TOPIC GUIDES
PIMUN 2018

The European Council

Table of Contents

INTRODUCTION LETTERS

Dear Delegates,

My name is Dimitra and I am honoured to serve as one of your chairs for this year's PIMUN Council of the EU Committee. I am Greek and currently I am doing my LLM in Human Rights at Cardiff University and pursuing to finish my degree at Public Administration at Panteion University of Athens at the same time. Having been involved in the MUN circuit of England for 4 years, I have participated in many conferences as a Delegate, Chair and even Secretariat Member in many different countries of Europe. Though, this is my first ever PIMUN.

In our committee we will discuss two very crucial contemporary topics that the European Union has to deal with, under the general theme "Europe of Defence". The first one is "European strategy on cybersecurity" and the second one is "Coordinating and managing military budgets".

In this study guide you will find the most fundamental relevant information about the background of the topic and it will be a good starting topic for your research, so you are kindly requested to read it. You should not limit your research to this study guide. As this is an advanced committee you are expected to conduct your own research too.

I look forward to meeting all of you in March,

Dimitra

Greetings delegates and welcome at PIMUN 2018!

My name is Clémence Albert-Lebrun, and I will be chairing the council of the EU at PIMUN 2018!

I am a second-year economics student at the university Paris Dauphine International, London campus. I am originally from Versailles, France. I have had an interest in social sciences and politics for as long as I can remember which is why I am very enthusiastic about everything MUN related!

I have been doing MUN for 5 years, both at a high school and university level. This is my second PIMUN conference, and my 11th conference overall. I hope to see some fruitful and passionate debate on both our two very interesting topics! We will make sure you all have the best experience possible.

I very much look forward to meeting you all in May!

Best

Clémence Albert-Lebrun

Introduction to the Committee

The European Council

The European Council is an EU body responsible for defining the EU's overall political direction and priorities and set the political agenda. It meets at least once every six months and is comprised of one representative from each EU government. The decisions it takes are to be voted on consensus, except for certain policies such as common defence.

It was created in 1947 as an informal forum for discussion between heads of state or government of the EU member states. In 1992 the treaty of Maastricht formalised it as the body providing the general political guidelines for the EU, and the Lisbon Treaty made it one of the 7 EU Institutions.

The European Council's goals are to protect the values and objectives of the EU as a whole, and to guide measures and initiatives in the interest of all Member States.

This body must not be confused with the Council of the EU, which is a legislative organ of the EU, or the Council of Europe, which is not an EU body.

EU Summit, meeting of the European Council, 2016

<http://hum.port.ac.uk/europeanstudieshub/learning/module-1-understanding-eu-institutions/the-european-council/the-meetings-of-the-european-council/>

The history of the European Council

- 1961 **first 'European Summit'**: meeting of Heads of State or Government of the Union's Member States in Paris

- **1974 Paris European Summit**: decided that these meetings would be held on a regular basis under the name 'European Council' (EC); these meetings would aim to define a general approach to the problems of European integration and coordination

- **1986 Single European Act**: included the EC in the body of the Community Treaties, defining its composition and providing for bi-annual meetings; the Act aimed to reform the Union's institutions in preparation for Portugal and Spain's membership and speed up decision-making in preparation for the single market

- **1992 Treaty of Maastricht**: formalised the EC's role in the European Union's institutional process

- **2009 Treaty of Lisbon:** made the EC a full institution of the EU (article 13 TEU), defined its role as to 'provide the Union with the necessary impetus for its development and define the general political directions and priorities thereof' (article 15 TEU).

Topic A: Managing and coordinating military budgets

Introduction

According to NATO, the EU's current strategy on defence is "financially inefficient, politically fragmented and strategically incoherent". It could in fact be considered that this particular area of European integration needs improvement in order to maximise both efficiency and security.

Through different institutions and agencies, the European Union has a general policy on security and defence which applies to all Member States. The Common Security and Defence Policy (CSDP) is the framework used by the EU to secure their defence policy both within the continent and abroad, mostly on peace keeping missions and, more generally, to strengthen international security. The European Defence Agency is part of this framework and aims to facilitate the implementation of measures taken by Member States. The latter stay nonetheless very independent. The EU defence policies are unanimously decided by the European Council, meaning it cannot go against national policies or interests. There are however a mutual defence clause and a legal obligation to implement the CSDP. EU countries vote on their defence budgets individually, but efforts to encourage coordination in the interest of efficiency have been made in the past. European citizens realise that modern threats transcend borders, and that the EU as an institution has the potential to provide a more complete and viable protection. 75% of EU citizens have thus declared themselves in favour of a European coordinated defence policy.

The issue of budget coordination is particularly divisive amongst EU leaders. This division undermines the efforts for cooperation, as was seen for the 2017 proposal for a European Defence Fund. This focused mostly on the development of the defence industry and an economic aspect, a less controversial side, more than actually coordinating the national budgets and creating a multifunctional fund. The challenges faced by the EU countries in trying to coordinate are numerous and multi-faceted. With 28 current Member States, the divergence in policy between major powers is a problem. Overall, the same threats are omnipresent in all EU countries, which include terrorism and cybercrime; therefore, it is arguable that coordinating budgets would make the overall response more efficient. However, countries have different policies on conflicts, diplomatic incidents and threats, both internal and external to Europe, and different priorities. This explains why keeping their sovereignty on military budgets is so important to some. Indeed, coordination would imply a consensus on which country gives what amount, how this amount is calculated, whether this should be voluntary or mandatory, and where and how to manage and allocate that budget.

This is particularly problematic due to disparities in budgets and GDP/capita within the EU. A lack of coordination therefore implies that countries are not equally protected, and in a context such as the migrant crisis this is a problem.

In trying to find a solution one should take into account what the EU considers its role to be, the scope of its past actions and the interests of its individual members. Countries are more or less willing to be involved in different conflicts, so a compromise must be found between national sovereignty and the benefits of an increasingly involved EU in how national armies are allocated, managed and funded. Indeed, the question of whether the EU strives towards military integration remains at hand.

