



COMPLEX SECURITY CHALLENGES – COMPLEX RESPONSES

*Endre SZŰCS PhD**
*Miklós SZAKALI***

Due to the increasing complexity of the security challenges, it is necessary to change the approach and understand security in a much more complex way than before. We consider it even more important to provide the capabilities needed to meet complex security challenges than changing the theoretical approach. Without providing the necessary capabilities, we will not have a chance to prevent and manage complex security challenges.

In the present article, we examine the possibility to ensure complex military and civilian capabilities corresponding to complex security challenges. Also, it is being considered the development and the usability of the defence planning system, generated and used by the military, in order to provide civilian capabilities. Furthermore, we propose to set a parallel structure for military and civilian capability development to provide adequate complex capabilities for complex challenges.

Keywords: *complex security; security challenge; defence planning; national security strategy; international security; international security structure; critical infrastructure.*

** Endre SZŰCS, PhD, is Supervisor and Senior Lecturer of the Doctoral School of Security Studies at Óbuda University, Budapest, Hungary. E-mail: szendre63@gmail.com*

***Lieutenant colonel Miklós SZAKALI is a Senior Analyst and Planner within the Ministry of Defence, and a PhD Candidate in the field of investigation of the interactions between security and defence planning within the Doctoral School of Security Studies at Óbuda University, Budapest, Hungary. E-mail: mszakali@hotmail.com*



Introduction

Throughout history, security has been identified with military security by many branches of science, politics and common knowledge alike. Based on this approach the main driver of security was to avoid armed conflicts and war, almost everything had to promote this policy. The international security institutional system and states' security structures were also established with focus on the management of the military field of security. Accordingly, every effort was made to provide the necessary military forces and capabilities essential for military security.

However, new types of non-military security challenges are increasingly gaining ground in our time. If we consider the basic problems of our days, the COVID-19 pandemic, the effects of climate change, and the extremely rapid development of technology, we can experience that they have already determined our security and expect to have an even stronger impact on it in the future. These challenges do not only cause security risks or dangers in the security dimension, but rather appear in a complex way and have a significant impact on several areas of security. One must admit that neither the international security institutional system, which mainly focuses on military security, nor the states are prepared to deal with comprehensive security challenges. Certainly, international security organizations are trying to adapt to the current challenges and help in the prevention and management of new types of security challenges. However, they lack the capabilities, resources and in many cases, the authorization in dealing with the roots of the problems and thereby, real crisis management. Beside the field of military security, there is no scientifically based method or procedure for capability development and crisis management appearing in any other non-military dimension of security. This statement is even more exact with regard to complex security challenges touching numerous dimensions of security. However, considering the nature of potential security challenges covering several areas, it is not possible to develop specific capabilities to deal with each challenge due to the limited availability of resources and the time-consuming nature of capability development process. Therefore, a solution must be found which, although not specific, can ensure the survival of a country and its population and the management of the emerging crisis by maintaining and developing vital capabilities in the long term. A tool already developed and applied successfully in the field of military security, which is defence planning, can significantly help, since this tool was of crucial importance in security and peace preservation during and after the Cold War, including current changes in the security environment.

1. Defence Planning and Changing Challenges

The 20th century security concept was also reflected after World War II when the international security institutional system (UN, NATO, EU, etc.) was established.



The basic task of the institutional system was to prevent the outbreak and escalation of armed conflicts, thereby avoiding a new war. (UN, un.org 1945) (EU, european-union.europa.eu 1945-59) Therefore, the international security institutions developed their own specific policies, capabilities and assets to fulfil this determinate objective. In the security environment defined by the military confrontation, it became obvious that only those organizations were important enough and could achieve real results in maintaining security, which had real military strength and capabilities. (NATO 1949) Organizations without effective military power became weightless and had no influence in security issues.

On the Western side, the system of defence planning was one of the decisive tools that ensured the West's military strength and capabilities during and after the Cold War, in the midst of multilateral challenges. At the beginning of the Cold War, NATO's military and civilian planners were not yet thinking in terms of long-term forward-looking planning. In April 1951, NATO forces were limited to twelve land divisions, 400 fighter planes. (Bitzinger 1989)

After the German capitulation, the 4,720,000 Western forces were reduced to only 879,000 troops. The Soviet Union, on the other hand, maintained its wartime armed forces of 4 million gaining an obvious superiority over the West. (Bitzinger 1989) The emerging military situation forced the Western planners to balance the Soviet military superiority as soon as possible, which also meant averting a potential military conflict.

