Asia-Pacific Economic Cooperation

ATIDMUN VII

Table of Contents

Chair Letters

Yonatan Ram

I am happy and honored to welcome you to The Asia-Pacific Economic Cooperation in ATIDMUN2021!

My name is Yonatan Ram, and I am a junior at Atid Lod High School for Sciences and Leadership. My majors are Chemistry and Biology.

After school, you will probably find me practicing Powerlifting, Calisthenics and Bodybuilding, which I do on a daily basis, hanging out with my friends, listening to every type of rap or binging anything that I am able to find on Netflix.

This is my fifth year being associated with our Atid Lod MUN and Debate club in Atid, during which I have been debating in every single one of those years, and have been doing MUN since my 8th grade. I had the privilege to participate in more than 10 conferences (and yes, some were online) both as a delegate and as a chair, and to get awards in most of them.

My co-chair and I are really excited to meet y'all and debate about the topic, make memes, raise our placards, punish you for no reason, and genuinely make sure that you're going to remember this conference as the best one you ever had.

Yours,

Yonatan Ram.

If you have any questions or thoughts, you are more than welcome to contact me!

Yonatan.ram2005@gmail.com - My email (obviously)

Yonaatn_Ram2310 - Instagram ;)

Ido Vaktor

Welcome to APEC Committee at ATIDMUN 2021!

My name is Ido Vaktor. I am an 11th grader at Atid Lod High School for Sciences, majoring in physics and chemistry, and I participate in the activities of Atid Lod MUN Club.

My first experience with MUN was two years ago in "Holyland MUN 2019" when I represented Ukraine in the WHO Committee. My second conference was much better- I got the Best Delegate Award, having learned from my mistakes. Since then, I have participated in 9 more conferences, and chaired two committees.

I also take part in the Agricultural Union Scout movement activities; I am a swimmer and a huge fan of the "How I Met Your Mother" TV show.

Beside chairing you, I'm also a talented editor of the AtidMUN 2021 website, and if you have any questions just let me know I would be happy to review them.

I look forward to meeting you and hope to see you soon!

Sincerely Yours, Ido Vaktor- idovaktor@gmail.com

Topic A: Threats of Cybersecurity Attacks on Asian Economies

Key Terms

- Cyber-attack: an attempt by hackers to damage or destroy a computer network or system.
- ASEAN: Association of Southeast Asian Nations, the name of a regional body for cooperation.
- Dwell time: the time between an attacker's initial penetration of an organization's environment and the point at which the organization finds out the attacker is present.
- Cyber Threat Actors: Cyber threat actors are states, groups, or individuals who, with malicious intent, aim to take advantage of vulnerabilities, low cyber security awareness, or technological developments to gain unauthorized access to information systems in order to access or otherwise affect victims' data, devices, systems, and networks
- Smishing: Smishing is a form of Phishing conducted via text or phone SMS messaging, in which the threat actor attempts tricking a user into sharing personal information.
- Internet Penetration: Internet Penetration is the proportion of the population which uses the Internet

Background to the Issue

Only in the last decade, as the world became increasingly digitized, has cyber risk emerged as a real threat. Cyber attacks are known to be a low cost yet effective method, capable of causing severe damage by having the potential to disrupt everything from the safety of our finances to how we consume news without any geographical boundaries. The term "cyber attack" is mainly used to describe a scenario where there is an attempt by an individual or group to compromise a

computer system, network or device with the intention of causing harm; these attacks can be against governments, businesses or individuals. With its ever-evolving nature, cyber risk has grown pervasive and dangerous, rendering it hard to combat.

As the economy of ASEAN member-states becomes increasingly digitized, cyber attacks become a greater threat. Furthermore, hackers are 80% more likely to target businesses that operate in the Asia-Pacific (APAC) region over those that operate in North America and Europe. Rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation.

Throughout history there were major cyber attacks which harmed many governments, companies and corporations.