European Defence, by Paresh Nath, November 2017
<https://www.caglecartoons.com/viewimage.asp?ID={4C355A9C-F9FC-40FA-B06F-71006FCB37A7}>

Part A: Timeline of the topic

December 1991: The European Council creates a Common Foreign Security Policy (CFSP) and the beginning of a common defence policy

June 1999: Launch of the European Security and Defence Policy (ESDP) in Cologne to reinforce the CFSP

December 2002: 'Berlin Plus' arrangement allows the use of NATO structures, mechanisms and assets to implement ESDP missions

December 2003: Brussel Summit adopts a European Security Strategy to improve European security, identify threats they could be facing, define their strategic objectives and set out the political implications

July 2004: Creation of the European Defence Agency (EDA) to sustain the ESDP and improve crisis management

December 2009: Treaty of Lisbon after which the Common Security and Defence Policy (CSDP) replace the ESDP, thereby creating the European External Action Service

December 2013: Priority actions were defined for stronger cooperation, which included increasing effectiveness, visibility and impact of the CSDP, enhancing the development of capabilities and strengthening Europe's defence industry

June 2016: Creation of the EU Global Strategy

July 2016: EU-NATO joint declaration at the NATO Summit in Warsaw, both parties acknowledged the increasingly threatening challenges faced by Europe from the East and the South

November 2016: Creation of the European Defence Fund to encourage and support efficient spending on joint defence capabilities, measures to strengthen security and industrial base

December 2016: 40 proposals endorsed by the EU Council aiming to implement the EU-NATO joint declaration

May 2017: Meeting on potential improvements of the EU Global Strategy, new focus on crisis management structures, capacity building, civilian crisis management, and deepening European defence cooperation

5 December 2017: New proposals for more EU-NATO cooperation with a focus on counter-terrorism, women, peace and security, and military mobility

17 December 2017: Establishment of the Permanent Structured Cooperation (PESCO) signed by 25 Member States, which exclude Malta, the United Kingdom and Denmark

6 March 2018: Roadmap of PESCO

EU leaders at the negotiations of PESCO, <https://www.euractiv.com/section/defence-policy/news/bad-news-for-enemies-eu-leaders-officially-launch-defence-pact/>

Part B: Discussion

The Common Security Defense Policy

The primary focus should be understanding the outline of the CSDP as the framework for the specific EU defence policies.

The CSDP was created in 2009 by the Treaty of Lisbon and replaces and enlarges the ESDP. This change mostly allowed willing Member States to enhance military efforts with each other, within EU framework of course. It also emphasised the need to improve common European defence capacity building.

Common Security and Defence Policy <https://tvnewsroom.consilium.europa.eu/event/common-security-and-defence-policy-d3c7>

The goals of this policy are both simple and very large. During and after the Cold War and the conflicts in the Balkans, the EU was in need of a legitimate military force, crisis management capabilities and conflict prevention skills. The general aim remained peace keeping, cooperation and coordination, but also included the establishment of a strong Europe, with the image of a stable continent capable of defence. The specific goals were outlined throughout the years by the different treaties, conventions and summits held on the EU's defence policies, such as the 'Berlin Plus' arrangement or the creation of the 'High Representative for Common Foreign and Security Policy'.

The CSDP's course of action is fairly straight-forward. EU countries must provide civilian capabilities and military equipment to the EU to implement the CSDP. All actions are to be decided unanimously, in accordance with the mutual defence clause and the respect for certain Member States' obligations to abide to NATO rules. The CSDP mainly takes on humanitarian and rescuing missions, conflict prevention missions, the combat of forces in crisis management situations, joint disarmament, military advice, and/or post-conflict stabilisation. However, because actions are to be unanimously decided upon, these tasks are often delegated to voluntary EU countries. Therefore, ambiguity remains on the types of operations the EU as a whole can undertake. National countries can take initiatives, possibly with other Member States, and NATO can be a medium to take on some missions.

Within the CSDP many key institutions impact the EU's defence policy and its potential coordination. The European Defence Agency (EDA) for example supports and guides national initiatives by setting common EU objectives in terms of military capacity. It can introduce and manage programmes to achieve these objectives. It

has the mandate to harmonise EU countries' operational needs by encouraging maximum 'pooling and sharing' of military resources. Its goal is to strengthen the EU's industrial and technological base and help make military expenditure, or national defence budgets, more effective.

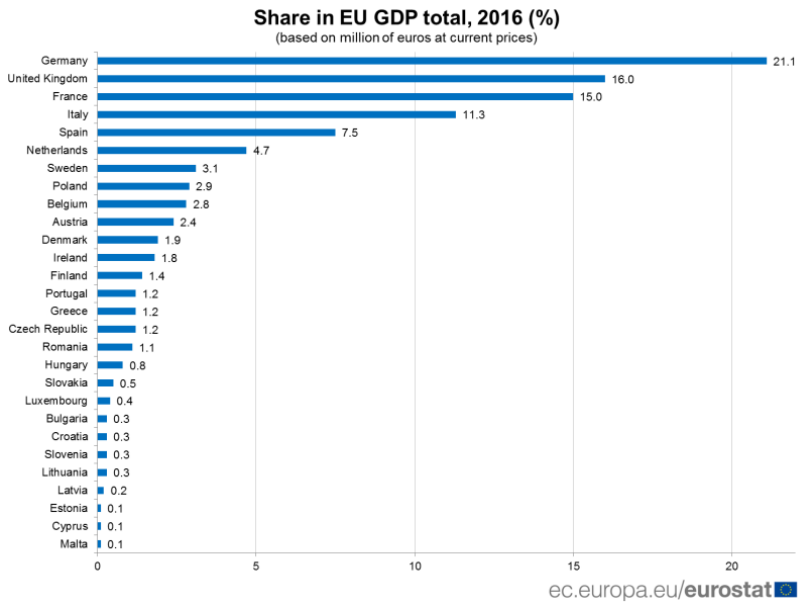
The Permanent Structured Cooperation in defence (PSCD), as defined by the Lisbon Treaty, targets the commitment of EU countries to develop their defence capabilities and supply combat units for CSDP missions. These contributions are further assessed by the EDA.