When they achieved this short term and very demanding aim, the lessons had been learned, namely the "reactive mode" (force and capability balancing) should be avoided. They recognized that a forced situation where they always had to follow in their opponent's footsteps required great effort and resources in the short term, and in case of failure, the opponent could gain advantage that might upset the military balance and increase the risk of armed conflict. This realization was followed by the forward-looking planning of military forces and capabilities for an increasingly longer term. Only such long term forward-looking planning could continuously provide the necessary military forces and capabilities for maintaining the regional security and ensure the advantage, ultimately, the victory of the Western bloc in the Cold War.

It became general opinion that relying on the economic advantage of the West did not make it easier to overcome the military power of the Eastern bloc. In our view, given the recognition of the West's economic advantage, the role of defence planning should be highlighted. The Western planners recognized the fact that it is not enough to spend more and more resources on the development of military forces and capabilities, it is not enough to "pour money into defence". Even the richest country was not and is not currently in a position to spend the maximum of resources on every segment of defence (maintenance, capability development, operations, etc.).



Therefore, “smart spending” became particularly important, which determined the proportion of resources to be spent on the main activities, maintenance, operations and capability development, as well as provided the resources for the implementation of the most important objectives (priorities).

Without this theoretical approach, there was a risk of wasting resources with multiple negative consequences, i.e. resources ran out and usable, advanced forces and capabilities were not created. All these considerations made necessary the application and development of defence planning. In the development of defence planning process one of the cornerstones was the development of the US Planning-Programming-Budgeting System (hereinafter: PPBS) (Britannica 1961) (Tulkoff-Gordon-Dubin-Hinkle. 2010), which brought the political objectives, military capabilities, resources and time constraints to the same platform and dealt with them based on their interrelations. Building all of this on a short, medium and long term time horizon provided the necessary foresight and capability development to meet expected security challenges. The system was adapted by NATO and its member states and further developed according to their goals and characteristics. (Stojkovic-Dahl 2007) The system of defence planning proved to be successful during the Cold War and, then, also responded in a flexible manner to the challenges of the changed and more demanding security environment following the Cold War. It has been able to provide adequate forces and capabilities for crisis management, counter-terrorism and anti-piracy operations and currently for the deterrence and defence strategy of the West to prevent the spill over of the Russian-Ukrainian war.

The 21st century has passed beyond the exclusive nature of military security challenges and complex security challenges has gained ground and became decisive. Nowadays, there is no security challenge that affects one security dimension exclusively, and does not spread to other sectors of security (political, economic, societal, military and environmental) (Buzan-Waever-Wilde 1997), turning it into a comprehensive challenge or crisis. (NATO-ACT 2017) Considering the recent security events, it became clear that these complex security challenges cannot be managed using the old instruments of international security institutions. Certainly, they do everything possible to support countries in crisis situations, according to their mandate and instrumental possibilities, however they are unable to remedy the root of the problems. They were not able to prevent and stop the COVID-19 pandemic, or to prevent and manage the development and effects of climate change, illegal mass migration, water shortages, energy crisis, food crisis, or prevent the outbreak and escalation of armed conflicts (Azeri-Armenian, Russian-Ukrainian, and Turkish- Syrian).

Next, we would like to illustrate the change and complexity of security challenges by highlighting the following two examples. Terrorism is not a new phenomenon, but becoming transnational, it has created a new situation and a complex global



challenge that is not limited to separate states or regions. (Brown 2022) . Using the results of digitalization and technological developments makes the danger of terrorism grow constantly and expands all dimensions of security. With their attacks, they create mistrust in state institutions, and the population questions the government's intentions and the effectiveness of the security system to protect citizens. The effects of terrorist attacks may lead to general discontent that can culminate in a social explosion, ultimately even to a civil war. As we can see, common crimes against societal security (explosions, attacks on critical infrastructure, etc.) have an impact on the political, economic, military and environmental dimensions of security as well. Therefore, we can assess the prevention and treatment of terrorism as not primarily a military task, however it can be achieved by a comprehensive solution.

