Forum: North Atlantic Treaty Organisation

Issue: Adapting NATO to a world of strategic competition

Student Officer: Wiktoria Galas

Position: President

Table of contents

“Table of contents” **1**

“Introduction” **1-3**

“Definition of key terms” **3-4**

“Background information” **4-11**

“Involved NATO Organisational Units” **11-13**

“Timeline of events” **13-14**

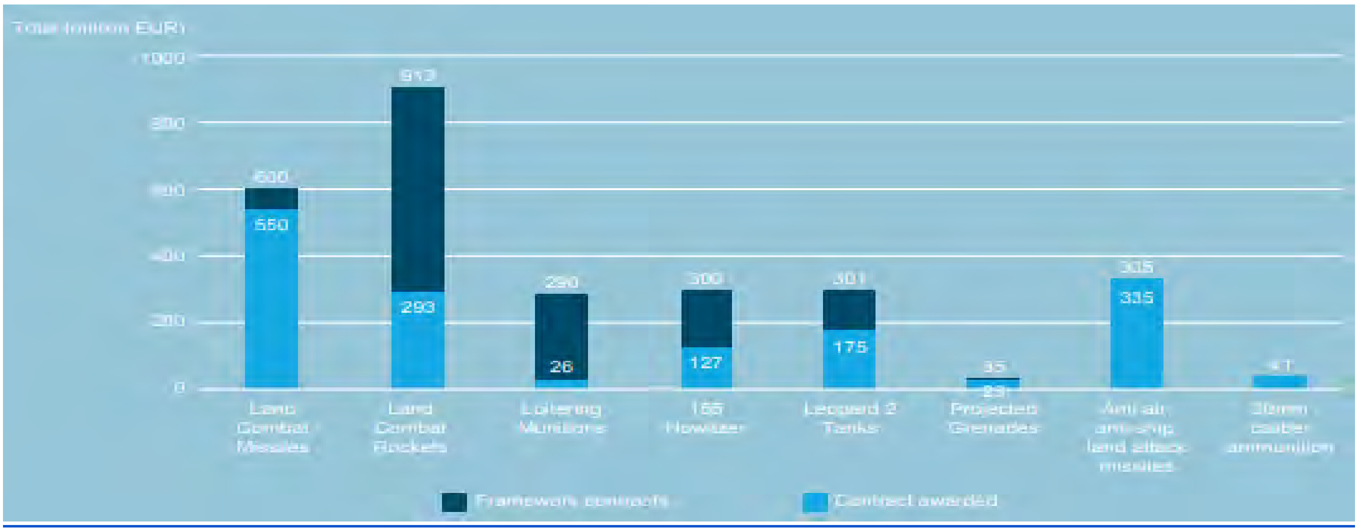
“Possible solutions” **14-15**

“Bibliography” **15-17**

Introduction

As time has passed The North Atlantic Treaty Organisation (NATO) has recognised that the amount of challenges and threats facing it is growing exponentially and therefore so is the need for policies and tactics adapted to a world of strategic competition.

NATO’s strategies focus a lot on countering Russia and its other adversaries by making sure that the organisation’s technological edge is upkept. The Alliance is committed to investing in cutting-edge technology and making sure that its interoperability capabilities are of the highest order. To achieve this, the organisation has developed “High Visibility Operations” - a group of projects that aim to address key NATO defence planning priorities. Currently there are 27 such projects underway addressing one of seven issues; command and control, training structures, high-end acquisition, military mobility and countermobility, ammunition, (Chemical, Biological, Radiological and Nuclear) CBRN defence and finally space technologies. NATO also has dedicated frameworks designed to help Allies procure supplies and currently the Alliance has crested framework contracts, together worth a total of €3.4 billion.



Priorities for NATO Partnerships in an Era of Strategic Competition

Source: https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1008&context=inss-strategic-perspectives

Still there remains work to be done in this domain as NATO is still facing challenges with language barriers amongst personnel, training standards, system overloads, coordination and compatibility of systems.

Part of upkeeping the level and standard of technology that NATO possesses is scouting out, identifying, fostering and protecting innovative and disruptive technologies and their diverse ecosystems throughout the Alliance. To support this, in June 2022 NATO launched The NATO Innovation Fund which is the world's first multi-sovereign venture capital fund that invests directly into start-ups and indirectly into other venture capital funds that are working on cutting-edge technology.

6G and Internet of Things are amongst the technologies that are currently being examined and are thought to be potentially transformative for NATO's communication networks. More notably, the Alliance is currently working on implementing Artificial Intelligence (AI) for areas such as cyber security, imagery analysis, undersea infrastructure security, situational awareness and more. In 2022 the organisation established the Data and Artificial Intelligence Review Board whose task is to deliberate on the standards, assessments and tool kits for the certification of AI applications in defence and security.

In June 2023, NATO also established The Defence Innovation Accelerator for the North Atlantic (DIANA) programme, which aims to build a new alliance of entrepreneurs to help provide NATO with the necessary tools it needs to preserve peace and security. To do so the DIANA issues challenges and asks entrepreneurs to respond to them with a possible solution, the best ones get chosen and are provided with access to testing environments that connect them to defence experts and are provided funding.

While NATO is working on a lot of its challenges and finding solutions on a daily basis, some major problems concerning technology have risen over the past years and are yet to be solved. Currently the Alliance is fighting to maintain its edge, but it is also facing the problem that the People's Republic of China is fighting them when it comes to innovation on things like semiconductors, more commonly known as computer chips. Furthermore the Alliance is also currently having a problem with its supply chain, facing a shortage of such technologies.

The combination of intelligence and technology is what creates strategies for NATO. Since Russia's invasion of Ukraine (February 24, 2022) the importance of up-to-date, accurate and relevant intelligence has risen significantly and NATO has put a lot of effort into bolstering its surveillance, recognition and intelligence capabilities. Currently the Alliance Future Surveillance and Control initiative is pioneering a trailblazing multi-domain surveillance and control formation to create a harmonious, network-centric "system of systems". Additionally the Organisation is working on making sure that the next generation of its Alliance Ground Surveillance system, a fleet of currently five Phoenix aircrafts that provide constant aerial monitoring over extensive areas, regardless of weather and light conditions will be ready to set into action after the Phoenixes operational lives are over. Besides that in 2023, 19 NATO Allies launched the Alliance Persistent Surveillance from Space Initiative. Its goal is to create" Aquila" - a virtual constellation, made up of national and commercial space assets to help unify data collection, sharing and analysis within the Alliance.

Definition of Key Terms

Strategic competition:

Refers to competitive activity taking place between great powers of the world on a strategic plane, resulting from often long-standing tensions between the different parties involved. This leads them to compete against each other across all domains of statecraft, including economics, defense, national security, cyberspace, intelligence and espionage, intellectual property, disruptive technologies, diplomatic maneuvers and soft power reasons.

