for greater voluntary intervention. However, the UK’s cyber regulatory infrastructure is not by any means a leading framework in the policy world.

Singapore is an interesting case study, and could serve as an example for other nations to follow. A major financial center, Singapore has been the victim of relative high-profile attacks. This prompted the nation to amend its Computer Misuse and Cybersecurity Act (CMCA) in an attempt to address the country’s shortage of cybersecurity professionals. The CMCA is important for it officially introduces active defense policy within its legal system. Active defense, or proactive cybersecurity, entails that rather than simply recuperating from a cyberattack as quickly as possible, corporations can actually counter-attack the perpetrator. Specifically, while the CMCA does not fully authorize private active defense, it does create a mechanism by which the government can grant corporations a temporary right to engage in proactive cybersecurity to deal with perpetrators.

Policy Discussions

This section hopes to summarize some of the major policy discussions that the chair hopes to see come the first committee session. Delegates are nevertheless encouraged to go beyond these policy questions and come up with their own – the realm of cybersecurity is extremely large.

Should government even be regulating cybersecurity practices? Certainly so, or we wouldn’t be meeting as a DISEC body. However, the question is: to what extent should government be involved, especially when policy wonks might not understand the complexity of cyber defense? As such, the DISEC body needs to engage in a discussion regarding the role of the private sector vis a vis the public sector. Should it be a top-down
approach, in which the government dictates the rules? Or should it be a bottom-up approach, in which the government acknowledges the private sector’s most common practices? There is, as always, a middle ground that we can call “polycentric governance”, in which a multitude of players would be involved. However, there are inefficiencies associated with this last proposal.

There is also an educational aspect to cybersecurity that this committee needs to discuss. Not only is there a knowledge generational gap, but it would be fair to state that most nations lack an education system that incorporates cybersecurity best practices, or “cyber hygiene”. While governments are behind, private corporations are not necessarily ahead. Although corporations recognize the threat of cyber intrusion as more imminent than governments, many still lack adequate training for their employees. As policy makers, we need to think of creative ways as how to best educate citizens, both in private and public spheres.

Lastly, there are three interrelated points to discuss: a lack of cybersecurity professionals, the use of proactive cybersecurity, and an appropriate regulatory environment. Similar to the educational gap, there is an urgent need for professionals to specialize in cybersecurity. However, these professionals need to have clear parameters to know what type of activities they can engage in. More specifically, the DISEC body should be ready to develop a concise policy regarding the use of proactive cybersecurity – who is authorized to allow these measures, and who is qualified to carry them out? Finally, these policies need to be implemented into national regulatory frameworks with the appropriate incentives/disincentives to achieve the desired outcome.

**Country Policy**

Contrary to past DISEC committees, policy positions on the issue of cybersecurity cross-cut the traditional developed vs developing alliances. Some developed nations, such as the U.K, lack comprehensive policies, while some developing nations, such as Singapore, have very comprehensive systems in place. As such, the chair would encourage delegates to thoroughly research their respective country’s stances on the wide variety of policy problems.
Keywords

- Proactive cybersecurity
- Cybersecurity standard of care
- Polycentric governance
- ATP’s
- Information sharing
- Top-down vs. Bottom up
- Cyber hygiene

Questions for Consideration

- Where does your country stand on the international ranking for cybersecurity measures?
- Has your country, whether the government or private corporations, been victim of cyberattacks?
- Where does your country stand on proactive cybersecurity?
- How would you classify your country’s cybersecurity regulatory framework?
- What other countries are you most likely aligned to?

References

[5] To clarify, there is no need to go on technical rants during your speeches. All I would like to see is that the appropriate terms are referenced to, and that the delegates show that they’ve done their fair amount of research. If you have any questions, feel free to reach out.
TOPIC B: The Small Arms Trade in Latin America

Introduction

What is the current state of the illicit trade of small and light weapons (SALW) in Latin America? Who are the main actors in these trades, and what policy solutions are appropriate to tackle the issue at hand? These and many more are some of the policy questions we’ll deal with when the DISEC committee convenes.

