Model United Nations Prague

PragueMUN 2021

OUT OF THE BOX

8th - 10th February

STUDY GUIDE

NATO

It's time to be Unique!

Table of Contents

Letter of Welcome

Dear Delegates,

Manon and I are excited, delighted and thrilled to welcome you to PragueMUN 2021. Last year, both of us were in your shoes, being delegates of PragueMUN's 2020 edition. We had such a good time that we decided to contribute to this year's edition and take it to another level by chairing a committee.

Since NATO is characterised by its consensus decision-making, for us personally it embodies the very essence of MUN'ing. Of all committees usually present at an MUN conference, the need to look for common ground and take and give is especially crucial. Without losing your country's interests out of sight, the main aim is security, which can only be preserved when there is agreement on how to proceed. The challenging part is that one vote against is enough to make a communiqué fail. The interesting side is that you have to unleash the best version of your inner diplomat in order to get all delegations on the same page.

We do realise both topics are quite challenging and can require an extensive preparation. We strongly encourage you to come as prepared as possible since this determines the very quality of the committee and naturally, we want all of you to have the best experience possible.

We look forward to tense debates, to witness eagerness and for you to have an experience of a lifetime.

With any questions, please feel free to contact us or the PragueMUN secretariat.

Kind regards,

Manon Duymelinck and Mattiece Vantyghem

About the Committee

In 1947, the Treaty of Dunkirk was signed, a treaty of mutual assistance and alliance between the United Kingdom and France. The ratio of the treaty was joining forces against future German aggression. One year later, The Netherlands, Luxembourg and Belgium joined this initiative hereby creating the Western Union, established by the Treaty of Brussels. In 1949 North America joined together with Portugal, Canada, Norway, Italy, Iceland and Denmark, creating the North Atlantic Treaty organization (NATO alliance). Originally there were 12 member states, today there are 30.

The raison d'être of NATO is the protection of the security and freedom of its 30 member states through military and political means, thereby promoting democratic values and encouraging cooperation between the members regarding security matters.

The core principle of collective defense of NATO is laid down in the Article 5 of its Treaty, stating that that an armed attack against one of its members is considered as an attack against all of them. This article was only triggered once in history after the terrorist attacks on September 11th, 2001 in the United States of America (USA).

It is important to note that NATO is not a United Nations-body, meaning that the decision-making process and the results of it are different. The primary political decision-making body is the North Atlantic Council, located in Brussels. The Council can assemble on different levels, it can be held at Permanent Representative Level or it can be composed of Heads of Government or Ministers of Defense of the Member states.

To summarize, NATO is a body which gathers high-level representatives of members whose pressing issues and policies are then manifested in a communiqué. Unlike UN bodies, the outcome of NATO negotiations is a communiqué. Decisions made in NATO represent a collective will of all the members and are therefore made by consensus.

Topic A: Multilateral cooperation in cybersecurity

Introduction

Over the current and past century, our world has been changing drastically. We've seen men go into space, women fight for gender equality and races all over the globe come together as one – even if the division in the modern world is still very present to this day. The world is no longer divided into isolated continents but is connected through several media. One of the big catalysators in this process has been the internet and the social media that comes with it. In the current social climate, everyone is connected with one another. Whereas our great-grandparents mostly had friends in their hometown and perhaps a bit beyond, the new generation has connections all over the planet. From Mozambique to New York, connecting with a stranger, a friend or even the culture and local news is only one click away.

However, with great power comes great responsibility. This is no different for the five largest technology companies worldwide (from now on referred to as the "Big Tech" or "Big Tech companies") that often run these social media platforms. These Big Tech companies (i.e., Google, Apple, Microsoft, Facebook & Amazon) are the most dominant players on the market when it comes to information technology.[1] On one hand, they have the responsibility to protect their users from data breaches by cybercriminals. This is an all-together effort that does not just concern the Big Tech but the intergovernmental bodies and states as well. On the other hand, it has been evident over the years that the tech companies have been commercializing the data that they harvest from their users more and more. Consequentially, they sell this data to the highest bidder, no matter their respective motive. This issue as well has lately been getting more and more criticism by NGO's and international organisations alike. The previously mentioned divides the topic into two separate problems that however often find themselves to intertwine with one another.

In conclusion, cybersecurity is a broad and eventful subject. It's also a new and often unexplored judicial area and lots of debate is still to be held on the international level.

[1] Sandbu, M. (2019). The Economics of Big Tech. https://www.ft.com/economics-of-big-tech (Last Access: November 19th, 2020).

History of the topic

When talking about the start of the internet, there is no clear starting point. The idea of a "world wireless system" was being discussed as early as the 1900s (i.e. Nikola Tesla). However, we will only discuss the most pivotal points of this evolution. Concretely, in this chapter, first a timeline is presented, followed by the measures that have already been taken against cybercrime and excessive mass data collection.

The first pivotal point is situated in the late 1960s with the creation of the Advanced Research Projects Agency Network (ARPANET). Funded by the U.S. Department of Defence, ARPANET was a system that allowed switching between multiple computers within a single network to communicate.[2] The internet started to exponentially boom in 1990s. It started with the second-generation cellular network[3] (2G) that used digital signals between mobile phones and cellular towers. The 2G network increased overall system capacity as it stepped away from the classic analogue transmission and introduced us to data services such as text messaging.[4] This is followed by the launch of the first commercial web publication and first website to offer clickable advertisements, the Global Network Navigator (GNN) in 1993. By 1994, the largest commercial databases reach up to 10 terabytes. From 1996, it has become a fact that digital storage is more cost-effective than paper regarding the storage of data and by 2002, digital information storage officially surpasses the non-digital storage. Consequently, by 2007, it has become clear that the new age is digital as 94% of the world's information storage capacity is digital. By the summer of 2014, the world reached a total of 3 billion Internet users worldwide. With so much data on the web and so many users transforming from consumers into data subjects[5], a new legal framework and stricter regulations on cybersecurity are required.

When looking at the measures taken in the realm of cybercrime, the 2001 *Convention on Cybercrime* by the Council of Europe can be noticed, which has so far been the sole global agreement controlling certain types of malpractice online.[6] On a continental level, the *Directive on Security of Network and Information Systems* (2016) was adopted by the European Union

[2] Andrews, E. (2019). Who Invented the Internet? https://www.history.com/news/who-invented-the-internet (Last Access: November 19th, 2020).
[3] Cambridge University Press. (s.a.). 2G. https://dictionary.cambridge.org/dictionary/english/2g (Last Access: November 19th, 2020).
[4] Press, G. (2015). A Very Short History of Digitization. https://www.forbes.com/sites/gilpress/2015/12/27/a-very-short-history-of-digitization/?sh=70eb1f0f49ac (Last Access: November 19th, 2020).
[5] Chapter I, Art. 4 (1) of the *Regulation of the European Parliament and of the Council. (27/04/2016)*
[6] Stolton, S. UN backing of controversial cybercrime treaty raises suspicions. https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/ (Last Access: November 20th, 2020).

among others. On a corporate level as well, an interest in cooperative measures in the war on cybercrime emerges. A primary example of this is the *Cybersecurity tech accord* by the Microsoft Corporation in 2018. Signed by well over a hundred technological companies, such as Facebook, Dell and Nokia, the accord aims to improve security, resilience and stability of cyberspace by partnering up on initiatives.[7] Furthermore, when it comes to personal data protection and the role of the Big Tech in it, the 2014 *Convention on Cyber Security and Personal Data,* adopted by the African Union is a great illustration. Over the summer of 2020, the European Union as well has taken measures against these Big Tech companies by creating a 'hit list' of up to 20 large internet companies. This hit list will make that the internet companies will face new and tougher rules aimed at curbing their market power.[8]

To summarize, a more regional approach is used in the case with cybercrime. The consequential lack of a global multilateral approach so far is the weak spot of this topic. To look for solutions to this problem, it is essential to first dive a bit deeper into the problems behind the subject.

[7] Microsoft Corporation. (2018). About the cybersecurity tech accord. https://cybertechaccord.org/about/ (Last Access: November 20th, 2020).
[8] Reuters Staff. (2020). EU planning tougher regulation for 'hit list' of big tech firms. https://uk.reuters.com/article/us-eu-tech-idUKKBN26W0XV (Last Access: November 21st, 2020).