Cybercrime came to be known in our modern societies firstly through hacking, documented in the early 1970s when computerized phones were becoming a target. Tech-savvy people known as "phreakers" found a way around paying for long distance calls through a series of codes. They were the first hackers, learning how to exploit the system by modifying hardware and software to steal long distance phone time. This made people realize that computer systems were vulnerable to criminal activity and the more complex systems became, the more susceptible they were to cybercrime. This innovative type of crime was a difficult issue for law enforcement, due in part to lack of legislation to aid in criminal prosecution, and a shortage of investigators skilled in the technology that was being hacked. It was clear that computer systems were open to criminal activity, and as more complex communications became available to the consumer, more opportunities for cyber crime developed. As technology developed, so did new forms of cybercrimes. However, the first big-scaled operation related to this new form of crime was registered only in 1990, where a large project named "Operation Sundevil" was exposed: FBI agents confiscated 42 computers and

over 20,000 floppy disks that were used by criminals for illegal credit card use and telephone services. This operation was costly and lasted for over two years, demonstrating for the first time to the public eye that this new form of crime posed indeed a threat. Nowadays cybercrime has become an increasingly large problem in our society, even with the criminal justice system in place. Both in the public web space and dark web, cybercriminals are highly skilled and are not easy to find, as will become clear in the next section.

The Current Situation

Digital Transformation and Increased Electronic Connectivity

The Asia-Pacific region is home to some of the world's fastest-growing economies, such as China, India and the Maldives, 60 percent of the world's population, and, by 2019, a full 50 percent of the global internet user base. It is thus not surprising that Asia actually leads in digital innovation, ranking ahead of many other regions including Europe and the Americas. Moreover, Asia's top ten smartphone brands – the likes of Samsung, LG, Xiaomi, and Sony – already account for 69 percent of global handset sales. And because of the associated digital ecosystem, a third of the world's 2.3 million app developers are based in Asia. The rise of interconnection between companies and their employees has exposed vulnerabilities in hardware and software environments, giving cybercriminals greater attack surfaces to exploit. This includes employees' smaller, personal electronic devices (smart phones, computers, and televisions), which can provide a potential backdoor into more well-protected systems. In spite of that fact, many companies are still leaving their systems unprotected and haven't implanted the crucial cybersecurity protocols which are meant to detect and prevent these cyber attacks.

Lack of Government Regulation

Not only corporations are left unprotected, but there is a lack of government regulation in the ASEAN countries. Unlike in the west, where digital progress was gradual and slow, which means that regulators had time to adapt and implant crucial cyber defenses, the rapid speed of digital transformation in APAC has limited governmental action as governments do not have the time or power to implant those crucial defenses, which are still only in early stages of development. Even in countries where there are cyber laws there are still many regulatory issues which haven't been resolved yet, such as a lack of enforcement, a misalignment of regulations and perceptions, and a general lack of organizational compliance.

Extremely Long Dwell time

In 2020, APAC'S dwell time was one of the longest dwell times in the world, and it sadly still is. While the dwell time in the Americas region (both North and South America) is only 9 days - the only region with a single digit dwell time - APAC's dwell time is more than 74 days, and it is still rising. According to the FireEye 2021 M-Trends Report, 10% of the breaches investigated in APAC during 2020 had dwell times of more than three years while 4% showed dwell times of more than nine years. This extremely long dwell time is very attractive for cybercriminals, who see this as an opportunity to perform harmful activities without being detected.

The Covid-19 Pandemic

The pandemic forced corporations to adopt new technologies in order to secure the option of working remotely. Sadly, 53% of APAC companies stated that they were unprepared for these security requirements. As we can see, many APAC struggle with the pace of security developments. Furthermore, low budgets and a general lack of interest causes further challenges to implementing an effective cyber security plan.

The Main Cybersecurity Threats to APEC

After covering the main reasons behind APECs high cyberattack risk, we will now cover the biggest security threats that APEC (you guys) are facing.

Mobile Attacks

Mobile platforms have been an extremely attractive attack vector since their creation, with social media and the Google Play app store serving as popular means to distribute malware. Many mobile attack campaigns have been targeted at the APAC region, like the "PhantomLance" campaign — a five-year-long Android espionage campaign carried out by the Vietnamese APT OceanLotus from 2015-2020. Aimed at several Southeast Asian countries (e.g. India, Indonesia, Bangladesh, Malaysia, etc.), this campaign involved malware that was hidden in the Google Play store. Another example is "Roaming Mantis", a Chinese-speaking threat group that has been impersonating logistics companies in smishing messages. These messages are targeted at Japanese Android users in the hope to infect their devices with a new malware named SmsSpy, which extracts data from users' text messages, intercepts incoming texts, and hijacks targets' contact lists.