The CSDP is complex and ambiguous. It lacks efficiency and a united stance on certain issues, which means before a coordinated budget there is a need for a more coordinated and straight forward EU defence policy.

The impact of disparities within the EU on military budgets

Significant disparities remain between EU Member States. The need to coordinate and harmonise expenditure related to the military is urgent. The amounts invested nationally are very unequal.

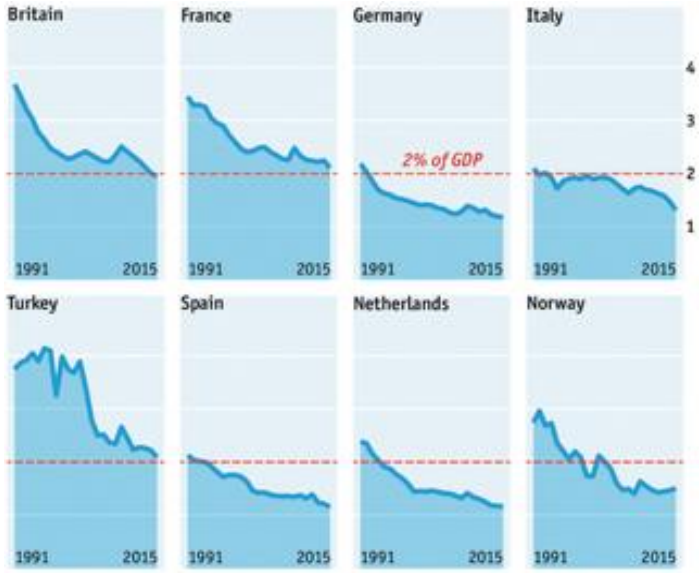
Economic disparities notably can have a direct impact on the harmonisation of defence policy and can lead to conflictual differences. According to an OECD report, the 2008 economic crisis' consequences are still being felt today. Income inequality, within the EU and internally in Member States, has not returned to pre-2008 lows. There are also non-negligible gaps in life expectancies, health statuses, and unemployment depending on age, origin and gender. These disparities are reflected in the distribution of the EU's GDP, as can be seen in the graph below.



Share in EU GDP Total, 2016 (%)
<http://ec.europa.eu/eurostat/web/products-eurostat-news/-/DDN-20170410-1>

Considering these differences in GDP, it makes sense to assume that there would be major differences in military budgets as well. These differences however are very much surprising. Because of geopolitical events such as the migrant crisis, countries like Greece have a very high defence budget compared to others, despite most having a higher GDP.

In 2014 France spent 592€/capita on defence, or 1.83% of its GDP. The UK spent 747€/capita, or 2.17% of its GDP. These two countries have the biggest defence spending in the EU, which is apparent when compared with countries like Czech Republic (142€/capita or 0.96% of its GDP). In 2015, Germany and Latvia spent the same percentage of their GDP on defence, which represented about 1%, despite a significant difference in their nominal GDP.



Military as a % of GDP from 1991 to 2015 <https://www.nextbigfuture.com/2017/07/canada-and-some-other-nato-countries-plan-to-increase-defense-spending.html>

European countries are highly divided on the issue of military intervention. For example, in Germany, Angela Merkel practiced a policy of constraint, but Germany's defence minister and President called for stronger involvement and a worthy European defence policy to support France in its foreign military aid initiatives. On the other hand, the UK and France have been reluctant to delegate control over their respective militaries.

Beyond these divisions, there are simple differences of opinion. There are multiple ways to allocate funds, and various valid receivers of these funds. Some examples include research and development, weapon production, and peacekeeping operations, but not all countries agree on which to prioritise.

Budgets allocated to domestic and foreign defence

There is a discussion possible on which aspects of European defence can plausibly be coordinated amongst Member States. Beyond the debate on who gives, who allocates and where, defence policy can be separated into sections, some more controversial than others.

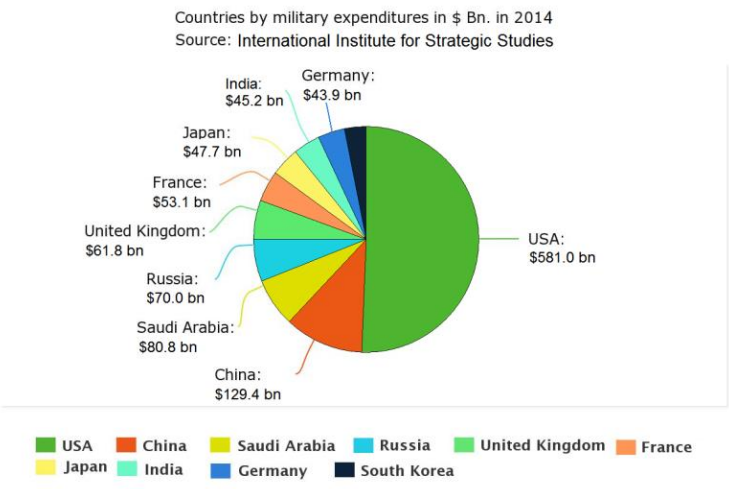
Firstly, domestic defence policies are designed to tackle internal threats. As stated before, a number of threats are common to EU countries, and all have to combat them, more or less intensively. One of the most obvious examples is terrorism. After terror attacks in Paris, London, Brussels, Stockholm, Manchester, Barcelona,

Berlin, Nice and others, no EU country can pretend to be safe. This can explain why counter terrorism has been put as a priority, notably at the 2017 EU-NATO Summit. Climate change is another common threat against which a single country is powerless. Coordination and EU-led initiatives are the most efficient responses. More controversially, the migrant crisis has been the most challenging threat to EU stability in recent years. Because of political differences, it is extremely difficult and onerous to reach a consensus on what to do and where to allocate a potential budget. Considering previous points on countries' GDP and economic disparities, there is an urge for a united front and coordinated policies, financially, politically and militarily. Geographically Greece, Italy and Hungary are at a disadvantage, which imposes a further financial, political and logistical constraint in the context of this particular crisis.