A typical 21st century challenge is the cyber threat. It is one of the most dangerous current security challenges, which can be used in many ways, independently and as part of other operations (information, psychological, hybrid, etc.). It poses a particular danger because the attack can remain unnoticed even for a long time since its effect is not manifested in spectacular destructions or casualties. A cyber-attack can be aimed at one or all of the security dimensions, causing huge damage to the given sector or to the whole country. Think of the presidential election, a vital political event for the US, but also decisive for the world, which was already accompanied by international tension in 2016 due to the Russian cyber-attack. According to experts, the Russian President gave direct instructions to the St. Petersburg Internet Analysis Agency to influence US public opinion. (National Intelligence Council 2021) In addition to political influence, economic benefit and destruction have also become the targets of cyber activities. In May 2021, the East Coast oil company USA Colonial Pipeline was hacked causing significant supply shortages for the economy and the public as well. The company used to deliver 2.5 million barrels per day, 45 percent of the fuel supply of the East Coast. The shortage persisted for many days and the USA had to declare an emergency situation to ease the crises. (Manageengine 2021) The incident highlights that cyber-attacks pose an increasing threat not only to the economy and the politics, but also to the elements of the national critical infrastructure, which provide the basis for the daily life of society.

We have selected the two examples above because, based on their connections, one can get an overall picture of the complexity of security challenges. Terrorism itself is a serious threat to security, this is well illustrated by the example of ISIS, which exercised state-like functions and extended its power to all dimensions of security. (Besenyő 2019) In this way, it has become a decisive player from the individuals and smaller communities level to country and region level. The impact of terrorism on security is further enhanced by access to the results of advanced technology, such as the use of the Internet, cyberspace and digitalization. All of these possibilities significantly eases the planning, organization and execution of terrorist



activities, increasing the effectiveness and danger of terrorism. This symbiosis is very well presented in the article “Hezbollah and the Internet in the Twenty-First Century” (Besenyő-Gulyás-Trifunovic 2023) and points out to the need for a comprehensive response to security challenges even more understandable. All of it does not mean that the military dimension of security will lose its importance. Based on experiences in Afghanistan, Iraq, Mali and other hotspots, military capabilities remain indispensable and should be further developed, however we have to admit that alone this is not enough to solve complex challenges.

It became obvious that the countries alone have to cope with security challenges and crises with relatively little international support, at least in the beginning. It is also clear that it is not possible to develop separate capabilities to deal with each of the diverse and complex security challenges. The limited availability of resources and time constraints do not allow us to counterbalance each element of complex challenges with distinct forces and capabilities. Therefore, a strong general base should be established to provide primary resistance, defensive line and provide time and opportunity for developing specific capabilities. We consider critical infrastructure as the most suitable assets for a general base to further build on, since their basic purpose is to provide the necessary products and services for social and individual survival. The importance of critical infrastructure is clearly shown by the fact that during COVID-19 pandemic, several countries (Italy, Hungary, Spain, etc.) have ordered and secured the operation of critical infrastructure under all circumstances, involving the armed forces and the police. We can also see the decisive role of critical infrastructure in the Russian-Ukrainian war, where the Russia is deliberately attacking them, trying to make the Ukrainians’ life unbearable and, in this way, break the resistance of defence.

2. The Possibilities of Defence Planning in the Development of Civilian Capabilities

Bearing in mind the facts and considerations above, the questions which arise would be: Is it possible to develop forces and capabilities that can meet the requirements of comprehensive security challenges? Can the defence planning system developed for the military component of security be applied to provide complex capabilities? Where and what changes need to be made for the defence planning system to be suitable for the development of civilian capabilities? These questions must be asked at the national level by the authorities of each country, since at the international level both NATO and EU made reference to the development of resilience (civilian capabilities) as a national responsibility (NATO, nato.int 2016) (Lasconjarias 2017) (EU, commission.europa.eu 2020).

Our study aims at searching and providing an answer to the afore questions, i.e. whether the defence planning system can be applied to the development of critical infrastructure and, thus, civilian capabilities. After examining different defence planning models, we consider NATO's defence planning model and procedure a possible basis of our investigation. It is a general model based on the above-mentioned PPBS principles that harmonizes the national defence planning models based on similar grounds, thus it has a sort of integrating and synthesizing function, which makes it suitable for the intended purpose.