Discussion of the problem

When discussing issues that the topic encompasses, it is important to make a distinction between the classic and perhaps the better-known problem of cybercrime on one hand and the issues regarding mass data collection by the Big Tech companies on the other. Therefore, this chapter is divided into three subcategories, namely the discussion of the aforementioned two problems and a conclusion.

Cybercrime

When discussing the first question, it is important to focus on data leaks in particular as they are the biggest form of cybercrime today. According to the definition used by the European Commission, a data breach "occurs when the data for which a company/organisation is responsible, suffers a security incident resulting in a breach of confidentiality, integrity or availability".[9] An example of such a data breach is the 2017 Equifax blunder, where a data hack aimed at the American multinational consumer credit reporting agency had exposed the personal information of 147 people.[10] Such personal information included birth dates, home addresses, driver's license information and even Social Security numbers and tax ID numbers.[11]

The way these data breaches occur will be analysed, as this helps in understanding the core problem better. According to the Verizon's 2020 Data Investigations Report, roughly 45%[12] of all data leaks is due to criminal hacking – mainly involving stolen credentials. These credentials could be acquired through purchasing them on the dark web or using a password-generating machine for example. From there on the criminals can extract as much sensitive information as possible to sell it back on the dark web or to commit fraud.[12] Another common reason for data leaks is a simple human error (22%)[12]. These errors could refer to an employee either sending sensitive information to the wrong person or misconfiguration of a database containing this information, albeit without malicious intent. Furthermore, social engineering (22%)[12] and the use of malware (17%)[12] are important factors as well in the data breaches.

[9] European Commission. (s.a.). What is a data breach and what do we have to do in case of a data breach? https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en (Last Access: November 21st, 2020).
[10] Federal Trade Commission. (2020). Equifax Data Breach Settlement. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (Last Access: November 21st, 2020).
[11] Ramsey, D. (2019). How a Data Breach Can Impact You. https://www.daveramsey.com/blog/data-breach-impacts (Last Access: November 24th, 2020).
[12] Irwin, L. (2020). The 6 most common ways data breaches occur. https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur (Last Access: November 24th, 2020).

This social engineering happens through methods such as phishing and pretexting, where cybercriminals obtain information under false pretences and later commit fraud with this information, sell it once again on the dark web or contact a third-party.

As seen in the previous paragraph, the most frequent causes of a data breach – apart from malware – find themselves happening because of non-technological malpractices like the use of one's cunning or wit to obtain the sensitive information. This adds an extra layer to finding solutions for the issue of cybercrime, as we will discuss further in the chapter Possible Solutions.

Mass data collection

In addition to cybercrime, another side of the problems surrounding cybersecurity finds itself within the dangers of mass data collection by Big Tech companies. This data is collected by so-called 'cookies', which are messages that web servers pass to your web browser when you visit Internet sites. Your browser then stores each message in a file and when you request another page from the server, your cookie sends the message back to the server. These messages usually contain information you either volunteered, such as your name and interests, or about your visit to the page in general.[13] The information they gain from these cookies is usually accessible only for the creator of that website. However, in recent years, a commercialisation of the acquired information has been established, where the data is offered to the highest bidder. In the following paragraphs concrete examples of this commercialisation will be shown, as well as the dangers that come with it and the difficulty of solving this issue.

Firstly, the 2018 Facebook data-sharing scandal will be discussed. The New York Times acquired a cache of documents from within Facebook that exposed that the social network gave other tech giants such as Amazon, Spotify and Microsoft far greater access to people's data than it had disclosed.[14] These so-called data-sharing arrangements allowed not only the companies with granted data access to grow, but also enabled Facebook information in return,

[13] Indiana University. (s.a.). What are cookies? https://kb.iu.edu/d/agwm (Last Access: November 25th, 2020).
[14] Dance, G. (2018). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (Last Access: November 25th, 2020).

thus, making Facebook a bigger player on the market (e.g. Facebook's "People You May Know" feature used data from sites such as Amazon).[15] [16]

Secondly, abuse of power by the Big Tech will be illustrated. During early November 2020, the European Commission sent out a Statement of Objection to Amazon for the use of non-public independent seller data.[17] Additionally, it opened up a second investigation into its e-commerce business practices. Concretely, the Commission charged Amazon with abuse of its dominant position in online retail market to gain an unfair advantage over its competitors.[18] According to the Commission, Amazon does so by using its size, power and data to gain this advantage over smaller merchants that sell on its platform. The European Union (EU) regulator further explained that Amazon also collects the data of the competitors that sell on their platform and uses the sensitive information that they get to better target its own products.[19] The effects of the mass data collection by Big Tech companies not only influences individuals, but also global economies and its respective actors as well.

Lastly, perhaps the most notorious abuse of big data in recent years will be addressed - the Cambridge Analytica (CA) case. In 2015, the Guardian made the first reports that the political firm Cambridge Analytica was hired by the Republican party – and thus later by the Trump campaign - to acquire access to private data of millions of Facebook users.[20] More specifically, the firm offered tools that could identify personalities of American voters and influence their behaviour in the process. The aforementioned data included details on users' friend networks, identities and "likes". This information was then used for targeted digital advertising by Cambridge Analytica.[21] While this could be seen as a data hacking, the access to the data was

[15] Madrigal, A.C. (2018). Facebook didn't sell your data; It gave it away. https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/ (Last Access: November 25th, 2020).
[16] BBC. (2018). Facebook's data-sharing deals exposed. https://www.bbc.com/news/technology-46618582 (Last Access: November 26th, 2020).
[17] European Commission. (2020). Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 (Last Access: November 26th, 2020).
[18] BBC. (2020). Amazon charged with abusing EU competition rules. https://www.bbc.com/news/business-54887650 (Last Access: November 26th, 2020).
[19] Yun Chee, F. (2020). Europe charges Amazon with using dominance and data to squeeze rivals. https://www.reuters.com/article/us-eu-amazon-com-antitrust/europe-charges-amazon-with-using-its-dominance-and-data-to-squeeze-rivals-idUSKBN27Q18E (Last Access: November 26th, 2020).
[20] Davies, H. (2015). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data (Last Access: November 27th, 2020).
[21] Granville, K. (2018). Facebook and Cambridge Analytica: What you need to know as fallout widens. https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=sectionfront (Last Access: November 26th, 2020).

once again granted without any problems. It seems Facebook's terms of service allowed this data to be used for academic research. The team of CA claimed indeed to be using the data for such academic research, but then proceeded to sell it to Strategic Communications Laboratories.[22] Therefore, the Cambridge Analytica is the perfect illustration of a merger between the two issues discussed in this chapter. It has certain aspects of a data hacking; however, it also puts Facebook at blame for putting such extensive amount of information to be accessible and prone to abuse. Therefore, a regulation on these practices is of high importance.

Sadly, when observing efforts made by (inter)national bodies to restrict the Big Tech, an obsolescence following these efforts can be noticed. In a recent report by the European Court of Auditors (ECA) on the antitrust legislation of the European Commission, the verdict was that the Commission was too slow, lacked the arsenal to handle anti-competitive practices adequately and that "upscaling of market oversight was necessary".[23] [24]

Conclusion

To summarize, it is on one hand evident that the issues regarding the topic of cybersecurity are complex. In addition, the consequences of these issues are even more widespread – varying dramatically in impact. On the other hand, solving these issues has not been so straightforward task. A lot of different factors often influence possible solutions in numerous ways. These factors will be elaborated on in the next chapter as it presents previous actions taken by NATO and the United Nations.

[22] Madrigal, A. C. (2018). What took Facebook so long? https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866/ (Last Access: November 27th, 2020).
[23] Lemmens, K. (2020). Europese Commissie holt achter big tech aan. https://www.standaard.be/cnt/dmf20201119_98120262? (Last Access: November 27th, 2020).
[24] European Court of Auditors. (2020). Special Report No 24/2020: The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight. https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=56835 (Last Access: November 27th, 2020).

Previous NATO and UN involvement

In this chapter, the actions formerly taken by NATO and in extent the United Nations will be reviewed, as it is prominent figure within the international community as well. After having discussed these measures in two separate subsections, a conclusion will close off this chapter.