It is arguable that an EU-coordinated policy on internal threats is beneficial and increases efficiency; however, this is not necessarily true for external military actions. Countries like the UK and France have expressed concerns of loss of national sovereignty if the EU was given more responsibilities in the management of national military budgets on missions outside of the European continent.

Challenges

To illustrate how national policies and interests can be a challenge in coordinating military budgets, the example of national intervention in the Middle East can be quite revealing. France has been quite present, with troops on ground and multiple air strikes against Da'esh, and a very violent denunciation of the Bashar el Assad regime. They moreover have an influence in Northern Africa, where they target Al-Qaeda and Boko Haram. Overall in recent years not only have they been physically present in conflict zones, they have also increased their military defence budgets to support operations within France and in said unstable regions. In comparison, Germany's stance in the region has been surprisingly subtle, with very little military intervention and a focus on economic interests, refugees and arms sales. Considering the gap between these two military and political choices, the challenge of an EU budget on military intervention in unstable regions becomes apparent. France has been pushing Germany to spend more on such efforts, but this has only been partially heard.



Furthermore, beyond the choice given to each country on their military stance, the issue of sovereignty remains a challenge. Should the EU impose a maximum or minimum budget/country allocated to defence? Should the EU be in charge of managing this budget? Should there be a coordination regarding how the budgets are spent? If yes, who should get to decide?

<https://upload.wikimedia.org/wikipedia/commons/b/b6/Top_ten_military_expenditures_in_US%24_Bn._in_2014%2C_according_to_the_International_Institute_for_Strategic_Studies.PNG>

It is all the more important to start a serious coordination of EU budgets and military initiatives considering the emergence of new global powers and the disengagement of the US military. Indeed, the US previously supported the EU in their initiatives, allowing them to branch out. Without them, and with countries like China and India with an increasing economic influence potentially convertible to military power, the EU's place in international military politics could be compromised.

The future: improvement and innovation

In dealing with the lack of coordination, considering both the limitations of current solutions and coming up with new ones is important.

The Common Security and Defence Policy is highly criticised for its inefficiency and passiveness. Such critics argue that, ever since the Treaty of Lisbon, nothing concrete has been implemented, giving the impression that the policy is altogether a waste of time and money. Although this point of view is not the majority's, and quite a reductive evaluation of the policy, certain limitations of the CSDP could be improved. This framework is firstly dependent on political will. The lack of concrete results can indeed be explained by the fact that in the EU, projects can be initiated by the High Representative; however, this is rarely the case. Most are proposed by individual countries, and so require others to stand behind them. The success of such operations is often jeopardised by a sloppy commitment, and a lack of resources allocated to them. Moreover, the EU has been criticised for its inability to run operations efficiently. Despite improvements in analysis, decision making, planning and running military and civilian operations, the EU remains largely unexperienced and dependent on NATO and the US.

A new defence plan has been proposed late November 2017, which includes an investment fund for defence spending, notably on military hardware at a lower cost, and research. Moreover, it has been proposed that in the interest of saving money, joint military training programmes are put in place. Finally, the idea of a European Peace Facility has been put forward to equip the EU with means and resources to live up to its ambitions.

Part C: Bloc Positions

NATO

NATO and the EU share interests, values, members, and have faced similar challenges. Out of the 29 members of NATO, 22 are part of the EU. In this sense NATO-EU cooperation is both inevitable and completely logical.

Within NATO, budgets are also a divisive issue. Only Poland, the US, Greece, Estonia and the UK currently meet the 2% of GDP target set by NATO as a goal for military expenditure. The general goals of an EU-NATO partnership for NATO are to fully strengthen the strategic partnership, "in the spirit of full mutual openness, transparency, complementarity and respect for the autonomy and institutional integrity of both organisations", to improve all practical aspects in crisis operations, to enlarge the diplomatic and political partnership, to broaden the understanding and analytical skills of both organisations through more communication, and to minimise costs through such partnerships.

The US

As the biggest contributor, President Trump has questioned the US involvement in NATO. This was a response to what he saw as a lack of commitment from EU countries due to their inability to meet the 2% goal. He suggested that the US could step away from their current position, which would completely delegitimise the organisation. As the UK leaves the EU, France becomes the bloc's main military power, which increases the constraints on its promises to the US. Considering the US's demands, France may find it difficult to fulfil them and may need more EU support. The main goal would be for tensions not to escalate as the US warns the EU not to take their economic and military cooperation for granted. A diminished EU-US military cooperation could only jeopardise the safety of EU citizens.

The UK

Because of Brexit, the UK finds itself in an unprecedented position. The country currently contributes to the CSPD through the EU budget but is not a particularly significant contributor compared to its capacities and resources. The UK has previously hindered cooperation and military integration within the block. Indeed, it fought against an increase of the EDA budget, and vetoed the creation of a single military headquarters in Brussels. Brexit may therefore mean that further military integration can be implemented, but it would be in the interest of both the UK and the EU for security and defence policy to be mentioned in a post-Brexit deal.