NATO Defence Planning Process (hereinafter: NDPP) follows a four-year cycle and sets short, medium and long term capability development goals for the Alliance and, thus, also for the member states. However, the NDPP focuses on the short and medium term. Short term planning horizon includes 1-6 years, medium term 7-19 years and long term 19+ years. (NATO, nato.int 2022)



Figure no. 1: The NATO Defence Planning Process
(NATO, nato.int 2022)

The main steps of the NDPP:

1. Political Guidance;
2. Determine Requirements;
3. Apportion Requirements and Set Targets;
4. Facilitate Implementation;
5. Review Results.

The planning process is politically driven, since the security challenges and planning priorities for the planning period are initially defined. With this step the political leadership acknowledges and assumes responsibility for the fact that it is not possible to provide a complete response to all challenges and that even with the



most careful planning, some security risks will exist and politics must take them. It is also a political obligation to provide the necessary resources to achieve the defined objectives. Aside from the political aspect, the military side also plays a decisive role in the process, given that the military establishment “translates” political objectives into military forces and capabilities. Military expertise informs us of the quantitative, qualitative and readiness requirements of the necessary military forces and capabilities, by which the given objectives can be achieved, such as the collective deterrence and defence of the Euro-Atlantic region.

We have concluded that the theoretical approach and structure of the defence planning system provide the possibility to use it for civilian capability development. Following the process of the NDPP, the political guidelines should be translated into civilian capabilities. Adapting the military part of the process, civil professionals must determine the civil forces and capabilities and its related quantitative and qualitative requirements to ensure the implementation of the political will and the achievement of the set goals. To this end, the key issue is the professional implementation of step number 2, where this translation takes place and civilian capabilities are defined with all the necessary parameters. However, this is a complex and difficult task requiring great expertise and experience. The implementation of this task requires a team of experts who are aware of the expected consequences of potential military and non-military security challenges and their civilian capability requirements. Assessing all of the requirements should provide them with the ability to determine the necessary civil capabilities and identify those elements of the critical infrastructure that need to be developed. We do not see the need to make any differences in the structure and the sequence of the further steps of the planning procedure. The basic function of the steps should remain as it is in the present, however, their content may change according to the specifications of the planned domain. For instance, step number 3 includes the allocation of the capability development goals to the competent governmental portfolios and private sectors. There are no changes in the function of the step no. 4, dedicated to the capability development. In this phase plans become reality, it will turn out that our plans and calculations were correct or not and the planned capabilities are achievable or not. The final step of the process is the feedback, the review process, where we have to face our positive and negative results and continue the journey we started or make corrections. The aim is the objective analysis and assessment of our entire planning and implementation activities, otherwise we could get lost in this very difficult and complex process.

We should be aware that capability development is not a short term process. It usually takes about 6-10 years for a capability to become fully operational since it includes the provision of infrastructure, human resources, legal, financial and professional elements, as well as the developing, testing and introductory procedures.



In our opinion, DOTMLPFI¹ (NATO, The NATO Defence Planning Process 2016) system established by NATO for military capability development can also be adapted for civilian capabilities, this also helps to achieve usable capabilities. Taking all of it into consideration we found out that the planning objectives and directions should be defined, at least, for medium and long term, if it is possible, and the resources and other necessary conditions for implementation must be fixed in those plans as well.

For medium and long term capability development plans, especially with regard to critical infrastructure that includes several governmental portfolios, private sectors and sub-sectors, a well-coordinated work on concept and strategy development is essential. It might be useful to introduce the linkage between strategies and capability development process using our national (Hungarian) practice on the hierarchy of strategic documents. The comprehensive National Security Strategy (Government, honvedelem.hu 2020) is the highest policy document that identifies the main challenges, risks and threats and defines those elements essential for their prevention and management. This strategy also defines the priorities of national security and the main directions of capability development.

This is followed by the development of the strategy for each governmental portfolio or sector. It defines the expected main sources of security threats, risks and challenges, which must be countered with the sector's instruments and to this end, it sets the sector's main tasks and directions of capability development. These tasks and directions for capability development are planned in the medium and long term plans of the sector with resource allocation and deadline. However, we found that only some governmental sectors fulfil the obligation and prepare its own strategy related to the National Security Strategy. In many cases the sector-specific strategies are not in line with the National Security Strategy's requirements. This means that there is no centrally managed work on comprehensive capability development that responds to the complex challenges identified by the National Security Strategy.