NATO

So far, the most substantial statement released by NATO in regard to cybersecurity were articles 72 and 73 of the 2014 Wales Summit Declaration.[25] The policy established that cyber defence is part of the Alliance's core tasks of collective defence. Aside from its top priority of protecting the information and communication systems operated by NATO, the policy also provides for streamlined cyber defence governance, the integration of cyber defence into operational planning and procedures for assistance to Allied countries that have fallen victim to cyber-attacks.[26] In addition, a Memorandum of Understanding (MoU) on cyber defence was signed during NATO's Defence Minister's meeting in October 2016. In that MoU, NATO and each of the 28 Allied cyber defence authorities set out arrangements for the exchange of a variety of cyber defence related information and assistance to enhance cyber incident resilience, prevention and response capabilities.[27]

Another of NATO's cybersecurity policies is the 2016 Cyber Defence Pledge, which is a key element in enhancing cyber resilience. Concretely, the pledge states that while each Ally is responsible for its own defences, NATO aids its members in extending these defences, i.e. sharing real-time information about threats through a dedicated malware information sharing platform, developing targets for Allies to facilitate a common approach to their cyber defence capabilities, and lastly, maintaining rapid-reaction cyber defence teams that can be sent to help Allies.[28] Finally, at the Warsaw Summit in 2016, NATO also declared cyberspace as a domain of operations – just like air, sea and land.[29]

[25] NATO. (2014). Wales Summit Declaration. https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber (Last Access: November 27th, 2020).
[26] NATO. (2016). NATO Cyber Defence Fact Sheet July 2016. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (Last Access: November 27th, 2020).
[27] NATO. (2016). Signing of Memorandum of Understanding on Cyber Defence. https://www.nato.int/cps/en/natohq/photos_136551.html (Last Access: November 27th, 2020).
[28] NATO. (2019). NATO Cyber Defence Fact Sheet February 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf (Last Access: November 27th, 2020).
[29] NATO. (2016). Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Last Access: November 27th, 2020).

Unfortunately, NATO's measures still seem to fall short from time to time. Over the summer of 2020, a Russian hacker group, known by names such as APT28, Fancy Bear, Sednit and STRONTIUM, aimed a targeted attack campaign at multiple government bodies.[30] The modus operandi of the group was to deliver a hard-to-detect strand of malware to these government bodies. For this, they pretended to be providing NATO training materials.[31] This example showcases that cybercriminals are very swift, innovative and adaptable.

United Nations

Seeing as the United Nations is not the current body of debate, only one recent illustration of high importance of the United Nations commitment to cybersecurity will be presented. In December 2019, a Russian-led and Chinese-backed resolution A/RES/74/247 on Countering the use of information and communications technologies for criminal purposes was adopted by the General Assembly.[32] The resolution has been met with considerable criticism, mainly by Western powers, over perceived attempts for state cyber controls and limitation of internet freedom[33]. According to the Council of Europe's head of cybersecurity, Alexander Seger, "such a treaty may become problematic in terms of human rights and rule of law protection."[34] Other opponents of the resolution fear that the plans adopted by the United Nations may lead to an erosion of freedom of expression online rather than combat the actual issue of cybercrime. This example goes to show that multilateral cooperation in light of cybersecurity seems difficult, as views on effective measures and freedom of speech among states seem to differ more greatly than ever.

Conclusion

To conclude, in addition to the issues mentioned in the chapter Discussion of the problem, a lack of secure transfer of training materials/knowledge by NATO and conflicting objectives between human rights and effective measures can be identified.

---

[30] Cyber Security Review. (2020). Russian hackers use fake NATO training docs to breach govt networks. https://www.cybersecurity-review.com/news-september-2020/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/ (Last Access: November 29th, 2020).

[31] Sharma, A. (2020). Russian hackers use fake NATO training documents to breach government networks. https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/ (Last Access: November 29th, 2020).

[32] Jabbar, F.H. (2019). Countering the use of information and communications technologies for criminal purposes. https://www.undocs.org/A/74/401 (Last Access: November 29th, 2020).

[33] Radio Free Europe / Radio Liberty (2019). U.S. Concerned Russia-Backed UN Resolution Will Hurt Online Freedom. https://www.rferl.org/a/us-russia-internet-un/30335318.html (Last Access: January 7th, 2021).

[34] Stolton, S. (2019). UN backing of controversial cybercrime treaty raises suspicions. https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/ (Last Access: November 29th, 2020).

Possible Solutions

Finally, the chapter of possible solutions is being examined. As in what can be described as perhaps the most inspiring chapter, some possible solutions that may help you in your thinking process on the subject will be discussed. Once again, this will be done by distinguishing the issue of cybercrime from that of mass data collection.

Cybercrime

When looking at solutions for cybercrime, the primary concern should be with individuals. Their safety and security are first and foremost of utmost importance. Therefore, it is necessary to look at the vulnerabilities of the internet users themselves. Cybercrime is often based on the manipulation of unsuspecting users. This happens when the cybercriminals pose as other people or organisations. To fight such scams, blacklisting and whitelisting webpages in an even more extensive way are essential. This will reduce the risk of infection as the users stay away from the 'bad neighbourhoods' of the internet.[35] In addition, educating every internet user about the dangers of the internet seems necessary.[36] Another way of targeting cybercrime would be to take on these cybercriminals directly. This could be done through several measures, e.g. active targeting of underground fora in order to disrupt the circulation of easy and powerful tools, such as malware kits and botnets; developing insight into the behaviour of the contemporary cybercriminal; and active targeting of the proceeds of cybercrime in collaboration with the financial sector.[37] The last proposal is an easy-to-formulate, though hard-to-enact solution. It refers to the strengthening of international cooperation and dialogue. Not only between governments, but also with the United Nations, NATO, INTERPOL (The International Criminal Police Organization) and many other partners, including civil and business society with a stake in stopping cybercrime.[38]

[35] UNODC. Asia Pacific Regional Workshop on Fighting Cybercrime. https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/SYMC_UNODC_ITU_Cybercrime_Workshop.pdf (Last Access: December 1st, 2020).
[36] DELL. Top 10 Steps To Help Stop Cybercrime. https://www.dell.com/downloads/ca/support/top_10_steps_to_protect_against_cybercrime_dell_en.pdf (Last Access: December 1st, 2020).
[37] Guha, D. (2019). Cyber Crimes- Challenges & Solutions. https://www.researchgate.net/publication/284398152_Cyber_Crimes-_Challenges_Solutions (Last Access: December 1st, 2020).
[38] UNICWASH. (2019). Taking action where we can to stop cybercrime. https://unicwash.org/oped-cybercrime/ (Last Access: December 1st, 2020).

Mass Data Collection

Perhaps the toughest issue to regulate is the mass data collection by the Big Tech companies. In the area of antitrust, a solution could be accomplished by making Big Tech corporations share their data with smaller companies.[39] This way viable alternatives for the Big Tech are created. However, as stated earlier, antitrust should not be the focus.[40] Instead, interests should aim at accommodating internet users with the best possible protection from Big the Tech, although it might contain some antitrust regulation. A first solution could be to create an overarching regulatory structure among all Allied states.[41] Here all states together decide upon an appropriate regulatory scope for the tech industry. This will create clarity for both companies and individuals on what is protected and what is not. For this, a risk-based approach, where prioritisation of risky activities and companies could be used. Working together with the private sector here should be essential. A last solution could be to supervise new technology in a more effective manner. Nowadays, the tech industry generally ships products from the moment they function. This is known as a minimally viable product and often leaves quality (and damage) control to end users (e.g. failures in new categories like facial recognition and AI). That is why new technologies, much like new medicines, are ought to demonstrate safety and efficacy before coming to the market. In addition, Big Tech should be held financially accountable for any harm their products cause, just like chemical companies right now. Personal liability for engineers and executives could be highly important in this regard.[42]

[39] Foroohar, R. (2019). Our personal data needs protecting from Big Tech. https://www.ft.com/content/04d3614e-078a-11ea-a984-fbbacad9e7dd (Last Access: December 2nd, 2020).
[40] Chen, A. (2019). How to regulate Big Tech without breaking it up. https://www.technologyreview.com/2019/06/07/135034/big-tech-monopoly-breakup-amazon-apple-facebook-google-regulation-policy/ (Last Access: December 2nd, 2020).
[41] Charrie, A. and Quest, L. (2019). The Right Way to Regulate the Tech Industry. https://sloanreview.mit.edu/article/the-right-way-to-regulate-the-tech-industry/ (Last Access: December 2nd, 2020).
[42] McNamee, R. (2020). Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy. https://time.com/5872868/big-tech-regulated-here-is-4-ways/ (Last Access: December 2nd, 2020).