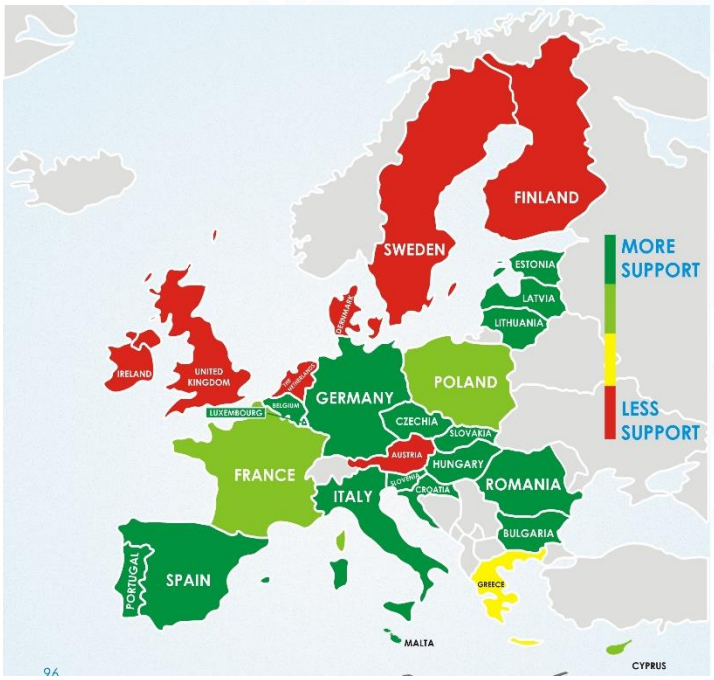
France:

European integration being a key point in his presidential campaign, French President Emmanuel Macron has repeatedly expressed his wish for a stronger European defence policy. He has proposed, amongst other things, a shared defence budget, a European military intervention force, and more generally a common strategic culture. He believes this would legitimise the EU's image of a united group internationally, a goal France is striving for.

Germany:

Germany supports France in most of its discourse and has taken increasingly more proactive measures. It is however somewhat held back by a "political culture of reserve". Indeed, according to The Economist, "across all aspects of Germany's foreign policy, the country is beginning to give up its cautious traditional doctrines, but much more slowly than many of its allies would like".

The EU in general:



Debates around PESCO, and the vote on European integration in defence policy, have revealed the gap in commitment within the Union. This map shows the support by the Members of Parliament for more EU integration in defence policy, by country.

E. Chitul, D. Frantescu, What chances for a real European Common Security and Defence Policy,

<http://www.dialogue-advisors.com/what-chances-for-a-real-european-common-security-and-defense-policy/>

Conclusion

Managing and coordinating military budgets within the EU is becoming urgent as the bloc faces a number of threats. Along with the risk of external conflicts, such as the crisis in the Middle East, and internal threats such as climate change, terrorism and a complex migration crisis, the CSDP's inefficiency may cause the EU to lose some of its international influence to emerging actors such as China or India. It is moreover threatening its relations with the US.

Managing budgets is controversial due to a national will to maintain sovereignty, combined with a need for coordination to fight against the challenges mentioned above. The CSDP and other solutions proposed have achieved a level of integration, but the threats remain, and diplomatic complications continue to threaten the continent.

The main obstacle to European Integration remains the difficulty to compromise. The extent to which a military integration would be beneficial must be discussed. Furthermore, without regard to the degree of integration agreed upon, consensus must be reached on military budgets allocated to EU-led missions, and the specifics of said budgets and missions. A lack of accuracy and precision would significantly jeopardise their potential success. Aspects which should be considered include, but should not be limited to, how to decide the amount given, which country gives what amount, which country or body is responsible of said amount, how it is allocated and where.

PIMUN

Bibliography

S. Soesanto, *NATO Review*, Europe needs less soldiers – but more European ones <https://www.nato.int/docu/review/2015/Also-in-2015/europe-defense-budget-military-soldiers/EN/index.htm>

Eurostat, How much is spent on defence in the EU?, 7 June 2017 <http://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20170607-1>

Eurostat, Government expenditure on defence, 7 June 2017 <http://ec.europa.eu/eurostat/statistics-explained/index.php/Government_expenditure_on_defence#Evolution_of_.27defence.27_expenditure_over_2002-2015>

R. Neukirch, G Repinski, *Spiegel Online*, Germany weighs stronger military role, January 2014 <http://www.spiegel.de/international/germany/germany-considers-increasing-role-in-foreign-military-missions-a-945771.html>

European Union External Action, The Common Security and Defence policy <https://eeas.europa.eu/topics/common-security-and-defence-policy-csdp_en?page=1>

European Union External Action, Time for EU to be bold. Mogherini outlines elements of "real work" to start now on EU security and defence, December 2017 <https://eeas.europa.eu/headquarters/headquarters-homepage/37504/time-eu-be-bold-mogherini-outlines-elements-real-work-start-now-eu-security-and-defence_en>

Department of Foreign Affairs and Trade, Common Security and Defence Policy, <https://www.dfa.ie/our-role-policies/international-priorities/peace-and-security/common-security-and-defence-policy/#>

Eur-Lex, The EU's Common Security and Defence Policy, 16 September 2015 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Aai0026>

R. Emmott, *Business Insider*, EU Countries agree to create a European mega-army, 13 November 2017 <http://www.businessinsider.com/eu-countries-agree-mega-army-2017-11>

European Council, Timeline: EU Cooperation on Security and Defence, 9 March 2018 <http://www.consilium.europa.eu/en/policies/defence-security/defence-security-timeline/>

European Commission, European Defence Fund and EU Defence Industrial Programme, <https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-294_en>

S. Biscop, *Diploweb, La Revue Géopolitique*, From ESPD to CSPD: Time for some strategy, January 2010 <https://www.diploweb.com/From-ESDP-to-CSDP-Time-for-some.html>

OECD, Understanding the socio-economic divide in Europe, January 2017 <https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiindm6kP3ZAhWBA8AKHSr-DYQQFggsMAA&url=https%3A%2F%2Fwww.oecd.org%2Fels%2Fsoc%2Fcope-divide-europe-2017-background-report.pdf&usg=AOvVaw0lJRZNVlo6ae-DGpERW8FQ>

BBC News, How is the migrant crisis dividing EU countries? , March 2016 <http://www.bbc.co.uk/news/world-europe-34278886>

Alice Foster, *The Express*, Terror attacks timeline: From Paris and Brussels terror to most recent attacks in Europe, 18 August 2017
<https://www.express.co.uk/news/world/693421/Terror-attacks-timeline-France-Brussels-Europe-ISIS-killings-Germany-dates-terrorism>