Unipolar moment:

Period of time in international relations, where one country achieves a preponderance of power, that no other country could possibly compete with. That period is only considered as unipolar if there is no possible counterbalance, the moment one appears the period is no longer deemed unipolar.

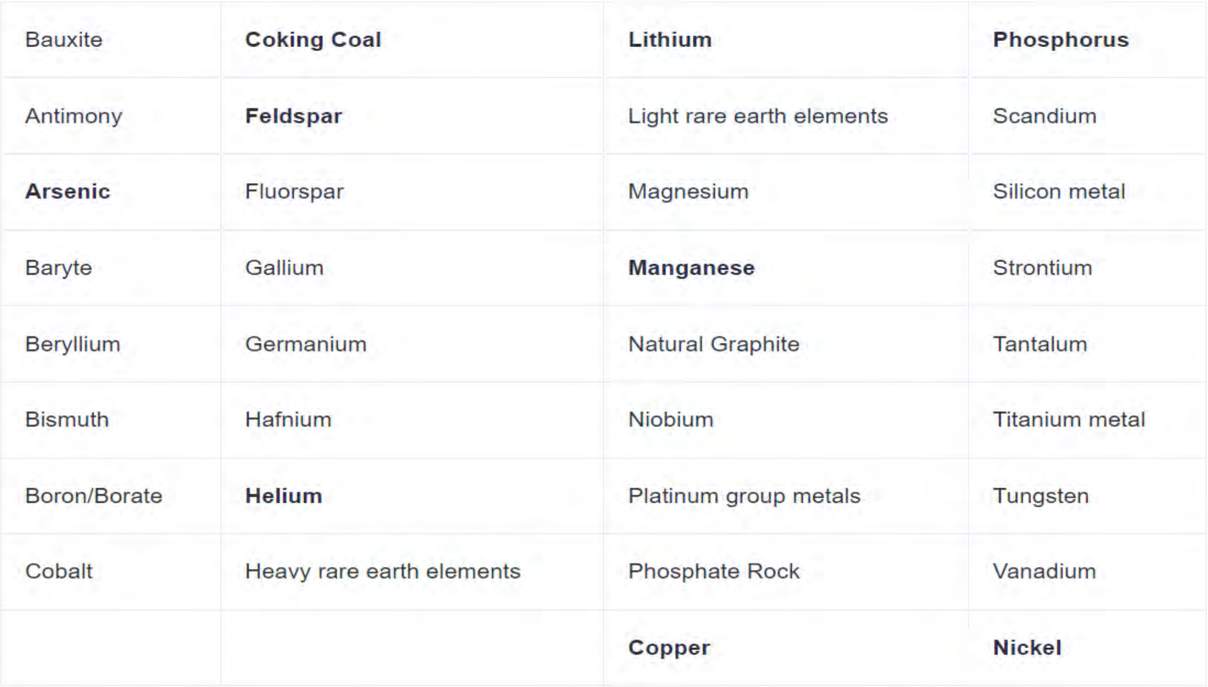
Interoperability:

The capacity of different systems to act in tandem with the intention of achieving common and agreed upon goals. In a case like NATO's interoperability allows for the coordination and cooperation of multinational forces.

Critical Raw Materials (CRMs) :

Refers to substances (ex: rare earth materials and other metals), deemed to be of high economic and defence importance with an exorbitant risk of disruption of supply, attributable to the concentration of their sources in only a few spaces and difficulty of substitution for another, less risk saturated element. Supply of CRMs is often provided by few producers, often making countries with lesser stockpiles of them reliant on imports from those suppliers.

In 2023 the European Union established their list of CRMs to being:



Bauxite	**Coking Coal**	**Lithium**	**Phosphorus**
Antimony	**Feldspar**	Light rare earth elements	Scandium
Arsenic	Fluorspar	Magnesium	Silicon metal
Baryte	Gallium	**Manganese**	Strontium
Beryllium	Germanium	Natural Graphite	Tantalum
Bismuth	Hafnium	Niobium	Titanium metal
Boron/Borate	**Helium**	Platinum group metals	Tungsten
Cobalt	Heavy rare earth elements	Phosphate Rock	Vanadium
		Copper	**Nickel**

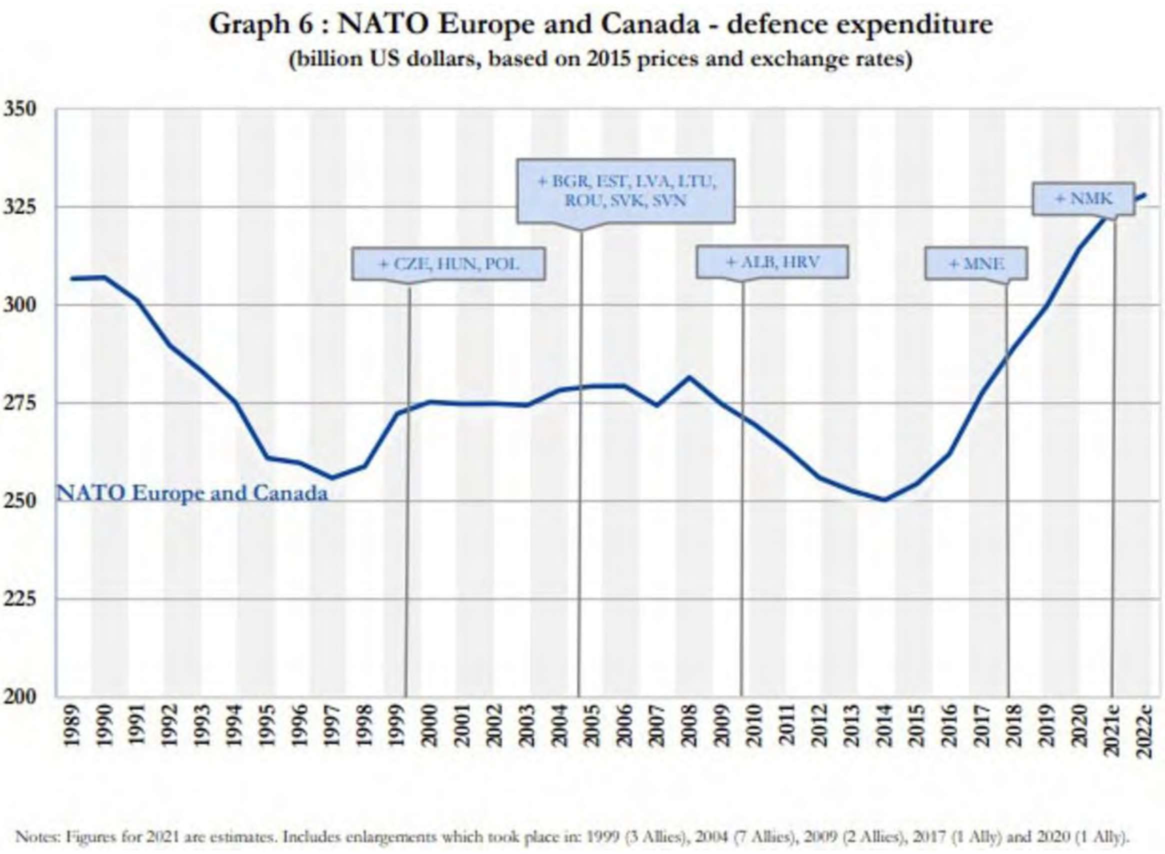
Source:https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials_en

Advanced persistent threat (APTs):

Refers to a state-sponsored group of tenacious cyber hackers, using the most advanced tactics and techniques, in order to compromise governmental or large/international organisations' infrastructure.