Bloc positions

In this chapter, typical bloc positions in a very brief manner are mentioned. Generally, and given the country matrix for this committee, we can distinguish two big blocs. The first one being the quintessential “Western Powers”, followed by the upcoming powers in Eastern Europe.

Western Powers

The so-called Western Powers are the first big bloc we can discern. Generally, the West is the main actor when it comes to investing in innovation and working with businesses and organizations.[43] For example, the United Kingdom (U.K.) passed a cybersecurity policy that spans from 2016 to 2021 and calls upon companies to improve security to appease risk to government and public organizations.[44] Additionally, the U.K. launched two cyber innovations centers, investing heavily on research and development. The United States as well decided to adopt the Cybersecurity National Action Plan.[45] These are no unnecessary measures, seeing as the United States and other West European states have been the nations encountering significant amounts of cyberattacks every year.[46] Consequently, these states have been very open to cooperating in the field of cybersecurity. However, they remain wary of too excessive cybersecurity measures and want to find balance between freedom of expression online and the measures on cybercrime.

[43] Careers in cybersecurity. (2016). From the U.S. to Europe and Asia: Cybersecurity Policies Around the Globe. https://careersincybersecurity.com/u-s-europe-asia-cybersecurity-policies-around-globe/ (Last Access: November 30th, 2020).
[44] HM Government. (2015). National Cyber Security Strategy 2016-2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Last Access: November 30th, 2020).
[45] The White House. (2016). FACT SHEET: Cybersecurity National Action Plan. https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (Last Access: November 30th, 2020).
[46] Analytics Insight. (2019). Top 6 countries with the best cyber security measures. https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/ (Last Access: November 30th, 2020).

Eastern Bloc

When discussing states in Eastern Europe it is important to stress that the main focus is on eccentric states that have a diverging view from the aforementioned Western countries. For the majority of the other Eastern European countries, it is safe to state that they do not have a controversial view on the matter of cybersecurity.[47]

However, three East-European states in particular remain subject to scrutiny when it comes to their actions on cybersecurity. From anti-terror surveillance legislation by Hungary that breaches privacy[48] [49], to crossing the line from regulation to discrimination in Poland.[50] The last example could be the augmented interest of the Turkish authorities in using legislative, judicial and technical capacity to block and monitor user activity online. This as well has raised concern for rights and freedoms online.[51]

Conclusion

To summarise, both the West and the East in our committee feel the need to act urgently upon the issue of cybersecurity. However, tensions may arise when discussing the ways of solving these issues. While Western-minded countries seem to be very eager to tackle cybercrime and the mass data collection by the Big Tech, they also stress the need to protect a certain set of basic human rights. In recent years, this is something that specific East-European countries seem to have less troubles with.

[47] Saljic, E. and Tusko, D. (2018). Cybersecurity Policies of East European Countries. https://www.researchgate.net/publication/325196481_Cybersecurity_Policies_of_East_European_Countries (Last Access: November 30th, 2020).
[48] ECHR 014. (2016). no. 37138/14.
[49] EURACTIV. (2016). Hungary anti-terror spy law breaches privacy: European rights court. https://www.euractiv.com/section/justice-home-affairs/news/hungary-anti-terror-spy-law-breaches-privacy-european-rights-court/ (Last Access: November 30th, 2020).
[50] Matthaiou, A. and Vermulst, E. (2020). Crossing the line from regulation to discrimination: the draft Polish National Cybersecurity Act as a protectionist step in the 5G race (Part 1). http://regulatingforglobalization.com/2020/09/17/crossing-the-line-from-regulation-to-discrimination-the-draft-polish-national-cybersecurity-act-as-a-protectionist-step-in-the-5g-race-part-1/ (Last Access: November 30th, 2020).
[51] Ergun, F. D. (2018). Naional Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy. https://edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/ (Last Access: November 30th, 2020).

Relevant international documents and further reading

After you have read this study guide, both of us, chairpersons, recommend you read further relevant documents on the matter in order to write a knowledgeable position paper as well as debate the topic eloquently. We also strongly encourage you to check out the sources cited throughout the study guide as they may often delve deeper into the topic.

Relevant international documents

- European Court of Auditors - Special Report No 24/2020: The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight (2020)
- NATO - Wales Summit Declaration (2014)
- NATO - Warsaw Summit Communiqué (2016)
- NATO Cooperative Cyber Defence Centre of Excellence – Talinn Manual 2.0 (2017)
- The United Kingdom - National Cyber Security Strategy 2016-2021 (2015)
- United Nations General Assembly - Resolution A/RES/74/247 on Countering the use of information and communications technologies for criminal purposes (2019)

Further reading

Bechis, F. and Gilli, A. (2020). NATO and the 5G challenge. Available at: https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html.

Birch, D. (2020). Big Regulation Coming for Big Tech. Available at: https://www.forbes.com/sites/davidbirch/2020/10/12/big-regulation-coming-for-big-tech/?sh=4659e2007001.

Careers in cybersecurity (2016). From the U.S. to Europe and Asia: Cybersecurity Policies Around the Globe. Available at: https://careersincybersecurity.com/u-s-europe-asia-cybersecurity-policies-around-globe/.

Charrie, A. and Quest, L. (2019). The Right Way to Regulate the Tech Industry. Available at: https://sloanreview.mit.edu/article/the-right-way-to-regulate-the-tech-industry/.

European Commission (2020). Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077.

Guha, D. (2019). Cyber Crimes- Challenges & Solutions. Available at: https://www.researchgate.net/publication/284398152_Cyber_Crimes-_Challenges_Solutions.

Jabbar, F.H. (2019). Countering the use of information and communications technologies for criminal purposes. Available at: https://www.undocs.org/A/74/401.

McNamee, R. (2020). Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy. Available at: https://time.com/5872868/big-tech-regulated-here-is-4-ways/.

NATO (2016). NATO Cyber Defence Fact Sheet July 2016. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf.

NATO (2019). NATO Cyber Defence Fact Sheet February 2019. Available at: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf.

The White House (2016). FACT SHEET: Cybersecurity National Action Plan. Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

United Nations Office on Drugs and Crime (2010). Asia Pacific Regional Workshop on Fighting Cybercrime. Available at: https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/SYMC_UNODC_ITU_Cybercrime_Workshop.pdf.

Woollacott, E. (2020). Big Tech Is 'Almost Human Rights-Free Zone' UN Report Warns. Available at: https://www.forbes.com/sites/emmawoollacott/2019/10/16/big-tech-is-almost-human-rights-free-zone-un-report-warns/?sh=124e03413217.

Questions to consider

1) What should your country focus on within the cybersecurity debate? Cybercrime or mass data collection?

2) How can NATO stop the use of our own technologies against us?

3) How can NATO and all its allies in extension be up to date with the Big Tech companies?

4) Which states may work towards or away from multilateral cooperation?

5) How will the committee address the right of free speech considering the regulation on cybercrime?

6) Should NATO broaden the cooperation field beyond Allied states?

7) What is the role of antitrust in regulating the Big Tech companies for internet users?

Topic B: The New START, Alliance stance towards and role in the new strategic structure

Introduction

The New START (Strategic Arms Reduction Treaty) is a nuclear arms treaty between Russia and The United States of America (USA) with the aim of limiting the amount and use of nuclear weapons. The New START Treaty replaces the START Treaty signed in 1991, limiting US and Russian nuclear forces even more.

The specific limits of the New START are as follows[52]:

- 1,550 nuclear warheads on deployed intercontinental ballistic missiles (ICBMs), deployed submarine launched ballistic missile (SLBMs), and deployed heavy bombers equipped for nuclear armaments (each such heavy bomber is counted as one warhead toward this limit);
- 800 deployed and non-deployed ICBM-launchers, SLBM-launchers, and heavy bombers equipped for nuclear weapons;
- 700 deployed ICBMs, SLBMs, and heavy bombers equipped for nuclear weapons.