Currently, the defence sector is following the afore mentioned process and is developing its own strategy, the National Military Strategy (Government, defence.hu 2021) operating the defence planning system to provide military forces and capabilities in line with the National Security Strategy and NATO's requirements. However, the military forces and capabilities are not enough to cope with complex challenges. There is a need for a structured civilian capability development process similar to the military one.

In this difficult period, only a complex governmental approach can provide the capabilities that offer the opportunity to cope with comprehensive challenges. The military side cannot exist without civilian capabilities and the reverse is also true, they can only form together the "two sides of the security coin".

¹ DOTMLPFI - Doctrine, Organisation, Training, Material, Leadership, Personnel, Facilities, Interoperability.

Therefore, we recommend the following structured approach to establish a national security planning system in order to provide military and civilian capabilities in an integrated manner.

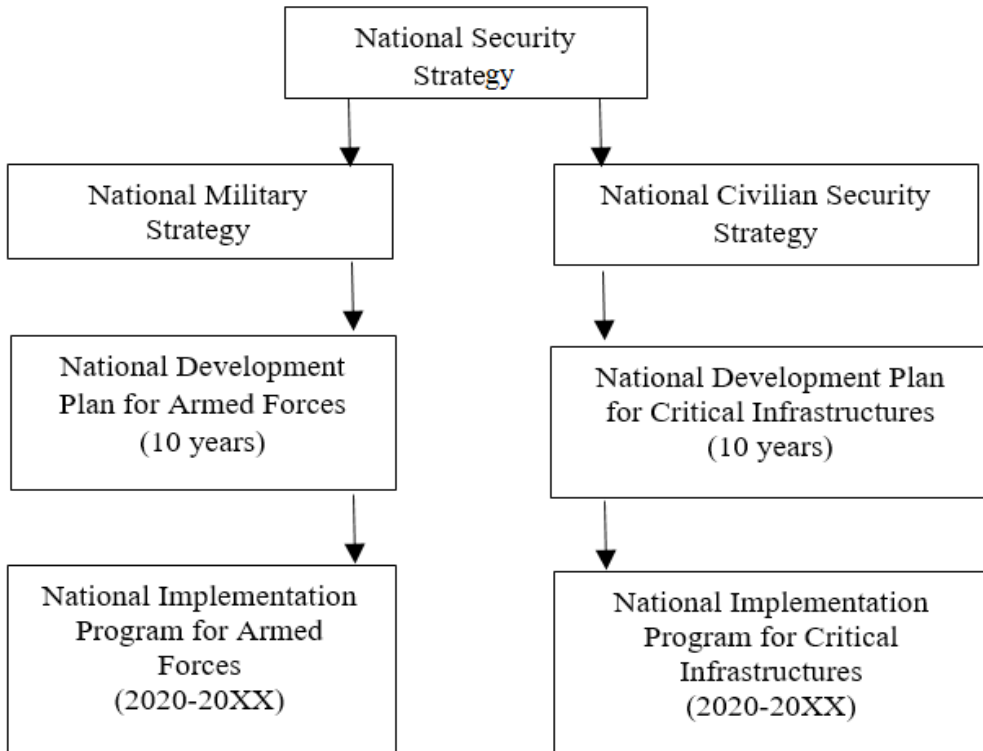


Figure no. 2: Possible structure of strategic planning and capability development on national level

In our view, the comprehensive interpretation of security includes the establishment of a joint structure for developing military and civilian capabilities in a harmonised manner to answer complex challenges. It would cost-effectively ensure the unity of efforts across priorities, avoiding duplication and overlap in capability development. It is our belief that the application of the defence planning system for the development of civilian capabilities would represent a significant step in answering complex security challenges.

Further research and experiments are necessary for the establishment and smooth operation of the integrated national security planning system, taking into account the differences and peculiarities of the civil sectors, but it is our strong belief that this idea should be continued and promoted.



Conclusions

Considering the complex and ever deteriorating security environment, there is a need to change our approach attitude to managing security challenges. We need to understand that the military and non-military security dimensions must be considered in equal measure, since both make up the whole of security. All of this must be reviewed in terms of the authority and tasks of international organizations involved in security matters, since nations received little help in managing recent crises.

We also consider necessary to follow a broader interpretation of security and to approach the security dimensions comprehensively on national level. As part of the security establishment, non-military dimensions should be integrated in the national security planning system on national level and the planning system of defence dimension is to be used as a common approach to develop the necessary capabilities.