Background Information

In the time succeeding the end of the Cold War and the fall of the USSR, the world saw a significant decrease in the defence spending of the member countries of the North Atlantic Treaty Organisation (NATO), who were hopeful that the time of conflict had passed. For comparison, during the Cold War NATO, Allies defence spending consistently averaged over 3% over their Gross Domestic Product (GDP), with some variation over the years, while during the first years post Cold War, many countries' defence spending dropped notably below 2% (a minimum theoretically required by NATO) .



Graph 6 : NATO Europe and Canada - defence expenditure
(billion US dollars, based on 2015 prices and exchange rates)

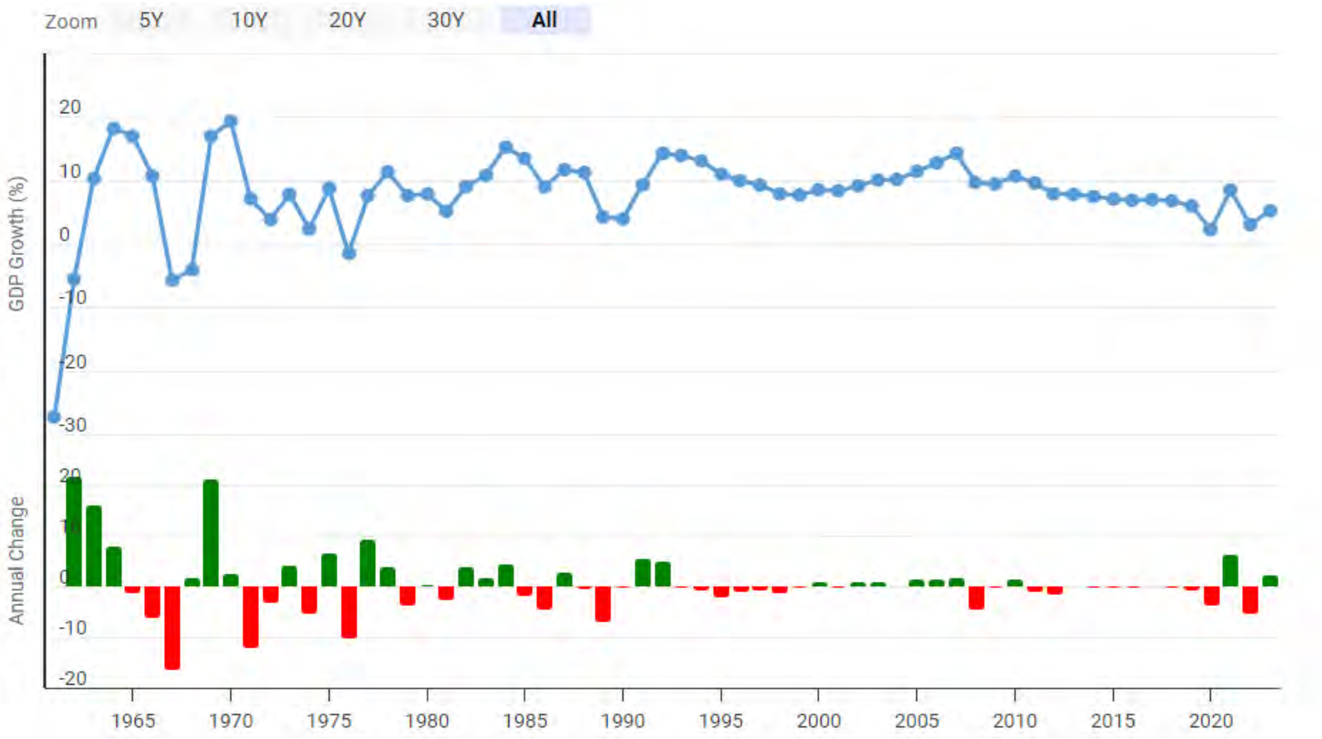
Notes: Figures for 2021 are estimates. Includes enlargements which took place in: 1999 (3 Allies), 2004 (7 Allies), 2009 (2 Allies), 2017 (1 Ally) and 2020 (1 Ally).

Source:https://www.macrotrends.net/global-metrics/countries/CHN/china/gdp-growth-rate

At the same time the countries, who were part of the “Eastern bloc”, were trying to resist the after effects of having been under the USSR for so many years. Many decided to join NATO and the European Union (EU) in hopes of rebuilding their economy, stabilising their democracy and regaining their place in the Euro-Atlantic relations.

The end of the Cold War also led the world to a “unipolar moment” . In between the years of 1991 and 2002, The United States of America was the world’s sole superpower as no other country could rival them. This led countries such as the People's Republic of China and the Russian Federation to oppose American hegemony. The global economic crisis and recession of 2008 officially marked the end of this era and the other major powers of the world were all again seeking to assert their dominance in the international arena.