To put into perspective, the New START treaty reduces the deployment of nuclear weapons of Russia and the USA by one third. It includes an efficient verification regime. In addition, it does allow for flexibility which is much needed to protect national security. This Treaty is a beautiful "lead-by-example" by the two most powerful nuclear nations in the world.[53]

This Treaty illustrates once again the commitment of the two largest nuclear powers in the world to reduce their nuclear arsenals.[54]

[52] U.S. Department of State (n. d.). New START Treaty. https://www.state.gov/new-start/ (Last Access: January 7th, 2021).
[53] Kimball, G. (2019). A New Nuclear Deal Begins With New START. https://www.armscontrol.org/act/2019-11/focus/new-nuclear-deal-begins-new-start (Last Access: January 7th, 2020).
[54] The White House. (2010). Readout of the president's call with Russian President Medvedev. https://obamawhitehouse.archives.gov/the-press-office/readout-presidents-call-with-russian-president-medvedev-0 (Last Access: December 12th, 2020).

An important feature of this treaty is that it preserves the balance of power between the USA and Russia. With no perception of 'losers' or 'winners' present, the incentive of breaking the agreement is discouraged.[55]

Still, mistrust will always remain as illustrated by the amendment by the Russian Duma before passing the Treaty, stressing Russia's right to withdraw from the New START if the USA would violate the strategic balance with any major missile defence initiatives.[56]

[55] BBC. (2010). Statement by former Russian president Mr. Medvedev. http://news.bbc.co.uk/2/hi/europe/8607985.stm (Last Access: December 12th, 2020).
[56] Weir, F. (2011). With Russian ratificiation of new START, what's next for US-Russia relations? https://www.csmonitor.com/World/Europe/2011/0126/With-Russian-ratification-of-New-START-what-s-next-for-US-Russia-relations (Last Access: December 12th, 2020).

History of the topic

The New START Treaty, despite its importance and significance, is merely one piece in the long chain of initiatives to limit the use and proliferation of nuclear weapons.

During the nuclear attacks on Hiroshima and Nagasaki in 1945, the whole world witnessed the disastrous effects of nuclear weapons in real life, which are felt to this day. This event triggered many initiatives, both international and multi- and bilateral. As the image of nuclear war was established, there was an international consensus that history must be prevented from repeating itself. At all cost should we add; however, the mere possession of nuclear weapons is an important way of expressing power and a powerful means of diplomacy, therefore states are reluctant to extensive dismantling of their nuclear arsenals, mainly funded on mistrust of other nuclear powers.

Luckily, the nuclear diner has always ended with the starters and it never came to a limited or full-scale nuclear war. However, in 1962, the world came close to it as tensions between the USA and the Soviet Union (USSR) reached boiling point with the latter constructing nuclear weapons stations on Cuba with the possibility to reach US soil.

The two most powerful nuclear forces today are Russia and the USA. Together with the international community, both have taken many initiatives towards nuclear disarmament, among others the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) signed by every nation in the world with exceptions of Pakistan, Israel, and India. In 2010, North Korea unilaterally left the NPT framework.[57] The first Strategic Arms Limitation Treaty (SALT I) was signed by Russia and the USA as well.

Yet an era marked by détente (term associated with a period of relaxation of strained relations between the USA and the Soviet Union during the Cold War) might come to an end with the possible demise of the INF Treaty (Intermediate-Range Nuclear Forces Treaty) (concluded between USA and USSR in 1987/1988). This event stresses the importance of the New START Treaty even more, since it is the only remaining treaty limiting nuclear proliferation between Russia and the USA.

[57] Kirgis, F. (2003). North Korea's Withdrawal from the Nuclear Nonproliferation Treaty. https://www.asil.org/insights/volume/8/issue/2/north-koreas-withdrawal-nuclear-nonproliferation-treaty (Last Access: january 7th, 2021).

Discussion of the problem

NATO is committed to nuclear arms control and non-proliferation, yet for as long as nuclear weapons exist, NATO remains a nuclear alliance and nuclear weapons remain a part of their defence arsenals.

From all the NATO members, only three possess nuclear weapons, however the Alliance is eager to ensure *'the broadest possible participation of allies in collective defence planning on nuclear roles, in peacetime basing of nuclear forces, and in command, control and consultation arrangements'*.[58]

An initiative preceding the New START Treaty is the previously mentioned INF Treaty. This treaty is characterised by the elimination of a specific type of nuclear weapons (land-based short- and intermediate range). Unfortunately, the USA decided to pull out of the Treaty responding to alleged Russian violations. Under this treaty, thousands of nuclear weapons were destroyed; therefore, being one of the most effective nuclear disarmament initiatives in history.[59]

With the demise of this Treaty new challenges appear at the surface, especially possible threats from Russia. As a result, the deterrence and defence posture of NATO needs to be revisited in order to keep it fit for purpose as well as for the NATO arms control playbook. One of the arguments Russia employs to justify its behaviour is the fact that the INF treaty did not bind other major nuclear players such as China and therefore lacked efficiency. Therefore, when assessing a future strategy for nuclear stability, one needs to take the security environment in the Asia-Pacific into account, especially possible effects on European security. Assessment of a more inclusive legal nuclear framework, seeing the rise of Asian nuclear powers, is of considerable importance.

In the current state of affairs, the New START Treaty remains the only treaty binding the USA and Russia; and thus, prevents a new nuclear arms race from happening. The New START is to expire in 2021, hence it would be high time to act. However, both presidents can agree to extend it for up to five years, as allowed in the treaty provisions.

The devastating downside of the INF's demise is that both sides can now freely flight test, develop and deploy previously banned systems in Europe and in Asia. On December 18th,

[58] NATO. (2010). Active Engagement modern defence: strategic concept for the Defence and Security of the members of the North Atlantic Treaty Organization, §19.
[59] Council on Foreign Relations (n.d.). U.S.-Russia Nuclear Arms Control 1949 – 2019. https://www.cfr.org/timeline/us-russia-nuclear-arms-control (Last Access: January 7th, 2021).

2019, the Russian President V. Putin stated that '*Russia would be forced to take additional measures to strengthen its security'*.[60]

Regarding NATO, there is no need to deploy these intermediate-range missiles in order to defend NATO or US allies in Asia, because the current existing weaponry, both on the sea and in the air, is sufficient to hold possible attacks from Russia or China. Besides, new systems would constitute enormous development and production costs and would take a considerable amount of time to complete.[61]

A new nuclear missile race should be prevented at all costs. The US Congress, for example, can play a considerable role by refusing to fund new nuclear initiatives. In January 2019, 11 US senators reintroduced the Prevention of Arms race Act of 2019, with the aim of prohibiting funding, flight-testing or deployment of a US ground-launched or ballistic missiles with a range between 500 and 5.500 kilometres until the administration would provide a report that meets certain specific conditions. These include identifying a US ally formally willing to host such a system and, in the case of a European country, demanding that all NATO countries agree to that ally hosting the system.[62]

It is important to repeat that without an extension of the New START Treaty from 2021 on, there would not be any legally binding limit on the world's two largest nuclear arsenals for the first time since 1972. This would entail a violation of Article VI of the NPT to pursue negotiations in good faith on effective measures relating to cessation of the nuclear arms race at an early date and to nuclear disarmament.

[60] Arms Control Association (2019). The Post-INF Treaty Crisis: Background and Next Steps. https://www.armscontrol.org/taxonomy/term/15/about/country-resources/country-resources/blogs/subject-resources/blogs/Daryl%20G.%20Kimball?page=9 (Last Access: January 7th, 2021).

[61] Kimball, D.G. (2018). INF Termination Is Bad, but It Could Get Worse. https://www.armscontrol.org/act/2018-11/focus/inf-termination-bad-could-get-worse (Last Access: December 12th, 2020).

[62] Arms Control Association. (2019). The Post-INF Treaty Crisis: Background and Next Steps. https://www.armscontrol.org/issue-briefs/2019-08/post-inf-treaty-crisis-background-next-steps (Last Access: December 12th, 2020).