D. Wagner & G. Cafiero, *The Huffington Post*, Germany's Arms Sales and the Middle East,
<https://www.huffingtonpost.com/daniel-wagner/germanys-arms-sales-and-t_b_3803403.html>

D. A. Graham, *The Atlantic*, What is France doing in Syria? , 15 November 2015
<https://www.theatlantic.com/international/archive/2015/11/france-syria-iraq-isis/416013/>

T. Tardy, CSDP In Action: what contribution to international security? , May 2015
<https://www.iss.europa.eu/sites/default/files/EUISSFiles/Chaillot_134_CSDP_missions.pdf>

TOPIC B: European Strategy on Cybersecurity

Introduction

Cybersecurity is often neglected when discussing the topic of defence. It is however becoming an increasingly significant threat to individuals, companies, governments and the EU as a whole, as is shown by the attack on the NHS (National Health System of the UK) last year. Both the UN and the EU recognise the necessity to coordinate cybersecurity policies globally and regionally. Indeed, the EU is quite homogenous in its position on cybercrime, and therefore eliminating obstacles towards a common policy is within reach. These obstacles include cultural and political differences on internet governance, control and freedom, on which it is paramount to find a compromise. This governance is a new challenge which the EU faces. As a leader in technological advancements and research and development, it can be considered that it is their duty to protect EU citizens from these threats.

The most basic threats which should be mentioned and tackled include phishing (usurping the identity of an individual or a company to trick someone into giving their personal information, such as credit card information), hacking, bots (robots used by hackers to find software weaknesses), non-compliance with cybersecurity policy, and efficient recovery planning after an attack.

Despite the relative homogeneity between EU countries, disparities remain. These are obvious in the Global Cybersecurity Index, published by the International Telecommunication Union. According to this index, France and Austria for example are leading countries in terms of cybersecurity policy, whereas Spain, Germany and Bulgaria are in the maturing stage. This index is particularly useful as it outlines the different factors taken into account when evaluating a country, which indicates what a country can learn and from whom.

It must be outlined that technology has had a very positive impact on people's quality of life, especially in the EU. Internet governance and dealing with cybersecurity should therefore consider the balance between these advantages and the threat. The policy resulting from the debate should be flexible and focus on prevention, as well as harmonisation on investment in research and development and innovation in the relevant industries.

PART A: History of the topic

a) Existing legislation by the EU

Directive on Network and Information Security (NIS Directive)

It was proposed by the Commission in 2013, with aim to ensure a high common level of cybersecurity in the EU. European Parliament, Council and the Commission reached an agreement on its text on 7 December 2015. It was adopted by the European Parliament on July 2016 and came into force on August 2016. It has three main pillars:

- ensuring Member States preparedness by requiring them to be appropriately equipped, e.g. via a Computer Security Incident Response Team (CSIRT) and a competent national NIS authority;
- ensuring cooperation among all the Member States, by setting up a 'Cooperation Group', in order to support and facilitate strategic cooperation and the exchange of information among Member States, and a 'CSIRT Network', in order to promote swift and effective operational cooperation on specific cybersecurity incidents and sharing information about risks;
- ensuring a culture of security across sectors which are vital for our economy and society and moreover rely heavily on information and communications technologies (ICT).

Directive on attacks against information systems

It has the aim to combat large-scale cyber-attacks by *requiring Member States to strengthen national cybercrime laws and introduce tougher criminal sanctions*. This Directive had to be implemented by Member States by September 2015 and the Commission is currently checking implementation. Five infringement procedures for partial or non-communication have been launched in December 2015.

Directive on combating the sexual exploitation of children online and child pornography

It has the aim to address new developments in the online environment, such as grooming (offenders posing as children to lure minors for the purpose of sexual abuse). This legislation had to be transposed by 2013, and the Commission is currently verifying implementation. Two reports on implementation were issued at the end of 2016.

Framework decision on combating fraud and counterfeiting of non-cash means of payment

It defines the fraudulent behaviours that EU States need to consider as punishable criminal offences. The Commission is assessing the need to revise this Framework Decision to cover new forms of money transmissions like virtual currencies and other aspects, with a plan to come forward with any new initiative for the first quarter of 2017.

b) The main EU strategies on Cybersecurity

EU cybersecurity Strategy (2013)

The EU cybersecurity strategy was introduced by the Commission and the European External Action Service in 2013. It sets out the top five priorities for the EU in order to achieve online security. Those are:

- increasing cyber resilience
- drastically reducing cybercrime
- developing EU cyber defence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- developing the industrial and technological resources for cybersecurity
- establishing a coherent international cyberspace policy for the EU and promote core EU values

European Agenda on Security (2015)

This agenda, that was adopted by the Commission in 2015 sets as one of its top priorities the fight against cybercrime, coordinated in a European Level. This can be achieved by:

- implementing existing policies on cybersecurity, attacks against information systems, and combating child sexual exploitation
- reviewing and possibly extending legislation on combatting fraud and counterfeiting of non-cash means of payments to take account of newer forms of crime and counterfeiting in financial instruments, with proposals in 2016
- reviewing obstacles to criminal investigations on cybercrime, notably on issues of competent jurisdiction and rules on access to evidence and information
- enhancing cyber capacity building action under external assistance instruments.

Communication on Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (2016)

This strategy was adopted by the Commission in July 2016. Its main pillars are the following:

- Stepping up cooperation across Europe.
- Supporting the emerging single market for cybersecurity products and services in the EU
- Establishing a contractual public-private partnership (PPP) with industry

PART B: Discussion

Why is cybersecurity crucial?

During the last decades, most of the economic activities are being conducted on the internet. More and more of governments, exchange information internally and externally on the internet. Different aspects of our economies run on cyberspace, for example finance, health, energy and transport. Many business models are built on the uninterrupted availability of the internet and the smooth functioning of information systems.

With these facts, it can be imagined that cybersecurity incidents, either if they are accidental or they are criminal, they can cause a lot of consequences in the countries' economies, hence the citizens' everyday life. Such incidents can disrupt from simple aspects of our everyday life, for example electricity, to more serious aspects for example the leaking of confidential information of a state's external policy.