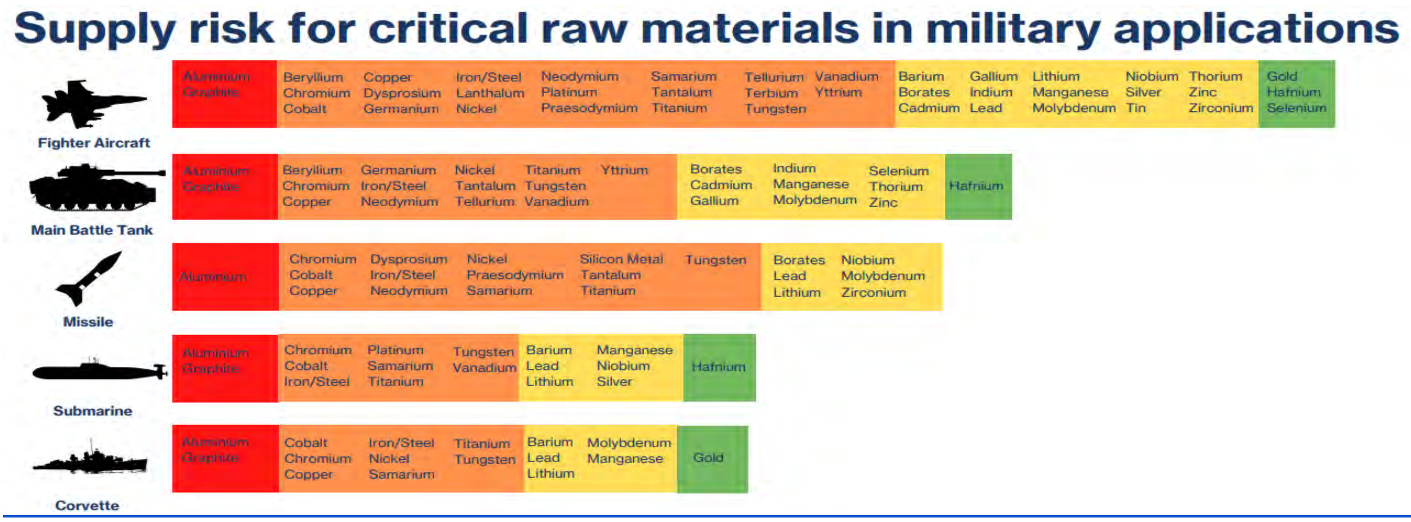
The latter 20th and early 21st centuries also saw the economic rise of the People’s Republic of China, who by opening itself up to international trade and investment as well as by introducing free-market reforms was able to grow its GDP by over 9% each year since 1978, when the reforms began. China’s rapid economic growth was impossible to stop by the governments of “western” countries. Year to year its economy developed more and more, eventually bringing it to being what it is today, a great leverage, effective in many negotiations.



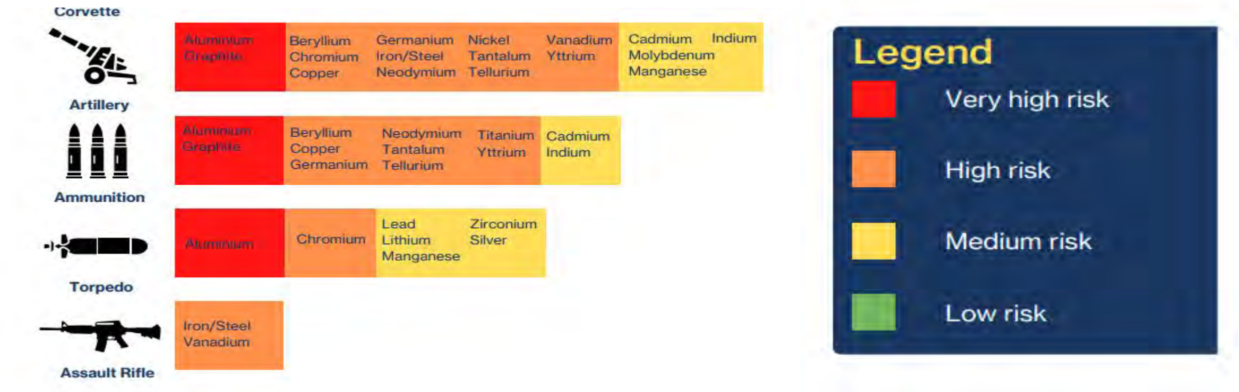
Source: *https://www.macrotrends.net/global-metrics/countries/CHN/china/gdp-growth-rate*

Supply chain problems and dependency on non-member countries:

NATO member countries are currently facing a rising supply risk of critical raw materials, vital to the manufacture of armament and to the upkeep of countries’ defence industry, military and economy in crisis and in peacetime. Metals such as cobalt, lithium, graphite, aluminium and rare earth elements are key ingredients in telecommunications, infrastructure, defence and energy and are therefore necessary to maintaining countries’ stability.



Fighter Aircraft	Aluminium Graphite	Beryllium Chromium Cobalt Copper Dysprosium Germanium Iron/Steel Lanthalum Nickel Neodymium Platinum Praesodymium Samarium Tantalum Titanium Tellurium Terbium Tungsten Vanadium Yttrium	Barium Borates Cadmium Gallium Indium Lead Lithium Manganese Molybdenum Niobium Silver Tin Thorium Zinc Zirconium	Gold Hafnium Selenium
Main Battle Tank	Aluminium Graphite	Beryllium Chromium Copper Germanium Iron/Steel Neodymium Nickel Tantalum Tellurium Titanium Tungsten Vanadium Yttrium	Borates Cadmium Gallium Indium Manganese Molybdenum Selenium Thorium Zinc	Hafnium
Missile	Aluminium	Chromium Cobalt Copper Dysprosium Iron/Steel Neodymium Nickel Praesodymium Samarium Silicon Metal Tantalum Titanium Tungsten	Borates Lead Lithium Niobium Molybdenum Zirconium	
Submarine	Aluminium Graphite	Chromium Cobalt Iron/Steel Platinum Samarium Titanium Tungsten Vanadium	Barium Lead Lithium Manganese Niobium Silver	Hafnium
Corvette	Aluminium Graphite	Cobalt Chromium Copper Iron/Steel Nickel Samarium Titanium Tungsten	Barium Lead Lithium Molybdenum Manganese	Gold