Previous NATO and UN involvement

NATO

NATO has a long-term relationship to nuclear arsenals as three of its members – the USA, the U.K. and France have been operating with nuclear weapons for decades. Although the nuclear deterrent and 'nuclear umbrella' over the Allies are one of the core principles of NATO ('supreme guarantee of the security of the Allies'[63]), the Alliance has continuously been decreasing its nuclear stockpile.[64]

Since the height of the Cold War (i.e. 1980s), there has been more than 90% reduction of nuclear weapons committed to the defence of NATO. However, NATO will remain a nuclear Alliance as long as nuclear weapons exist, although at the lowest possible level.[65]

Although 27 other members have under the NPT renounced the option to acquire nuclear arsenal, they all participate in all activities (consultations, training, exercises, etc.) involving forces, command and control. All members with one exception (France pursues its own national nuclear strategy) participate in the Nuclear Planning Group (NRG), where nuclear policies and postures are formulated, irrespective of nuclear weapons ownership.[66] Furthermore, five NATO states (Belgium, Germany, Italy, the Netherlands and Turkey) host US forward-deployed nuclear weapons.[67]

In the 2010 Strategic Concept, NATO pledges to create the conditions for a world without nuclear weapons, which besides other linked to commitments under the NPT. Moreover, in 2018, a working group Creating an Environment for Nuclear Disarmament (CEND; not exclusive to NATO members) was established at the instigation of the USA, with the purpose of 'making the security environment more conducive to further progress towards nuclear disarmament'.[68]

[63] Afina, Y. and Caughley, T. (2020). NATO and the Frameworks of Nuclear Non-proliferation and Disarmament Challenges for the 10th NPT Review Conference. https://www.chathamhouse.org/sites/default/files/2020-05-29-nato-npt-frameworks-caughley-afina-2.pdf (Last Access: January 7th, 2021).
[64] Ibid.
[65] Ibid.
[66] Ibid.
[67] Ibid.
[68] Ibid.

United Nations

Since the establishment of the United Nations, eliminating nuclear weapons has always been on the agenda. For example, the first resolution adopted by the UN General Assembly in 1946[69] established a commission to deal with problems related to the discovery of atomic energy, among others.

The United Nations has an agenda regarding nuclear weapons called 'Securing our Common Future: An Agenda for Disarmament.[70] In this agenda, the Secretary-General calls for resuming dialogue and negotiations for nuclear arms control and disarmament. He also supports extending the norms against nuclear weapons and in that regard appeals to states that possess nuclear weapons to affirm that a nuclear war cannot be won and must never be fought.

Finally, the agenda proposes preparing for a world free of nuclear weapons through numerous risk-reduction measures, including transparency in nuclear-weapons programmes, further reductions in all types of nuclear weapons, commitments not to introduce new and destabilizing types of nuclear weapons, including cruise missiles, reciprocal commitments for the non-use of nuclear weapons and reduction of the role of nuclear weapons in security doctrines.[71]

Many rules can be considered to constitute customary rules of international law by virtue of their near universal acceptance in legally binding instruments, widespread support within the General Assembly and the practice of states. Current developments however are straining many of these norms the most vital of which include the norms against use and testing.[72]

[69] United Nations. (1946). Resolutions adopted on the reports of the first committee. https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/1(I) (Last Access: December 12th, 2020).
[70] United Nations. (2017). Securing our common future: An Agenda for Disarmament. https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit (Last Access: December 12th, 2020).
[71] United Nations. (s.a.). Nuclear Weapons. https://www.un.org/disarmament/wmd/nuclear/ (Last Access: December 12th, 2020).
[72] United Nations. (s.a.). Nuclear Weapons. https://www.un.org/disarmament/wmd/nuclear/ (Last Access: December 12th, 2020).

Possible solutions

The are many effective, useful and balanced solutions to the discussed issue. There is common denominator to all of them – NATO has to be united and send a strong, unified message.

On of possible solutions would be for NATO to declare, as a bloc, that no European member would field any missiles that would have been banned by the INF Treaty as long as Russia reciprocally does not field once-prohibited systems that could reach NATO territory. This would require Russia to remove its approximately 50 9M729 missiles that have been deployed in western Russia.[73]

The US and Russian presidents could agree to this no-first INF missile deployment plan through an executive agreement that would be verified through national technical means of intelligence.

Another possible approach would be to negotiate a new agreement that verifiably prohibits ground-launched, intermediate-range ballistic or cruise missiles armed with nuclear warheads. As a recent United Nations Institute for Disarmament Research study explains, the sophisticated verification procedures and technologies already in place under the New START can be applied with almost no modification to verify the absence of nuclear warheads deployed on shorter-range missiles.[74]

A third variation would be for Russia and NATO to commit reciprocally to each other that neither will deploy land-based, intermediate-range ballistic missiles or nuclear-armed cruise missiles (of any range) capable of striking each other's territory[75]

In addition, national institutions of countries could prove useful in nuclear non-proliferation and disarmament agenda. For example, the US Congress can play a role in blocking US funding for nuclear purposes; therefore, providing a guarantee and managing expectations.

[73] Durkalec, J. (2019). European security without the INF Treaty. https://www.nato.int/docu/review/articles/2019/09/30/european-security-without-the-inf-treaty/index.html (Last Access: January 7th, 2021).
[74] Podvig, P., Snyder, R. and Wan, W. (2019).Evidence of absence: Verifying the removal of nuclear weapons. https://www.unidir.org/files/publications/pdfs/evidence-of-absence-verifying-the-removal-of-nuclear-weapons-en-722.pdf (Last Access: December 12th, 2020).
[75] Arms Control Association. (2019). The Post-INF Treaty Crisis: Background and Next Steps. https://www.armscontrol.org/issue-briefs/2019-08/post-inf-treaty-crisis-background-next-steps (Last Access: December 12th, 2020).

Bloc positions

The end of the INF Treaty represents a significant reduction of the European and global levels of security. The Treaty ceased to restrain Russia's behaviour at a time when NATO was already occupied with addressing challenges in the East and other strategic directions. The termination of the Treaty is also not isolated from the strategic developments elsewhere in the world, in particular the proliferation of intermediate-range missiles in Asia.

In response to the challenges posed by the Russian INF-range capabilities, the Alliance does already have a basis to develop upon. It can build on its adaptation measures from 2014. These steps alone, however, are insufficient. The expansion of Russia's long-range strike capabilities, including the deployment of the SSC-8/9M729 missiles, has created gaps in NATO's overall posture that need to be closed.

To close them, NATO does not need to match Russian investments qualitatively or quantitively. The question for the Alliance is not whether it should invest in new ground-launched missiles in Europe but how best to undermine Russia's confidence in its strategy of winning a short war. This requires measured, long-term and asymmetric adjustments across the whole spectrum of NATO's overall mix of capabilities.

The Alliance needs to overcome its major division along the East-West line. Whereas the West European Allies opt for a rather diplomatic and non-confrontational rhetoric, Eastern Allies, such as the Baltic states, Poland or Romania perceive Russia's actions (not limited to nuclear posture) as threat to their independence or even very existence; thus, preferring approach of pro-active deterrence. As the NATO leading power, it is also essential to take into account the new US administration and its stance on the issue.

Moreover, the Alliance should develop a common approach towards the Asian nuclear powers, be it either inclusive or other. Despite the fact that Russia and the USA are the major nuclear players in the world, there are other countries such as Pakistan, India, Iran, or China that can be defined as quickly evolving nuclear states. As the world's leading military power, NATO could lead the way towards a new, sustainable global nuclear architecture.

Relevant international documents and further reading

Relevant international documents

- Intermediate-Range Nuclear Forces Treaty (INF) (1987/1988)

- NATO's current nuclear policy is based on two major documents:
    - The 2010 Strategic Concept – sets out the Alliance's core tasks and principles, including deterrence (2010);
    - The Deterrence and Defence Posture Review (2012).

- Treaty on the Non-Proliferation of Nuclear Weapons (NPT) (1968/1970)

- United Nations Office for Disarmament Affairs (UNODA) - Securing Our Common Future: An Agenda for Disarmament (2018)

Further reading

Afina, Y. and Caughley, T. (2020). NATO and the Frameworks of Nuclear Non-proliferation and Disarmament Challenges for the 10th NPT Review Conference. Available at: https://www.chathamhouse.org/sites/default/files/2020-05-29-nato-npt-frameworks-caughley-afina-2.pdf.