It is obvious that we cannot counter complex security challenges by developing specific capabilities that respond to each element of a complex challenge because of the limited availability of resources and time constraints. There is a need for a comprehensive general base that ensures the availability of basic capabilities and provides time and opportunities for specific capability development in case of crises situation. In our view, this comprehensive base is the system of critical infrastructure that could provide the framework for civilian capability development. Development of civilian capabilities through critical infrastructure should be planned in a prospective approach using a medium to long-term planning horizon. We envisage the possibility to use defence planning system in an integrated manner that could provide the necessary military and civilian capabilities in parallel based on coordinated priorities. It could ensure better possibilities to meet the requirements of countering complex challenges.

BIBLIOGRAPHY:

- Besenyő, János, Attila Gulyás and Darko Trifunovic. 2023. Hezbollah and the Internet in the Twenty-First Century. *International Journal of Intelligence and Counterintelligence*. Volume 36/3. <https://doi.org/10.1080/08850607.2022.2111999>
- Bitzinger, Richard A. 1989. *Assessing the Conventional Balance in Europe, 1945-1975*. The Rand Corporation, Santa Monica, CA 90406-2138.
- Brown, Katherine E. 2022. *Transnational Terrorism*. In, McGlinchey, Stephen. *Foundations of International Relations*. London: Bloomsbury, ISSN 2053-8626.
- Buzan, Barry, Ole Waever and Jaap de Wilde. 1997. *Security: A new framework for analysis*, Lynne Rienners Publishers, ISBN 1555877842.
- EU 2020. *Strategic Foresight Report*
https://commission.europa.eu/strategy-and-policy/strategic-planning/strategic-foresight/2020-strategic-foresight-report_en



- EU 1945-1959. History of the European Union https://european-union.europa.eu/principles-countries-history/history-eu/1945-59_en
- Lasconjarias, Guillaume. 2017. Deterrence through Resilience, NATO Defence College, Eisenhower Paper Nr. 7, Rome.
- ManageEngin 2021. The Colonial Pipeline ransomware attack: Lessons from cybersecurity teams, Manageengin Blog, PLAM 360
<https://blogs.manageengine.com/corporate/manageengine/pam360/2021/06/15/the-colonial-pipeline-ransomware-attack-lessons-for-cybersecurity-teams.html>
- Britannica. 1961. McNamara, Robert S. <https://www.britannica.com/biography/Robert-S-McNamara>
- National Intelligence Council. 2021. Foreign Threats to the 2020 US Federal Elections
<https://www.dni.gov/files/ODNI/documents/assessments/ICA-declass-16MAR21.pdf>
- Government, HUN. 2021. National Military Strategy of Hungary. Budapest.
<https://defence.hu/news/national-military-strategy-of-hungary.html#:~:text=Hungary's%20strategic%20objective%20is%20to,and%20non%2Dmilitary%20threats%20and>
- Government, HUN. 2020. National Security Strategy of Hungary. Budapest.
<https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html#:~:text=Our%20primary%20security%20policy%20interest,in%20a%20constantly%20evolving%20environment.>
- NATO 2016. Warsaw Summit Communiqué. https://www.nato.int/cps/en/natohq/official_texts_133169.htm
- NATO-ACT 2017. Strategic Foresight Analysis 2017 Report. Norfolk.
https://www.act.nato.int/wp-content/uploads/2023/05/171004_sfa_2017_report_hr-1.pdf
- NATO Defence Planning Process,
https://www.nato.int/cps/en/natohq/topics_49202.htm.
- Stojkovic, Dejan and Bjørn Robert Dahl. 2007. Methodology for long term defence planning.
<https://issat.dcaf.ch/mkd/download/17291/202850/Long%20Term%20Defence%20Planning.pdf>
- The NDPP (2016), NATO Defence Planning Process, Brussels,
- The North Atlantic Treaty. 1949. Washington D.C. https://www.nato.int/cps/en/natolive/official_texts_17120.htm
- Tulkoff, Milton L., Vance C. Gordon, Rachel D. Dubin and Wade P. Hinkle. 2010. Planning, Programming, and Budgeting System (PPBS)/Multi-year Programming” Institute for Defence Analyse, IDA Document D-4057 Log: H 10-000982, Alexandria, USA
- UN 1945. Charter of the United Nations and Statute of the International Court of Justice, San Francisco. <https://treaties.un.org/doc/publication/ctc/uncharter.pdf>