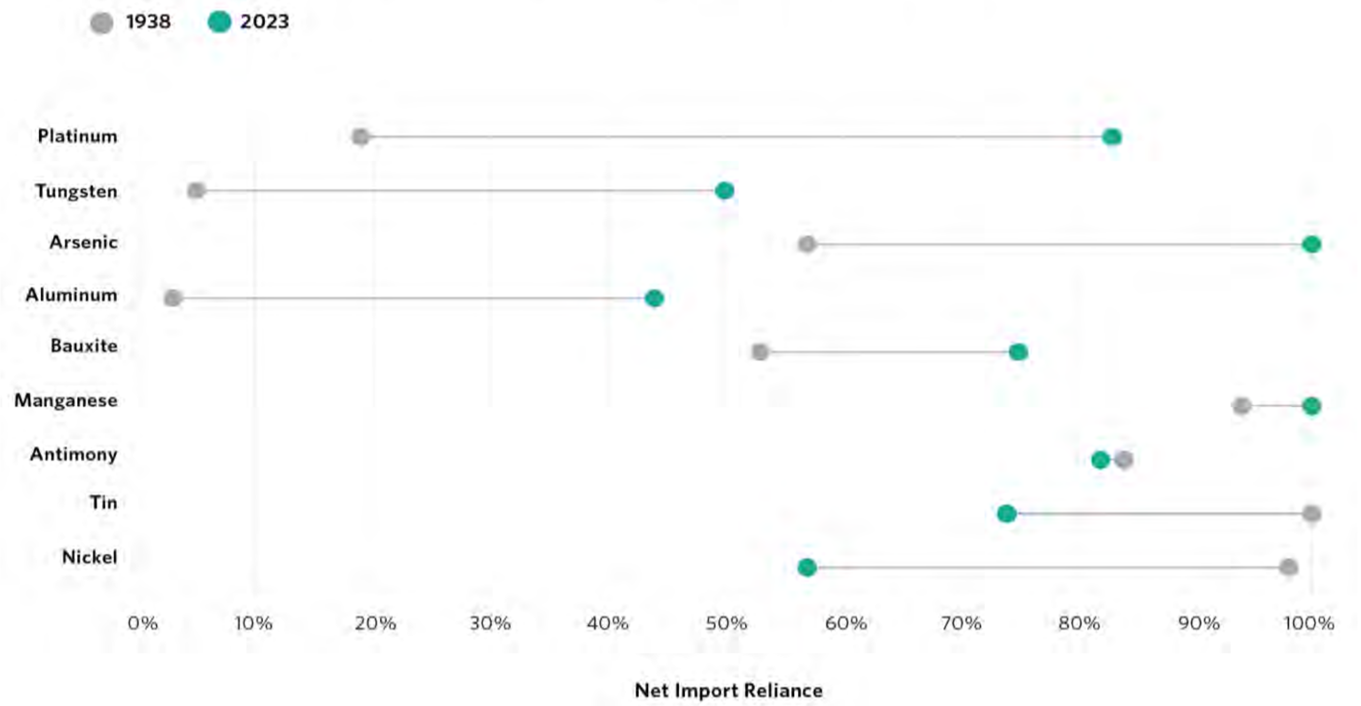


Source:https://hcss.nl/wp-content/uploads/2023/01/Strategic-Raw-Materials-for-Defence-HCSS-2023-V2.pdf

The importance of these materials means that they can be either a great leverage or a hazardous vulnerability if a country's supply chain is not reliable.

Unfortunately, because of their finite domestic production of CRMs, NATO members are heavily reliant on imports of CRMs from other non-member countries, including the People's Republic of China for items such as graphite, rare earth element and different minerals needed for the production of batteries as well as the Russian Federation for aluminum, nickel and titanium.

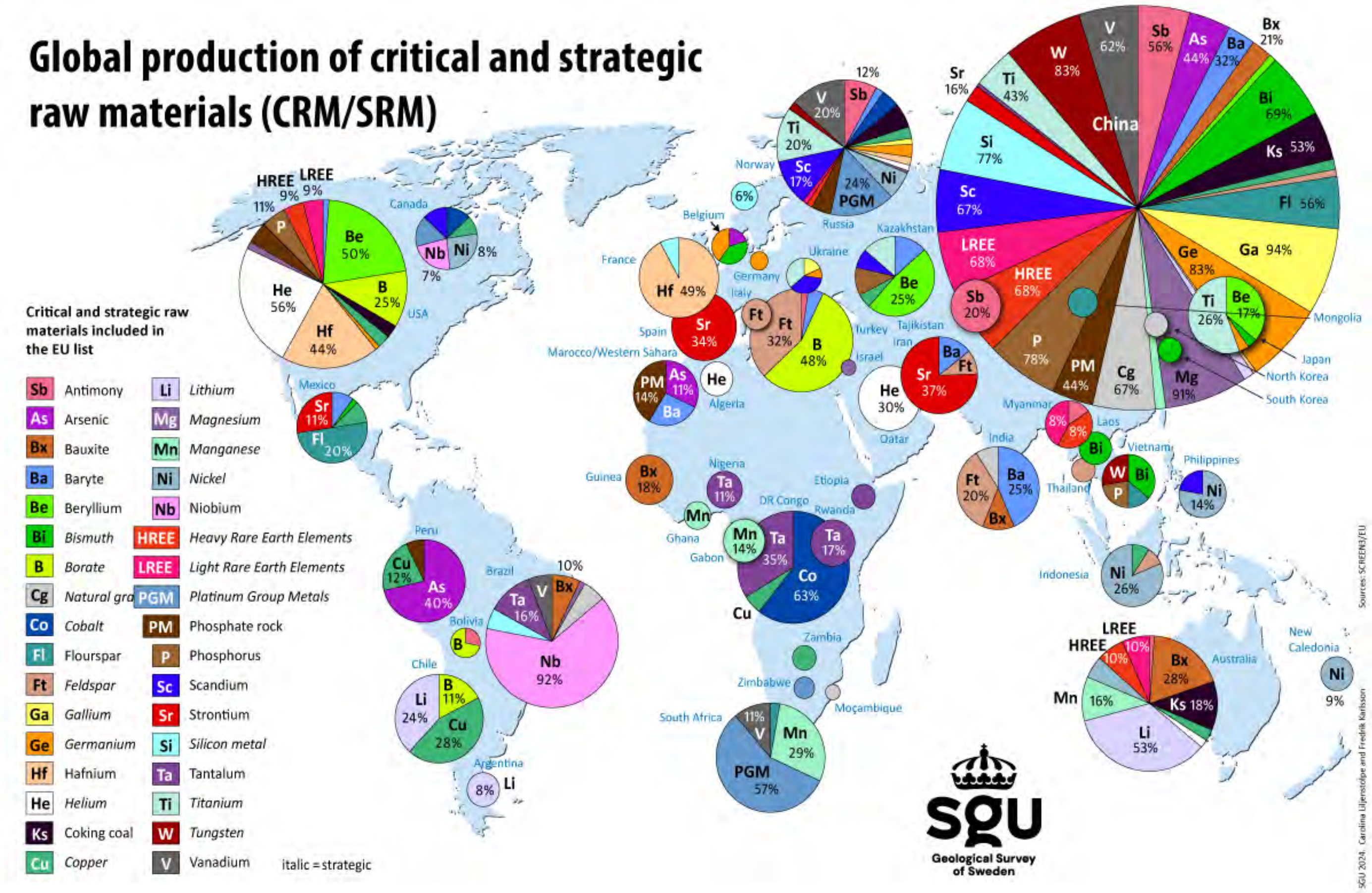
Figure 1. The U.S. Now Relies on Mineral Imports to Meet Its Consumption



Source:https://carnegieendowment.org/research/2024/02/the-us-military-and-nato-face-serious-risks-of-mineral-shortages?lang=en

In 2023 NATO Secretary General, Jens Stolenberg issued a statement advising the Alliance against becoming overly dependent on China's minerals in order to avoid a situation similar to when some

NATO members became overly dependent on Russia for gas. It is important to note that the European countries, who are also a part of the European Union, have decreased their consumption of Russian aluminium significantly (from 21% to 8%) since the war in Ukraine started (because of sanctions) .