This background document will first provide some information on the progress of the 2013 Arms Trade Treaty (ATT) in Latin America. It will then go on a case-by-case discussion of different countries in Latin America with the hope of providing students with an understanding of the different problems that the region faces. It will then go through a policy discussion, provide input as to how country blocs should look like, provide keywords and some questions to guide your research.

History of the Topic

In the 1980s, a series of civil wars, notably in Nicaragua and El Salvador, throughout Latin America became proxies of the larger Cold War standoff between the United States and the Soviet Union. Both sides discreetly provided mass quantities of small arms and light weapons to their respective allies, thousands of which are floating around Central and South America to this day. Despite the majority of these civil conflicts in Latin America ended along with the Cold War, easily accessible small arms and light weapons have contributed to the continuation of some of these tensions, notably in Colombia, while other countries have seen new hostilities come to light. Many Latin American actually saw an increase in gun violence following the end of formal warfare [1].

The rapid increase in the number of small arms and light weapons over the course of the decades that followed the armed conflicts in Latin America was largely uncontrolled, allowing the numbers to skyrocket as between 45 million to 80 million small arms and light weapons flooded the region [2]. In Latin
America, guns are the number one killer of Latin Americans between the ages of 15 and 44, with guns killing between 73,000 and 90,000 people total each year in Latin America. The influx of small arms and light weapons has had significant impact on the region, resulting in increased homicides, gang violence, crime and organized armed violence.

In 2005, at least $175 million dollars of small arms and light weapons, ammunition and spare parts were imported illegally to Latin America [3]. Major suppliers include the United States, Belgium, the Czech Republic, Germany, Israel, Italy, Russia, South Africa and Spain [4].

The trade of small arms and light weapons has thrived in Latin America, which has been referred to as a “smuggler’s paradise” due to a “vast coastline, densely forested mountains, porous borders, clandestine airstrips, widespread government corruption, a lack of governmental resources and political will to confront the trade, and entrenched and powerful narco-traffickers” [5].

On a global scale, illegal arms represents between 10 and 30% of the arm trades, an industry estimated at around $60 billion dollars a year [6]. Roughly 500,000 people die as a result of homicides committed using illicitly traded small arms and light weapons, according to Amnesty International.

Country Policy

While a global phenomenon, the issue of illicit arms trade is further exacerbated in Latin America by its relationship to the United States and by the unique problems the region faces. This section will focus primarily on describing these unique challenges through different case studies of individual countries. The aim is twofold: delegates should walk away with a fair understanding of the different policy concerns throughout Latin America, and should comprehend how complex and interconnected these issues are.

Before diving into the peculiarities of each nation state, it is important to quickly discuss the 2013 Arms Trade Treaty. The treaty certainly represents a step in the right direction – given the ease with which arms are transported across the globe, the ATT institutes measures to reduce the interstate trade of illicit weapons. However, the comprehensive framework fails to address concerns that are idiosyncratic to Latin America. Specifically, the most pressing issues in the region include illicit trafficking, domestic diversion, and
leakage[7]. Steven Dudley, an expert on Latin America and co-director of InSight, argues that the treaty “…offers a 100% solution for just 10% of the problem”[8]. Finally, it is worth mentioning that only 10 nations in Latin America have ratified the ATT – raisings question regarding the legitimacy and implementability of the treaty. With this important note in mind, we now proceed to discuss the situation of several member states.