Both groups have successfully leveraged various mobile platforms, exhibiting a smart and covert approach to distribute malware on a large scale.

Phishing

Phishing has always been a troubling issue for APAC, but has become even more problematic during the Covid-19 pandemic, which enabled actors to take advantage of the pandemic in order to trick victims into handing over personal and important data. Phishers use relevant events and disguise themselves as well-known institutions and people which causes the attacks to look more "authentic" and harder to spot for the average person. Small and medium businesses in countries like Indonesia, Malaysia and Vietnam are especially vulnerable to

phishing attacks, with Southeast Asian banks being one of the most targeted sectors in the world, accounting for 21% of phishing attacks globally in 2020.

China

China is the leading threat actor in the APAC region as Chinese state-sponsored groups are the most active perpetrators of cyberespionage and intellectual property (IP) theft. China is seeking to use cyberattacks to gain access to IP, specifically blueprints and trade secrets related to defense and technological advancement. Moreover, China also uses the cyber realm to spy on other government entities, and APAC countries are some of China's main targets due to ongoing disputes in the South China Sea as well as ongoing conflicts with many nations in the region, including India, Taiwan, and Hong Kong.

Questions to Consider

1. Has your country ever faced cyber attacks? If so, what protocols did it implement in order to prevent these attacks?
2. How does your country balance between cyber regulation and protecting human rights? For example, do demands for cyber security require that private firms and users surrender much of their previous freedoms to governmental supervision and oversight?
3. Has your country cyber attacked other countries, organizations, etc? For what reason?
4. Has your country ever aided other countries with implanting cyber security, or vice versa? If so, which countries and what aid?

Suggested Reading

- https://thediplomat.com/2016/07/chinas-secret-weapon-in-the-south-china-sea-cyber-attacks/

- https://www.southeast-asia.kearney.com/web/southeast-asia/article?/a/cybersecurity-in-asean-an-urgent-call-to-action
- https://billingtoncybersecurity.com/cybersecuritythreat-opportunity-asia-pacific-region-australia/
- https://www.oecd.org/digital/ieconomy/35486405.pdf

Bibliography

- Morgan Demboski (2014) https://www.ironnet.com/blog/apacs-vulnerability-to-cyber-attacks
- https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
- https://www.itnews.asia/news/cyber-attacks-in-apac-continue-to-keep-going-up-565497
- https://blog.checkpoint.com/2021/05/27/check-point-research-asia-pacific-experiencing-a-168-year-on-year-increase-in-cyberattacks-in-may-2021/
- https://blog.bosch-si.com/digital-transformation/asia-leads-the-world-in-digital-transformation/

Topic B- Foreign Trade and Escalation of Disputes

Trade Conflict

During the past years, the words "trade war" have been all over the news. A trade war is inflicted not by matters of security or over territorial disputes, but by economic differences and trade disagreements. For instance, while some countries consider trade as a win-win (a positive-sum game), in which the total amount benefits both partners, others believe trade to be a zero-sum game, in which a surplus means enrichment at the expense of a trade partner.

The weapons in a trade war are the tariffs and trade barriers set up by conflicting parties. Similarly to military action, imposing tariffs on imported goods from another nation may put economic pressure on that nation. These tariffs come at a cost, though: not only does it increase the cost for local consumers, the targeted nation could apply retaliative measures, leading to a spiral of tariffs.

Background to the Topic

In ancient times, Asia was a symbol of foreign trade: the Maritime Silk Road that connected Asia and China in particular to Europe, Egypt, and northern Africa contributed to trade relations among the Asian regions as well as parts of Europe and Africa. Particularly important in such trade were fine textiles, silk, gold, and other metals, various precious stones, and spices, and aromatic products.

After Alexander the Great invaded the western part of Asia, trade ties with Europe and the Greek empire expanded and more land routes were established, further connecting Asia to the West.

For many years, trade relations between the local Asian nations have grown. That is, until the 17th century, when European powers such as the Dutch and the

British established control over some Asian regions. These powers came seeking the exotic products of Asia: silks, cotton, and precious commodities such as spices and aromatic products. Disputes over exports between the Asian nations and the European colonial empires quickly escalated, and the British even went to war with China to block Chinese efforts to ban opium imports. The British victory in the Opium Wars caused China significant economic damage - it had to hand over Hong Kong Island to the British and increase the number of treaty ports where the British could trade and reside.