The European Council, needs to work harmonically (internally and externally, in terms of cooperation with other European Union Institutions) in order to strengthen cybersecurity. It needs to protect the cyberspace from malicious incidents and misuse. The European Union aims to strengthen its cyber security rules in order to tackle the increasing threat posed by cyberattacks as well as to take advantage of the opportunities of the new digital age. It should focus on two aspects, namely the precautions and the effective response in such incidents.

The main key player organisations in cybersecurity

a) The European Union Agency for Network and Information Security

Known by the acronym ENISA, it was founded in 2004. The purpose of its founding is a high level of network and information security in the EU.

ENISA helps the Commission, the Member States and the business community to address, respond and specially to prevent NIS problems. The main activities run by ENISA include:

- collecting and analysing data on security incidents in Europe and emerging risks;
- promoting risk assessment and risk management methods to enhance capability to deal with information security threats;
- running of pan-European cyber exercises;
- supporting Computer Emergency Response Teams (CERTs) cooperation in the Member States;
- awareness-raising and cooperation between different actors in the information security field.

b) The EU Computer Emergency Response Team

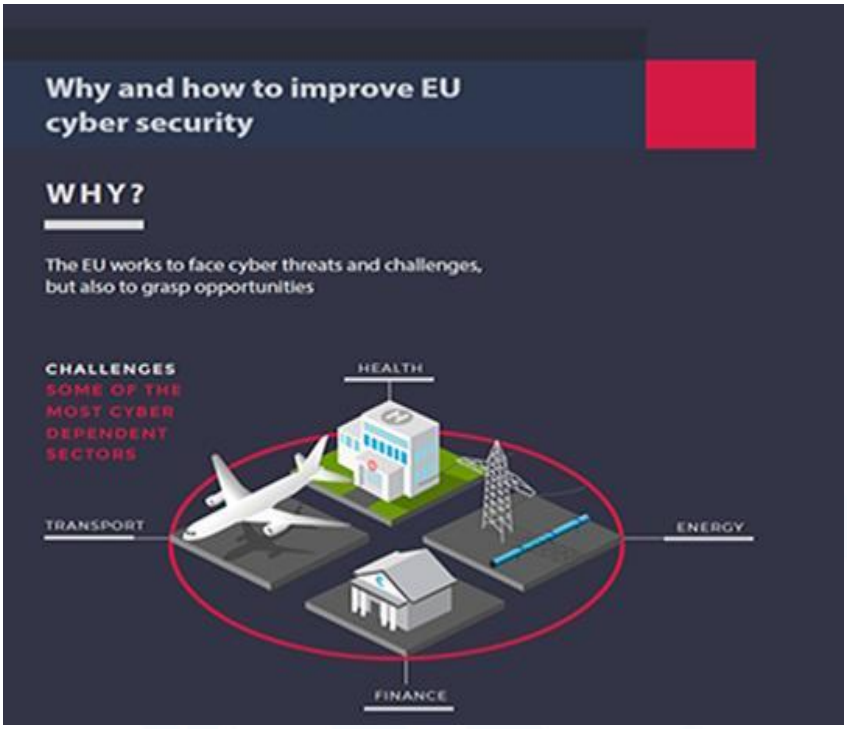
Known with the abbreviation CERT-EU. It was set up in 2012, with aim to provide response to information security incidents and cyber threats against the European Union's' institutions, agencies and bodies. It consists of some security experts and experts form the General Secretariat. Also, it co-operates with regional CERTs from the member states security personnel from specialized IT security companies.

c) The Europol's Cybercrime Centre

Set up in 2013, it is an integral part of Europol, specialized in preventing combating cybercrime, in cross-border terms. It is:

- serving as the central hub for criminal information and intelligence;
- supporting Member States' operations and investigations by means of operational analysis, coordination and expertise;
- providing strategic analysis products;
- reaching out to cybercrime related law enforcement services, private sector, academia and other non-law enforcement partners (such as internet security companies, the financial sector, computer emergency response teams) to enhance cooperation amongst them;
- supporting training and capacity building in the Member States;
- providing highly specialised technical and digital forensic support capabilities to investigations and operations;
- representing the EU law enforcement community in areas of common interest (R&D requirements, internet governance, policy development)

The purpose of a reform in the current cybersecurity policy by the European Union is to strengthen its current rules to tackle the increased cyberattacks more efficiently and take advantage of the new technologies available as well.



The European Union aims to strengthen its cyber security rules in order to tackle the increasing threat posed by cyberattacks as well as to take advantage of the opportunities of the new digital age.

In October 2017, the use of a common approach to EU cyber security was proposed by the European Council, following the reform package proposed by the European Commission in September.

This reform aims to build on the measures put in place by the cyber security strategy and its main pillar, the directive on security of network and information systems - the NIS directive.

The proposal sets out new initiatives such as:

- building a stronger EU cyber security agency
- introducing an EU-wide cyber security certification scheme
- swiftly implementing the NIS directive

These are the main reasons such a reform is needed.

- Security challenges are increasing day by day. The EU needs to raise awareness and speed and quality of response.
- The use of internet is already widespread and tens of billions of connected digital devices are expected by the end of 2020.

- Cyberattacks are estimated to cost 400 billion euros a year.

Furthermore, according to studies, the cyber-awareness in Europe is very low in some instances:

- 69% of companies have no or basic understanding of their exposure to cyber risks
- 60% of companies have never estimated the potential financial loses related to a cyber attack
- 51% of European citizens feel not at all or not well informed about cyber threats

In the Council

December 20th, 2017: EU institutions took an important step in strengthening their cooperation in the fight against cyberattacks. An inter-institutional arrangement established a permanent Computer Emergency Response Team (CERT-EU) covering all the EU's institutions, bodies and agencies. CERT-EU will ensure a coordinated EU response to cyberattacks against its institutions. In order to do so, it will work closely with IT security teams of the EU institutions and member states. It will also cooperate with NATO counterparts.