**Venezuela**

Venezuela is currently going through a full-on social, political, and economic crisis that will surely define the nation’s future. In these tumultuous times for Venezuela, foreign governments, both neighboring and abroad, agree that this represents an opportunity for non-state actors to gain dangerous weapons. The concern is especially concerning given that it was discovered that Venezuela possesses 5,000 Russian-made MNPADS surface-to-air weapons[9]. The weapons, which are shoulder-mounted and hence are classified as SALW, pose a serious threat to commercial and military aircraft. Colombia has accused Venezuela of arming guerillas in the past, and officials in Brazil last May voiced their concerns that local drug gangs are acquiring military weapons from their Venezuelan neighbor. Finally, there are reports of military and police officials stealing weapons. In the end, it’s a well-known fact that Venezuela is home to a thriving illicit arms trade – a reality that represents a serious danger to Latin America and other players in the region.

**El Salvador**

In El Salvador, more than 80% of the murders were carried out by firearms[10]. And yet, the country has no domestic gun manufacturers, which implies all guns in the nation come from external sources. Specifically, a report found that half of the guns in circulation in El Salvador come from the United States. There are a variety of means by which these weapons come into the country – some come in legally and make their way into the black market, some are sourced from the stockpiles held by the militias, and others are imported from outside the country by or on behalf of criminal syndicates[11]. Similar to Venezuela, military officials are known to sell stolen weapons in the black market, and there is the fear that the government instability will allow non-state groups to build their weapon stock. Particularly troublesome is the relationship
between the Defense Ministry and the gun retailers. Because many of the retired generals end up owning gun stores, there is little to no incentive to crack down on illicit trade. Even though El Salvador has some of the strictest gun laws and procedures, the rules are loosely enforced[12]. Finally, following the Latin American trend, El Salvador has a past history of civil war that further exacerbates the issue.

Colombia

“Goodbye weapons! Goodbye war!”, said Rodrigo Londoño, leader of the FARC. Colombia is particularly interesting because, similar to its Latin American counterparts, it has been victim to decades of guerilla fighting. However, on a more positive note, the government has also been able to end the war with its former rival Revolutionary Armed Forces of Colombia (FARC) through a successful peace negotiation process[13]. As of June, 25th 2017 the demilitarization of the FARC was near completion. The weapons were shipped away in large containers to be melted and constructed into monuments. The FARC plans to re-emerge as its own political party in upcoming elections. Colombia provides a good roadmap to other nations as to how best deal with non-state actors. While Colombia’s arm imports have reduced by 19%, the same cannot be said of other member states[14].

Mexico

Donald Trump might have misspoken when he said Mexico is sending drugs and weapons to the United States – it seems like the opposite is true in fact. Even though Mexico has some of the strictest gun laws in Latin America (and even the world), non-state actors can easily acquire firearms which they use to instill fears into the citizen population. The consequences are real: in 2002, there were more than 2,600 murder investigations involving firearms, however, in 2016 the number of cases increased to nearly 13,000[15]. Like El Salvador, most of the weapons used by criminal organizations come from the United States[16]. How exactly do Mexican criminal organizations get guns from the United States? It all goes back to the infamous “straw purchases” in the States. A straw purchase is when a person that is prohibited by federal statute to purchase weapons contracts a third party to engage in the transaction for them. The loophole allows for thousands of weapons to make their way to the black market. Surely enough, the US arms
manufacturers are greatly profiting from the existing legislation. Finally, it is worth pointing out that Mexico’s arms imports grew quite significantly by 184 per cent in the 2012-16 period vis-a-vis the 2007-11 period[17].

Brazil

There’s a little piece of Brazil in Yemen, and it’s not the music. Across numerous fragile countries in the Middle East, weapons manufactured in Brazil are continuously emerging. In fact, Brazil had ranked among the top global producers of small weapons and ammunitions for the past two decades[18]. For example, between 2005 and 2012, Brazil exported weapons to over 100 countries[19]. The weapons manufacturing industry in Brazil is substantial – the sector brings in $60 billion in revenues annually, with about $350 million coming from the sale of small weapons. And here’s an interesting fun fact: Brazil has yet to ratify the Arms Trade Treaty! While it originally seemed that Brazil would switch courses when it was one of the first to sign the ATT in 2013, the lower house of congress has yet to approve the international treaty. If anything, it’s a testament to the power of the private industrial complex.