In the second half of the 20th century, after the age of European colonies in Asia passed and the Asian nations regained their independence, many countries in Asia sought to develop industries of their own to produce substitutes for their former imports.

The Effect of the First World War On Foreign Trade

During World War I (WWI), the majority of industries were devoted to the war effort, and the few trade ties between countries were completely cut off or burdened with heavy tariffs. The First World War differed from other conflicts aimed to disrupt international trade, as the goal of the opposing sides was to prevent the import of food and of raw materials and not only to prevent the enemy from gaining export revenues, which was the predominant goal in previous wars.

The War greatly damaged international trade. The League of Nations (an organization similar to the UN, established for the purpose of establishing peace in the post-WWI-world), which was envisioned by then-US president Woodrow Wilson, believed the path for a peaceful world also includes "the removal, as far as possible, of all economic barriers and the establishment of an equality of trade conditions among all the nations consenting to the peace and associating themselves for its maintenance."

Ten years after the end of WWI, the world fell into an economic recession called "The Great Depression". Originating in the United States in 1929, the crisis peaked in 1933 with a 60 percent drop in US GDP and an 80 percent drop in industrial output. Unemployment jumped from 12.5 percent at the onset of the recession to close to 25 percent by the mid 1930s, and there were over 8,000 registered bank failures. In an effort to mitigate the crisis, the US administrations started levying tariffs of 50% on imported goods, so as to promote local industries and keep American money in the US market, which further diminished global trade. This, alongside other (more important) reasons, spread the crisis to the rest of the world. The crisis affected future APEC economies: the export of raw products of Australia was reduced by almost 30%, the Canadian industrial production had by 1932 fallen to only 58%, Chile lost 80% of the state revenue from exports and the list goes on and on…

The Effect of the Second World War on Foreign Trade

Similarly to WWI, World War II (WWII) significantly damaged international trade as it severed economic ties between most of the world. Those countries which still attempted to trade usually found their merchant ships were drowned by opposing navies. The effort of the markets was once again devoted to the war, and Wilson's vision was gone. After the end of the War in 1945 and the establishment of the UN in 1946, a new and promising agreement was signed between 23 countries in Geneva, called the "General Agreement on Tariffs and Trade" (GATT). The signatories of GATT agreed upon the promotion of trade and the reduction of trade barriers, specifically tariffs - countries were expected to reduce tariffs and placed a prohibition on ever raising tariffs in the future (with only a few possible exceptions).

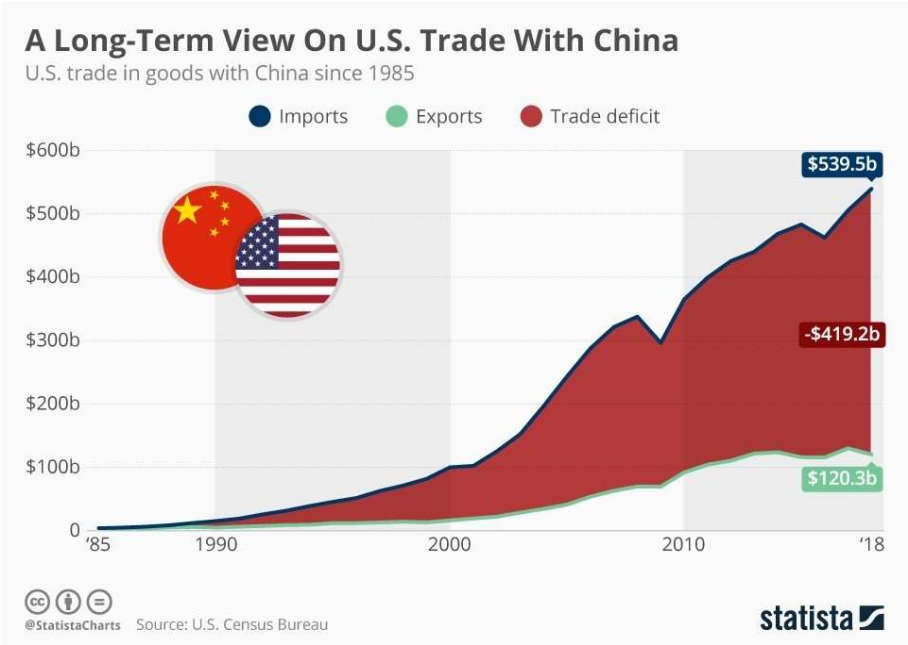
Just 3 years after the end of WWII, a GATT round of negotiations resulted in an exchange of 5,000 tariff concessions, and the continuing progress of Post-WWII trade liberalization. Later on, in 1956, GATT member-states managed to cut 23 billion dollars-worth of tariffs.