Source: https://www.sgu.se/en/mineral-resources/critical-raw-materials/

Additionally, current import problems caused by export controls imposed by non-NATO nations (NNNs) are worrying. It is important to note that some of the said NNNs continue to keep an adversarial stance toward NATO. In 2021, China placed a ban, preventing its manufacturers from exporting graphite to Sweden, most likely to hold back the development of green technologies in the country. In late 2023, China placed further restrictions, limiting the export of graphite, gallium, germanium and antimony to the United States of America.

Nowadays, concerns are being raised about the possibilities of China placing even more restrictions on exporting rare earth elements or bismuth to NATO members, which would have great impact. As a result of the Russian invasion on Ukraine the CRM market's size has significantly been reduced. Russia used to control a lot of rare elements supply, especially for EU members of NATO, but lost its position due to sanctions. Unfortunately there are limited sources that can be used instead.

Following that, another issue that keeps coming up is the utilisation of CRMs by NATO members in contrast with their stockpiles. With a lot of resources going to help Ukraine in the fight against Russia, members have seen an exact demonstration of how wartime needs can exceed theoretical assessments.

Chromium, copper, beryllium, natural graphite and aluminium are only some of the CRMs that are currently being spent very quickly, because of the increased production of defense platforms and munitions in order to keep up with demand.

With rising tensions on the horizon, the Alliance is also looking at the safety of supply lanes. Transporting CRMs often means using maritime lanes. It is the most efficient way during peacetime, however the transports' safety might be questionable during wartime as the required size of combined naval flotilla to provide effective escort for massive container ships is heavily disproportionate with the resources required to threaten them.

Cyber-security threats and cyber intelligence:

With the rise of the information age, a new domain with applications in defence and intelligence appeared, cyberspace, nowadays officially recognised as the 4th domain of warfare, it has become a key playing field for NATO.

Currently, the Alliance and its member countries, experience thousands of cyber-attacks on their networks per month, ranging from low-level attacks to extremely sophisticated incidents. While each country is in charge of its own cyber defences, NATO acts as a platform for Allies to coordinate their activities, discuss cyber defense issues and share knowledge on cyber threats. It is important to note that cyber attacks can be aimed directly at a specific member or at the Organisation's internal or Internet facing networks.

The most serious attacks are orchestrated by Advanced Persistent Threats (APTs) and pose considerable danger. APTs aim at gaining access to important infrastructure to either collect sensitive information or disrupt operations of governmental/NATO services. Nowadays it is rare that any attack against NATO or NATO countries turns into a serious incident, but the digital arms race remains a concern. It is likely that adversarial nations keep their APTs from using most advanced tactics and techniques to prevent revealing their capabilities in time of relative peace and preserve them to be used during potential direct conflict to disrupt critical military activities.

Another group of attackers are hacktivists. Both hacktivists and APTs are seeking the opportunity for promoting their agenda through propaganda and typically through simple attacks of Denial of Service (DOS) type - usually against the official governmental/NATO Internet websites. Some of the biggest windows for such cyber attacks are NATO Summits, when hackers try to derail the outcome of the meetings by spreading false information and alleged stolen intelligence using DOS attacks as attention drawing events. Another technique of spreading propaganda is through fake NATO/NATO Nations websites which are often built to mimic true websites and typically provide content with rather subtle modifications to redirect the thought process of a reader.

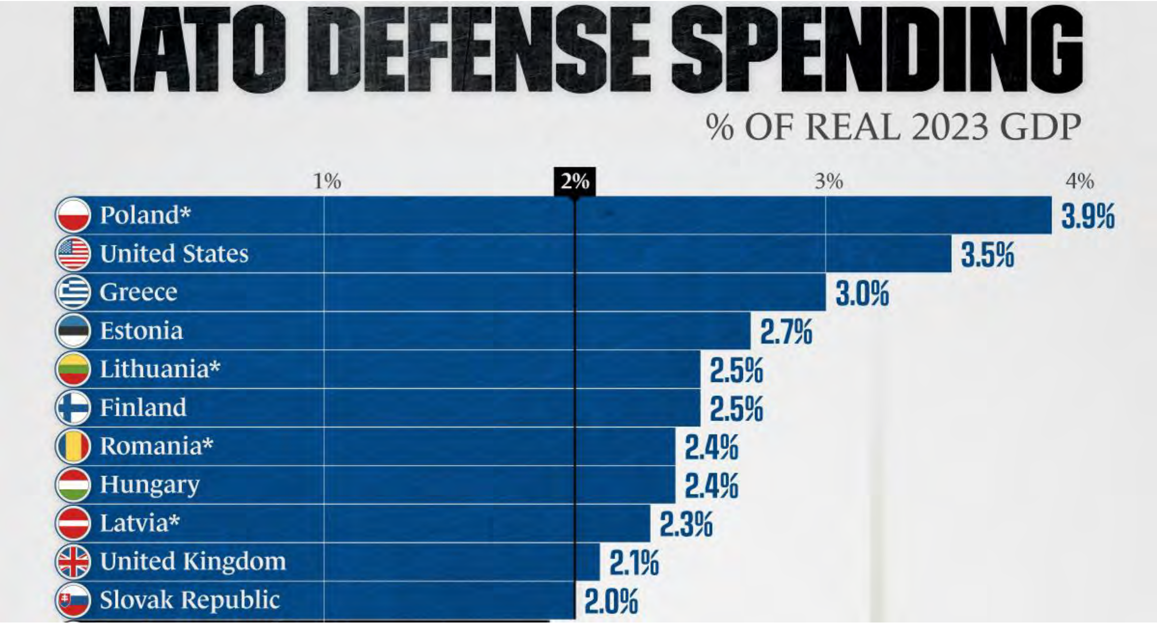
As already mentioned, cyber espionage is a serious threat. Part of NATO deterrence strategy is to maintain technological dominance in the military domain. APTs seek to collect all sensitive information, but their focus is on intellectual property, especially of modern technology and military applications. These range from direct assault at organisational boundaries in an attempt to break through perimeter defensive controls to phishing and spear phishing campaigns which jump over proverbial fences and try to exploit human nature to gain a foothold in the heart of the organisation.