Uruguay

Undoubtedly, Uruguay is one of the safest countries in Latin America. After having successfully transitioned from military to civilian rule over two decades ago, Uruguay features strong institutions with a long-lasting international presence. However, it’s reputation is in trouble as homicides have increased by 50 per cent from 2011 to 2012[20]. Particularly relevant to our discussion is the growing presence of international criminal organizations and the use of Uruguay as a transshipment point for the drug trade. The presence of both these factors lead to increased violence, and of course, increased presence of small and light weapons. There are two other compounding factors that are important to recognize: overcrowded penitentiary facilities, and an antiquated police force[21].

Policy Discussions

Hopefully, delegates have noticed recurring problems across the various Latin American countries throughout the case studies. This “Policy Discussions” section intends to designate those policy questions that the chair expects to be discussed during committee sessions. Given the diversity of issues related to the
illicit trade of small and light weapons, these discussions are by no means exhaustive. They should nevertheless point delegates in the right direction.

A common narrative between several nation states is the fact that these countries have gone through internal civil wars. During these periods of unrest, large amounts of weapons were collected by the opposing factions. While there are no more civil wars (albeit the case of Venezuela arguably), these stockpiles have not been properly removed. As such, many non-state actors find it quite easy to acquire these types of weapons, which mostly fall under the category of small and light weapons. The problem is then how to first identify these weapons, and then how to eradicate them?

A similar policy question is the role the military and police play in the illicit trafficking of arms. Should former military generals be allowed to join private defense or manufacturing companies? What kind of incentives, or disincentives, can be put in place to ensure officials do not engage in illegal contraband? In the case of the police, many times their units are underfunded and do not have the resources to carry out their operations. For this reason, sometimes they resort to the illegal markets. How can nations ensure that their police force have the necessary resources?

Not only is it appropriate to discuss the role of the official armed forces, but it necessary to entertain a conversation on the role of the private sector itself. As with the case of Brazil, we saw the significant sway the private sector holds over legislation. The same applies to the United States, in which private corporations benefit from loopholes such as the “straw purchases”. How should then DISEC consider and weigh the interests of the private sector? It would not be appropriate to ignore them, seeing as those corporations generate significant revenue and offer employment for many. What then would be an acceptable role for the private sector in this pursuit for safer nations?

Moving away from the private sector, it is important to recognize governments are at fault too. Especially in Latin America, there is a marked lack of cooperation between neighboring states to monitor arms transfers, trafficking, and leakage[22]. This is further exacerbated when we point out that countries are quickly trying to expand their market share in the defense industry. Similarly, arm transfer agreements are loosely adhered to in Latin America. For example, countries seldom report to the UN Register of
Conventional Arms, and the legally binding firearms convention on Organization of American States only has six countries reporting[23]. How can DISEC then encourage states to comply with agreed upon terms? What enforcement mechanisms can we craft?

Finally, the DISEC body must acknowledge that the issue of illicit arms trade is directly and indirectly related to a myriad of other societal problems. In many contexts, lack of career opportunities, poor education systems, crumbling social welfare systems, and weak legal systems have pushed people into the black market. The central question is thus: if we recognize the root of this problem, should DISEC be proposing measures to tackle poverty and education systems? If the answer is yes, this would greatly expand the prerogative of the DISEC body. For this reason, the chair is confident this will be a lively discussion, and is excited to hear all the delegates points.

Key Words

· Small and light weapons
· Leakage
· Arms Trade Treaty
· Private vs. Public interests

Questions

· Where does your country historically stand on the issue of illicit arms trade?
· What, if any, is the presence of private corporations that deal in arms manufacturing or trading?
· What is the state of your nation’s police and military?
· What has been the progress achieved so far in the implementation of the Arms Trade Treaty in your particular nation?
References

[4] Ibid.
[5] Ibid.
[8] Ibid.
[12] Ibid.
[19] Ibid.
[21] Ibid.
[23] Ibid.