November 20th, 2017: The General Affairs Council called for the strengthening of European cyber security and the enhancing of cyber resilience across the EU. These goals are in line with the priorities laid out by the European Council in October 2017.The ministers stressed the need for all EU countries to make the necessary resources and investment available to address cyber security. They also highlighted the important connection between trust in digital Europe and achieving cyber resilience across the EU.

October 24th, 2017: The Telecommunications Council agreed to set up an action plan for the reform of EU cyber security. The ministers stressed that online security is essential for European citizens and businesses.

The funding by the EU

From 2007-2013 the EU invested 334 million euros in cybersecurity projects. Two programmes that were funded dealt with trustworthy network and service infrastructures, cryptology and advanced biometrics. One of them was the 7th Framework Programme (PF7) and the Competitiveness and Intervention Programme (CIP).

For the PF7 alone, 50 million Euros were spent, in order to address topics such as the economy of cybercrime, risk analysis for infrastructure protection, money laundering and dedicated road mapping actions.

From 2014-2016 160 million Euros were invested, under the Horizon 2020 Programme for cybersecurity research and innovation projects. Also, on the period 2017-2020, the EU will invest 450 million Euros from the

Horizon 2020 programme to pursue cybersecurity research and innovation under the contractual public-private partnership on cybersecurity.

Cybersecurity and privacy are part of two streams of the Horizon 2020 programme:

- Under the Societal Challenge "Secure societies – Protecting freedom and security of Europe and its citizens". The Digital Security strand focuses on increasing the security of current applications, services and infrastructures by integrating state-of-the-art security solutions or processes, supporting the creation of lead markets and market incentives in Europe. Security is also a so-called "digital focus area" under other challenges (privacy and security in e-health; energy; transport; innovative security solutions for public administrations). The aim is to ensure digital security integration in the application domains. The Fighting Crime and Terrorism strand focuses on increasing the knowledge of the cybercrime phenomenon - its specificities, its economy (including its unlawful markets and its use of virtual currencies) and the means for law enforcement authorities to fight it more efficiently and to prosecute offenders with more solid evidence from specialised forensic activities

- Under Leadership in enabling and industrial technologies Projects on dedicated technology- driven digital security building blocks are funded (such as the 2014 calls on Cryptography and Security- by-Design). Security is also integrated as a functional requirement in specific technologies, such as the Internet of Things, 5G, Cloud, etc.

Part C: Bloc Positions

Leading countries with developed cybersecurity:

Countries as France, Austria, Switzerland, Sweden, Norway... They have an already developed level of cybersecurity in their country. Their role is to guide the other, less developed in cybersecurity issues countries and share their intelligence with them

Countries in a developing stage

Countries as Bulgaria, Croatia, Cyprus, Czech Republic, Germany, Greece, Italy, Romania, The Baltic countries, Spain, etc. Those countries are still in a maturing stage regarding cybersecurity. The ones with better economies are adapting better in the new technologies. The ones with weaker economies have the need of adaptability and the leadership of more aware, and economically strong countries.

Some points to focus on

A good point to start your research is to examine how effective are the existing measures and programmes regarding cybersecurity in the EU. Furthermore, you could think what could be done to strengthen the existing programmes. You can use your critical thinking to evaluate the proposed reform by the European Council and then think how it could be improved. Also, you could use your creative thinking and come up with ideas regarding other programmes could the EU establish for more cybersecurity or improvement of the existing one. Last but not least, you could research on what other funding sources could be used.

Bibliography

Global Cyber Security Index, 2017, published by the International Telecommunication Union <https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&cad=rja&uact=8&ved=0ahUKEwiJgNqx-IXZAhUlIcAKHUhkCr8QFggvMAE&url=https%3A%2F%2Fwww.itu.int%2Fdms_pub%2Fitu-d%2Fopb%2Fstr%2FD-STR-GCI.01-2017-PDF-E.pdf&usg=AOvVaw1_QmdsEagc2ghcHlyAc_Ez>

Ted Julian, *Info security group*, Defining moments in the history of cybersecurity and the rise of incident response, December 2014 <https://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/>

Robert K. Ackerman, *Armed Forces Communications Electronics Association*, International Cultural Differences Hinder Cyber Cooperation, December 2013, <https://www.afcea.org/content/international-cultural-differences-hinder-cyber-cooperation>

Chris Graham, *The Telegraph*, NHS Cyberattack: everything you need to know about the biggest 'ransomware' offensive in history, May 2017 <http://www.telegraph.co.uk/news/2017/05/13/nhs-cyber-attack-everything-need-know-biggest-ransomware-offensive/>

The Emerging Future, Human Intuitive Perspective on Technological Advancements (five, ten, twenty, thirty, forty, fifty years) <http://theemergingfuture.com/speed-technological-advancement.htm>

Directive on Network and information Security <http://europa.eu/rapid/press-release_IP-15-6270_en.htm> accessed on 21 March 2018

Factsheet on EU cybersecurity initiatives <http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf> accessed on 21 March 2018

Directive on attacks against information systems <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF> accessed on 21 March 2018

Directive on combating the sexual exploitation of children online and child pornography <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011L0093&from=EN> accessed on 21 March 2018

Framework decision on combating fraud and counterfeiting of non-cash means of payment <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32001F0413&from=EN> accessed on 21 March 2018

European Agenda on Security
<https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf> accessed on 12 March 2018

Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry
<http://europa.eu/rapid/press-release_IP-16-2321_en.htm> accessed on 11 March 2018

European Union Agency for Network and Information Security
<https://www.enisa.europa.eu/> accessed on 18 March 2018

Reform of Cyber security in Europe
<http://www.consilium.europa.eu/en/policies/cyber-security/> accessed on 18 March 2018

State of the Union, Cybersecurity
<http://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf> accessed on 18 March 2018

Horizon 2020 funding
<http://ec.europa.eu/research/participants/portal/desktop/en/home.html> accessed on 18 March 2018