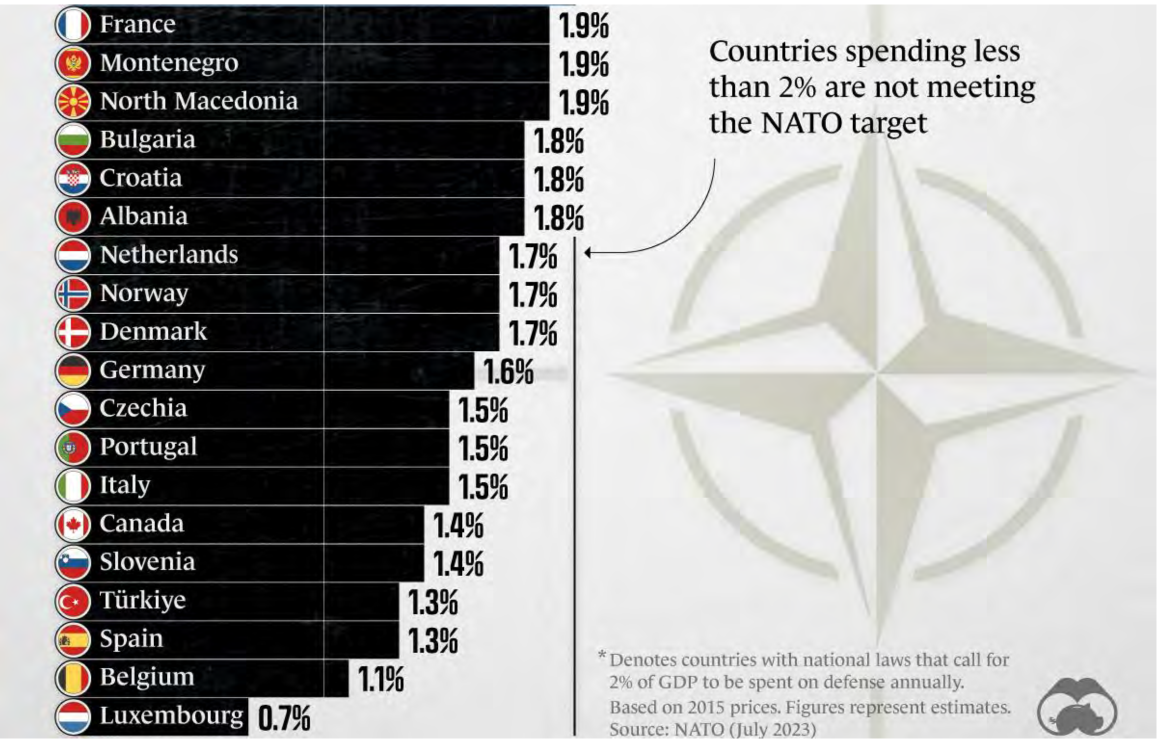
As it has been highlighted, the traditional supply chain is a considerable concern for the modern military. As it happens it is equally a big concern in the cyber domain. Trust in supplied goods, being hardware or software, cannot be taken for granted, as proven by Solarwinds or weaponised LoJack (aka Computrace) campaigns where malicious code implanted in seemingly innocent products allowed APTs to gain a very strong foothold into victims' infrastructure.

Military and defense challenges:

NATO countries are facing military equipment shortages. After the end of the Cold War, they started to invest less and less into their defence capabilities, believing that the time of conflict was over. Prolonged drop of financing led to weaker military stance both in hardware and human resources. Not only the number of new projects but also the maintenance of existing capabilities dropped. As a result, national armies are having problems with heavy artillery, armored vehicles, as well as air forces. A lot of the equipment is not in the best working condition. Moreover there is a shortage of ammunition for any prolonged conflict. To make things worse the production capabilities are reduced to almost nonexistent in most of the countries and the biggest supplier, namely the USA, is on a different continent than the majority of NATO countries. It is a long, long supply chain in case of conflict in Europe.

Even though, since Russia's invasion of Ukraine, many countries have expressed their intent to increase their spending on military to an agreed 2% of GDP, in reality not that many of them did it. Amongst others, countries are in dire need for more artillery shells, anti-tank missile surface-to-air missiles, etc.





Source:https://www.visualcapitalist.com/which-countries-meet-natos-spending-target/

Another issue is the size of NATO members' armies. The same phenomenon, which impacted the hardware supply also had effects on military personnel. Most of the countries significantly reduced the size of their armies. A lot of people, who have never known war and therefore have not felt the existential threat creeping up, were not/are not interested in joining or supporting the military. Notably, member countries' efforts to try and spike their army recruitment haven't been as good as they could have been either, with some experts going as far as saying that NATO forgot about its military for years.

On top of that, NATO has a decision process that is not necessarily made to work in the case of disagreement. Since the beginning The Alliance makes decisions by consensus - an agreement reached by common consent. This is not an easy process, especially nowadays when different countries have widely different stances on different topics. It is unclear how well it will work if the situation requires strong and drastic decisions.

In 2019, NATO Allies embraced a new Space Policy, declaring space as the newest, fifth operational domain and two years later the Allies affirmed that Article 5 is also applicable in the case of an attack on Allies' space assets. Since then the Alliance has worked on bettering its stand in the overwhelmingly more and more crowded domain but a lot of challenges still remain and have to be addressed.

Space is an increasingly more and more congested domain that plays a key role in most countries' various essential activities, such as but not limited to: military operations, economic transactions, communication, weather monitoring, etc. This dependency creates a number of vulnerabilities.

Amongst others, the Allies are facing a growing threat from opposing countries, such as China or Russia, who possess substantial anti-satellite capabilities and have the ability to carry out various hostile activities against NATO countries, through actions that can degrade the quality of/deny their space-facilitated military capacities. This was demonstrated amongst others in 2019, when during a NATO exercise, Russia conducted a series of activities, which interrupted NATO GPS signals and secure communication networks. After an investigation, the incidents were traced and connected to Russian sites. Additionally, it has been noted that the Republic of China is currently in possession of operation-ready ground missiles, aimed at attacking Low Earth Orbit (LEO) satellites with suspicion of pursuit of such capabilities for space assets in other orbital layers.

Involved NATO Organisational Units :

NATO Headquarters:

Located in Brussels, Belgium, NATO HQ acts as the administrative and political centre for the Alliance. It is the place where member countries' representatives can come together to discuss issues and make decisions on a consensus basis. The HQ is home to NATO's principal political decision body, The North Atlantic Council as well as to the political delegations from member countries.

Allied Command Operations (ACO):

ACO is the organisational unit in NATO, responsible for the planning and execution of all of the Organisation's military operations. ACO is in charge of several specialised commands which have permanent headquarters spread throughout the Alliance. Their commanders report directly to the Supreme Allied Commander Europe (SACEUR), who assumes overall responsibility of operations at the strategic level from his office at the Supreme Headquarters Allied Powers Europe (SHAPE) in Belgium. SHAPE is also a house of National Military Representatives (NMRs) at NATO, who are liaisons between national militaries and ACO.