Council on Foreign Relations (n.d.). U.S.-Russia Nuclear Arms Control 1949 – 2019. Available at: https://www.cfr.org/timeline/us-russia-nuclear-arms-control.

International Court of Justice (n.d.) Legality of the Threat or Use of Nuclear Weapons. Available at: https://www.icj-cij.org/en/case/95.

Questions to consider

1) Where is your country situated? Would it belong to the Western or the Eastern 'wing' of NATO? Is potential proximity of Russia a national security concern?

2) Does your country posses nuclear arsenal? Has your country previously hosted foreign nuclear weaponry on its territory?

3) What is your country's stance on nuclear weapons in general? Should you argue for a nuclear-strong NATO and deterrence or lead the Alliance towards the world without nuclear weapons?

4) Should NATO employ hard power or soft power policy instruments? What would your country prefer based on your foreign policy?

5) Would a new agreement (including new nuclear states) stand a chance of succes?

6) How significant will be the change in the US approach with the new administration?

7) What are the alternatives (if any) to the means of limiting nuclear proliferation we distinguish today?

8) How can establishing mutual trust between the nuclear states be revisited?

References

Afina, Y. and Caughley, T. (2020). NATO and the Frameworks of Nuclear Non-proliferation and Disarmament Challenges for the 10th NPT Review Conference. Retrieved from: https://www.chathamhouse.org/sites/default/files/2020-05-29-nato-npt-frameworks-caughley-afina-2.pdf (Last Access: January 7th, 2021).

Analytics Insight. (2019). Top 6 countries with the best cyber security measures. Retrieved from: https://www.analyticsinsight.net/top-6-countries-with-the-best-cyber-security-measures/ (Last Access: November 30th, 2020).

Andrews, E. (2019). Who Invented the Internet? History. Retrieved from: https://www.history.com/news/who-invented-the-internet (Last Access: November 19th, 2020).

Arms Control Association. (2019). The Post-INF Treaty Crisis: Background and Next Steps. The Arms Control Association. Retrieved from: https://www.armscontrol.org/issue-briefs/2019-08/post-inf-treaty-crisis-background-next-steps (Last Access: December 12th, 2020).

BBC. (2020). Amazon charged with abusing EU competition rules. The British Broadcasting Company. Retrieved from: https://www.bbc.com/news/business-54887650 (Last Access: November 26th, 2020).

BBC. (2018). Facebook's data-sharing deals exposed. The British Broadcasting Company. Retrieved from: https://www.bbc.com/news/technology-46618582 (Last Access: November 26th, 2020).

BBC. (2010). Statement by former Russian president mr. Medvedev. The British Broadcasting Company. Retrieved from: http://news.bbc.co.uk/2/hi/europe/8607985.stm (Last Access: December 12th, 2020).

Cambridge University Press. (s.a.). 2G. Retrieved from: https://dictionary.cambridge.org/dictionary/english/2g (Last Access: November 19th, 2020

Careers in cybersecurity. (2016). From the U.S. to Europe and Asia: Cybersecurity Policies Around the Globe. Retrieved from: https://careersincybersecurity.com/u-s-europe-asia-cybersecurity-policies-around-globe/ (Last Access: November 30th, 2020).

Charrie, A. and Quest, L. (2019). The Right Way to Regulate the Tech Industry. Sloan Review. Retrieved from: https://sloanreview.mit.edu/article/the-right-way-to-regulate-the-tech-industry/ (Last Access: December 2nd, 2020).

Chen, A. (2019). How to regulate Big Tech without breaking it up. Technology Review. Retrieved from: https://www.technologyreview.com/2019/06/07/135034/big-tech-monopoly-breakup-amazon-apple-facebook-google-regulation-policy/ (Last Access: December 2nd, 2020).

Council on Foreign Relations (n.d.). U.S.-Russia Nuclear Arms Control 1949 – 2019. Retrieved from: https://www.cfr.org/timeline/us-russia-nuclear-arms-control (Last Access: January 7th, 2021).

Cyber Security Review. (2020). Russian hackers use fake NATO training docs to breach govt networks. Retrieved from: https://www.cybersecurity-review.com/news-september-2020/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/ (Last Access: November 29th, 2020).

Dance, G. (2018). As Facebook Raised a Privacy Wall, It Carved an Opening for Tech Giants. The New York Times. Retrieved from: https://www.nytimes.com/2018/12/18/technology/facebook-privacy.html (Last Access: November 25th, 2020).

Davies, H. (2015). Ted Cruz using firm that harvested data on millions of unwitting Facebook users. The Guardian. Retrieved from: https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data (Last Access: November 27th, 2020).

DELL. Top 10 Steps To Help Stop Cybercrime. DELL Inc. Retrieved from: https://www.dell.com/downloads/ca/support/top_10_steps_to_protect_against_cybercrime_dell_en.pdf (Last Access: December 1st, 2020).

Durkalec, J. (2019). European security without the INF Treaty. Retrieved from: https://www.nato.int/docu/review/articles/2019/09/30/european-security-without-the-inf-treaty/index.html (Last Access: January 7th, 2021).

Ergun, F. D. (2018). Naional Security vs. Online Rights and Freedoms in Turkey: Moving Beyond the Dichotomy. The Centre for Economics and Foreign Policy Studies (EDAM). Retrieved from: https://edam.org.tr/en/national-security-vs-online-rights-and-freedoms-in-turkey-moving-beyond-the-dichotomy/ (Last Access: November 30th, 2020).

EURACTIV. (2016). Hungary anti-terror spy law breaches privacy: European rights court. Retrieved from: https://www.euractiv.com/section/justice-home-affairs/news/hungary-anti-terror-spy-law-breaches-privacy-european-rights-court/ (Last Access: November 30th, 2020).

European Commission. (2020). Antitrust: Commission sends Statement of Objections to Amazon for the use of non-public independent seller data and opens second investigation into its e-commerce business practices. Retrieved from: https://ec.europa.eu/commission/presscorner/detail/en/ip_20_2077 (Last Access: November 26th, 2020).

European Commission. (s.a.). What is a data breach and what do we have to do in case of a data breach? Retrieved from: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en (Last Access: November 21st, 2020).

European Court of Auditors. (2020). Special Report No 24/2020: The Commission's EU merger control and antitrust proceedings: a need to scale up market oversight. Retrieved from:

https://www.eca.europa.eu/en/Pages/DocItem.aspx?did=56835 (Last Access: November 27th, 2020).

Federal Trade Commission. (2020). Equifax Data Breach Settlement. Retrieved from: https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement (Last Access: November 21st, 2020).

Foroohar, R. (2019). Our personal data needs protecting from Big Tech. The Financial Times. Retrieved from: https://www.ft.com/content/04d3614e-078a-11ea-a984-fbbacad9e7dd (Last Access: December 2nd, 2020).

Granville, K. (2018). Facebook and Cambridge Analytica: What you need to know as fallout widens. The New York Times. Retrieved from: https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html?rref=collection%2Fsectioncollection%2Ftechnology&action=click&contentCollection=technology&region=stream&module=stream_unit&version=latest&contentPlacement=1&pgtype=sectionfront (Last Access: November 26th, 2020).

Guha, D. (2019). Cyber Crimes- Challenges & Solutions. Research Gate. Retrieved from: https://www.researchgate.net/publication/284398152_Cyber_Crimes-_Challenges_Solutions (Last Access: December 1st, 2020).

HM Government. (2015). National Cyber Security Strategy 2016-2021. The Government of the United Kingdom. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf (Last Access: November 30th, 2020).

Indiana University. (s.a.). What are cookies? Retrieved from: https://kb.iu.edu/d/agwm (Last Access: November 25th, 2020).

Irwin, L. (2020). The 6 most common ways data breaches occur. IT Governance. Retrieved from: https://www.itgovernance.eu/blog/en/the-6-most-common-ways-data-breaches-occur (Last Access: November 24th, 2020).

Jabbar, F.H. (2019). Countering the use of information and communications technologies for criminal purposes. The United Nations General Assembly. Retrieved from: https://www.undocs.org/A/74/401 (Last Access: November 29th, 2020).