The GATT has continued to lead the world towards a future of prosperous international trade and reduced tariffs and customs even at times when West Germany and the US went on a trade war for chicken breasts and potatoes. Eventually, during a GATT round of negotiations that began in 1986 and ended in 1994, member states agreed to create the World Trade Organization (WTO), which would replace the GATT as the main intergovernmental organization that regulated global trade. Indeed, in 1995, the GATT ceased to exist and was replaced by the WTO.

During the presidency of Donald Trump, the US reduced its involvement in global trade, believing that focusing on local industry would create jobs. More importantly for our discussion, Trump reduced trade with major Asia-Pacific economies such as Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, and Vietnam. Moreover, after promising to reduce the US trade deficit with China by implementing tariffs during his campaign, Trump directed the Office of the United States Trade Representative (USTR) in August 2017 to investigate Chinese economic practices. The results of the investigation showed that China allegedly used illegal harmful practices, such as dumping measures, and as a result, Trump ordered the imposition of tariffs on Chinese products, as well as restrictions on Chinese investment in high-tech sectors of the US economy and presented the charges against China to the WTO.

In response, the Chinese government claimed that the only reason for Trump's action is to "stop Chinese's growth as a world power", and matched the US's tariffs by implementing 25% tariffs on many US exports.

From January 2018 until the end of Trump's presidency, the US and China went on a game of 'tariff Ping Pong'. From soybeans to shoes to blueberries, tariffs were placed on nearly every facet of the economy. The fact that the trade war escalated so fast is concerning and leads us to the present issue.



Even after the end of Trump's presidency we still can't say that the war is over since Biden "isn't in a hurry to lift the tariffs", and is yet to take significant action on the issue.

Current Situation

The trade war caused economic pain on both sides. It has already cost more than 300,000 American jobs, and an additional 1.2 million jobs that the U.S. exports to provide and 197,000 Americans that are directly employed by Chinese multinational companies are at risk. The tariffs forced American companies to cut wages and jobs for U.S. workers, defer potential wage hikes or expansions, and raise prices for American consumers or companies.

China also felt economic pain as a result of the trade war. Indeed, as the trade war dragged on, Beijing lowered its tariffs for its other trading partners as it reduced its reliance on U.S. markets. Popular Chinese brands like Haier, Huawei and Shein are also suffering from financial costs due to the fact that a major part of their consumers come from the US.

Third party countries that aren't directly involved in the conflict are also experiencing difficulties: studies show that the world's recovery from COVID 2019 is expected to slow dramatically and experts believe that lack of cooperation between the two world powers will also postpone solutions for other world issues like Climate change, COVID and more.

However, there have been a few third party countries which have benefited from the trade war, since the US and China started looking for trade products with other countries like Argentina, South Africa, France, Singapore and Vietnam.

Questions to Consider

1. Has your country ever participated in a trade war?
2. What countries does your country export to?
3. What countries are your main source of imports?
4. Is your country a part of the World Trade Organization (the WTO)?
5. How does your country benefit from foriegn trade?
6. Is your country affected by the US-China trade war?
7. What should be done to reduce the risks of a future trade war?

Suggested Reading

- Timeline- https://www.dailyfx.com/research/trade-wars-history#
- https://edition.cnn.com/2020/05/19/economy/us-china-trade-war-resume-coronavirus-intl-hnk/index.html
- https://www.theguardian.com/us-news/2017/jan/23/donald-trump-first-orders-trans-pacific-partnership-tpp
- https://www.brookings.edu/blog/order-from-chaos/2020/08/07/more-pain-than-gain-how-the-us-china-trade-war-hurt-america/
- The trade war under Biden's presidency- https://www.scmp.com/economy/global-economy/article/3134191/us-china-relations-there-still-trade-war-under-joe-bidens