Kimball, D.G. (2018). INF Termination Is Bad, but It Could Get Worse. The Arms Control Association. Retrieved from: https://www.armscontrol.org/act/2018-11/focus/inf-termination-bad-could-get-worse (Last Access: December 12th, 2020).

Kimball, G. (2019). A New Nuclear Deal Begins With New START. Retrieved from: https://www.armscontrol.org/act/2019-11/focus/new-nuclear-deal-begins-new-start (Last Access: January 7th, 2020).

Kirgis, F. (2003). North Korea's Withdrawal from the Nuclear Nonproliferation Treaty. Retrieved from: https://www.asil.org/insights/volume/8/issue/2/north-koreas-withdrawal-nuclear-nonproliferation-treaty (Last Access: january 7th, 2021).

Lemmens, K. (2020). Europese Commissie holt achter big tech aan. De Standaard. Retrieved from: https://www.standaard.be/cnt/dmf20201119_98120262 Last Access: November 27th, 2020).

Madrigal, A.C. (2018). Facebook didn't sell your data; It gave it away. The Atlantic. Retrieved from: https://www.theatlantic.com/technology/archive/2018/12/facebooks-failures-and-also-its-problems-leaking-data/578599/ (Last Access: November 25th, 2020).

Madrigal, A. C. (2018). What took Facebook so long? The Atlantic. Retrieved from: https://www.theatlantic.com/technology/archive/2018/03/facebook-cambridge-analytica/555866/ (Last Access: November 27th, 2020).

Matthaiou, A. and Vermulst, E. (2020). Crossing the line from regulation to discrimination: the draft Polish National Cybersecurity Act as a protectionist step in the 5G race (Part 1). Regulating for Globalization. Retrieved from: http://regulatingforglobalization.com/2020/09/17/crossing-the-line-from-regulation-to-discrimination-the-draft-polish-national-cybersecurity-act-as-a-protectionist-step-in-the-5g-race-part-1/ (Last Access: November 30th, 2020).

McNamee, R. (2020). Big Tech Needs to Be Regulated. Here Are 4 Ways to Curb Disinformation and Protect Our Privacy. Time Magazine. Retrieved from: https://time.com/5872868/big-tech-regulated-here-is-4-ways/ (Last Access: December 2nd, 2020).

Microsoft Corporation. (2018). About the cybersecurity tech accord. Retrieved from: https://cybertechaccord.org/about/ (Last Access: November 20th, 2020).

NATO. (2010). Active Engagement modern defence: strategic concept fort he Defence and Security of the members of the North Atlantic Treaty Organization, §19.

NATO. (2014). Wales Summit Declaration. The North Atlantic Treaty Organisation. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_112964.htm#cyber (Last Access: November 27th, 2020).

NATO. (2016). NATO Cyber Defence Fact Sheet July 2016. The North Atlantic Treaty Organisation. Retrieved from: https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-cyber-defence-eng.pdf (Last Access: November 27th, 2020).

NATO. (2016). Signing of Memorandum of Understanding on Cyber Defence. The North Atlantic Treaty Organisation. Retrieved from: https://www.nato.int/cps/en/natohq/photos_136551.html (Last Access: November 27th, 2020).

NATO. (2016). Warsaw Summit Communiqué. The North Atlantic Treaty Organisation. Retrieved from: https://www.nato.int/cps/en/natohq/official_texts_133169.htm (Last Access: November 27th, 2020).

NATO. (2019). NATO Cyber Defence Fact Sheet February 2019. The North Atlantic Treaty Organisation. Retrieved from:

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf (Last Access: November 27th, 2020).

Press, G. (2015). A Very Short History of Digitization. Forbes. Retrieved from: https://www.forbes.com/sites/gilpress/2015/12/27/a-very-short-history-of-digitization/?sh=70eb1f0f49ac (Last Access: November 19th, 2020).

Podvig, P., Snyder, R. and Wan, W. (2019).Evidence of absence: Verifying the removal of nuclear weapons. The United Nations. Retrieved from: https://www.unidir.org/files/publications/pdfs/evidence-of-absence-verifying-the-removal-of-nuclear-weapons-en-722.pdf (Last Access: December 12th, 2020).

Radio Free Europe / Radio Liberty (2019). U.S. Concerned Russia-Backed UN Resolution Will Hurt Online Freedom. Retrieved from: https://www.rferl.org/a/us-russia-internet-un/30335318.html (Last Access: January 7th, 2021).

Reuters Staff. (2020). EU planning tougher regulation for 'hit list' of big tech firms. Reuters. Retrieved from: https://uk.reuters.com/article/us-eu-tech-idUKKBN26W0XV (Last Access: November 21st, 2020).

Ramsey, D. (2019). How a Data Breach Can Impact You. DaveRamsey. Retrieved from: https://www.daveramsey.com/blog/data-breach-impacts (Last Access: November 24th, 2020).

Saljic, E. and Tusko, D. (2018). Cybersecurity Policies of East European Countries. Research Gate. https://www.researchgate.net/publication/325196481_Cybersecurity_Policies_of_East_European_Countries (Last Access: November 30th, 2020).

Sandbu, M. (2019). The Economics of Big Tech. The Financial Times. Retrieved from: https://www.ft.com/economics-of-big-tech (Last Access: November 19th, 2020).

Sharma, A. (2020). Russian hackers use fake NATO training documents to breach government networks. Bleeping Computer. Retrieved from: https://www.bleepingcomputer.com/news/security/russian-hackers-use-fake-nato-training-docs-to-breach-govt-networks/ (Last Access: November 29th, 2020).

Stolton, S. (2019). UN backing of controversial cybercrime treaty raises suspicions. EURACTIV. Retrieved from: https://www.euractiv.com/section/digital/news/un-backing-of-controversial-cybercrime-treaty-raises-suspicions/ (Last Access: November 20th, 2020).

The White House. (2010). Readout of the president's call with Russian President Medvedev. Obama's White House. Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/readout-presidents-call-with-russian-president-medvedev-0 (Last Access: December 12th, 2020).

The White House. (2016). FACT SHEET: Cybersecurity National Action Plan. Retrieved from: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (Last Access: November 30th, 2020).

UNICWASH. (2019). Taking action where we can to stop cybercrime. Retrieved from: https://unicwash.org/oped-cybercrime/ (Last Access: December 1st, 2020).

United Nations. (s.a.). Nuclear Weapons. The United Nations. Retrieved from: https://www.un.org/disarmament/wmd/nuclear/ (Last Access: December 12th, 2020).

United Nations. (1946). Resolutions adopted on the reports of the first committee. The United Nations. Retrieved from: https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/1(I) (Last Access: December 12th, 2020).

United Nations. (2017). Securing our common future: An Agenda for Disarmament. The United Nations. Retrieved from: https://s3.amazonaws.com/unoda-web/wp-content/uploads/2018/06/sg-disarmament-agenda-pubs-page.pdf#view=Fit (Last Access: December 12th, 2020).

The United Nations Office on Drugs and Crime (UNODC) (2010). Asia Pacific Regional Workshop on Fighting Cybercrime.. Retrieved from: https://www.unodc.org/documents/southeastasiaandpacific/2011/09/cybercrime-workshop/ppt/SYMC_UNODC_ITU_Cybercrime_Workshop.pdf (Last Access: December 1st, 2020).

U.S. Department of State (n. d.). *New START Treaty.* Retrieved from: https://www.state.gov/new-start/ (Last Access: January 7th, 2021).

Weir, F. (2011). With Russian ratificiation of new START, what's next for US-Russia relations? CS Monitor. Retrieved from: https://www.csmonitor.com/World/Europe/2011/0126/With-Russian-ratification-of-New-START-what-s-next-for-US-Russia-relations_ Last Access: December 12th, 2020).

Yun Chee, F. (2020). Europe charges Amazon with using dominance and data to squeeze rivals. Reuters. Retrieved from: https://www.reuters.com/article/us-eu-amazon-com-antitrust/europe-charges-amazon-with-using-its-dominance-and-data-to-squeeze-rivals-idUSKBN27Q18E (Last Access: November 26th, 2020).

PragueMUN2021

©MUN Prague. 2021. All rights reserved.