Allied Air Command:

Located in Ramstein, Germany, the Allied Air Command or AIRCOM is the single Command for all of NATO's air and space needs. Its job is to provide 24/7 activity to reduce the effectiveness of any rival air operations and deter any air or missile threat.

Allied Maritime Command:

Located in Northwood in the United Kingdom, The Allied Maritime Command or MARCOM is the main Command of all Alliance forces. MARCOM assures the interoperability of all NATO maritime resources. The MARCOM Commander is the Alliance's primary advisory in any maritime issue and he reports directly to the SACEUR.

Allied Land Command:

Based in Izmir, Turkiÿe, the Allied Land Command or LANDCOM is in charge of coordinating NATO Land Forces by facilitating interoperability, standardisation and land domain readiness. The LANDCOM Commander is the leading advisory to the Alliance in all matters concerning land operations and he answers directly to the SACEUR.

NATO Cyber Security Center (NCSC):

The main hub of technical experts for cyber defence in NATO responsible for agile and resilient cyber defences to prevent, detect, respond to and recover from cyber security incidents across the estate. NCSC is part of the NATO Communications and Information Agency (NCIA) with its core operations being located in the Supreme Headquarters Allied Powers Europe (SHAPE) campus. NCSC provides 24/7 cyber technical services to the whole of NATO.

Strategic Cyber Threat Analysis Branch (CTAB):

Based in NATO HQ, in Brussels, CTAB' responsibility is to deliver evidence-based analysis of the cyber threats landscape to make sure that the Alliance is able to make risk-informed decisions by combining all-source data and cutting edge technologies in order to support and enhance NATO leadership's understanding on the nature of cyber competition and conflict. CTAB identifies strategic patterns and trends in cyber space and generates tailored insights to support network defence and mission assurance with predictive analysis, cyber threat intelligence, and threat hunting.

NATO Cyber Operations Center (CyOC):

During the Warsaw Summit in 2016 NATO recognised cyberspace as the newest NATO domain of operations. In result the CyOC was called into existence in the Supreme Headquarters Allied Powers Europe (SHAPE). Its primary mission is to defend NATO's digital landscape from cyber- attacks, ensuring the seamless operation of military and civilian functions. The centre's core objectives include preventive, defensive, collaboration as well as training and educative functions for cyberspace.

Office of the Chief Information Officer (OCIO):

The Chief Information Officer's (CIO's) office is located in NATO HQ, in Brussels. The office works directly under the North Atlantic Council aegis and its main task is to put into action the Allies' plans for Information and Communication Technology (ICT), by facilitating the cohesion, the integration and the alignment of all ICT systems across the Alliance's networks. CIO is also a single point of authority for cybersecurity.

Timeline of Events

Date	Description of event
December, 3rd, 1989	Date of declaration of the end of the Cold War
1991 - 2002	Unipolar moment: The USA are the sole superpower of the world
2007	Cyber onslaught against Estonia (first modern cyber attack on a large scale)
2007 - 2009	Great Recession
February 2014	Annexation of Crimea by Russia
July 2016	Warsaw Summit (cyberspace becomes NATO domain of operations)
December 2019	After a meeting in London, the Allies declare space as the 5th operational domain.
October, 22nd, 2020	A Space Center is established at the Allied Air Command in Ramstein.
2019 - 2021	COVID-19 Epidemic (highlights delivery chains' possible issues)
June, 2021	After the Brussels Summit, Allies declare that article 5 can be invoked in the case of an attack on Allies' space assets.
December, 1st 2021	China places ban on exportation of its graphite to Sweden
February, 22nd 2022	Russia invades Ukraine for the 2nd time
2023	China places multiple bans on exporting certain CRMs to The USA

Possible Solutions

Supply chain problems and dependency on non-member countries:

To help with the supply chain problems, NATO members should work on finding more reliable, substitute countries that can provide them with the CRMs. Furthermore, NATO members should make sure that all necessary CRMs are stockpiled for a case of emergency, these stockpiles could be funded by the implementation of higher tariffs on CRMs imported from rival countries such as China.

Additionally NATO members could expand their efforts on trying to find good substitutes for CRMs in certain industries such as the energy industry. Finding innovative ways to recycle CRMs may also prove to be a good tactic.

NATO members may also want to consider increasing their domestic mining of CRMs and should continuously support the search for new domestic mines, smelters and refineries, required to produce CRMs. They could do this by investing capital in enterprises that mine CRMs.

In order to deal with the length of the supply chain problem countries should invest into their own production capabilities. Potentially they can group up and form hubs when the financial investment is too high for a particular country.

Cyber-security threats and cyber intelligence:

In order to deal with trust toward supply chain issues NATO should establish better and stronger controls (oversight) over process and execution of the supply.

Generally, for all cyber security related threats NATO members should strengthen cooperation and exchange information about APTs. NATO as an organisation has a crucial role of the exchange facilitator.

In order to combat phishing, countries have to educate the general population and establish better security controls to prevent technical exploitation of human naivety.

In order to combat cyber espionage there should be increased effort to implement best security practices. To make it happen NATO members should build up their cyber forces.

Military and defense challenges:

NATO members should try and reach the minimum of 2% of GDP investment into their defence capabilities. Each nation should work out how to get to that goal. They can also work on expanding their efforts in army recruitment to ensure the size of their armies is proportional to the threats they face

Research Report vetted by Deputy Secretary-General Aryav Bhesania and Mr Alain Meidinger

Bibliography

“Multinational capability cooperation”

https://www.nato.int/cps/en/natohq/topics_163289.htm

“The Secretary General’s rapport”

https://www.nato.int/nato_static_fl2014/assets/pdf/2024/3/pdf/sgar23-en.pdf#page=75

“Adapting NATO to an unpredictable and fast-changing world”

https://www.nato.int/docu/review/articles/2018/02/19/adapting-nato-to-an-unpredictable-and-fast-changing-world/index.html

“NATO’s role in conventional arms control”

https://www.nato.int/cps/en/natohq/topics_48896.htm

“Operations and missions:past and present”

https://www.nato.int/cps/en/natohq/topics_52060.htm

“Defence spending: sustaining the effort in the long term”

https://www.nato.int/docu/review/articles/2023/07/03/defence-spending-sustaining-the-effort-in-the-long-term/index.html

“China’s Economic Rise: History, Trends, Challenges, and Implications for the United States”

https://www.everycrsreport.com/reports/RL33534.html

“Deterrence and defence”

https://www.nato.int/cps/en/natohq/topics_133127.htm

“Emerging and disruptive technologies”

https://www.nato.int/cps/en/natohq/topics_184303.htm

“NATO AND UKRAINE Successes and Complexities on the Path to Interoperability”

https://c2coe.org/wp-content/uploads/Library%20Documents/Annals/Seperate%20Articles/2024-01%20C2%20Annals%20-%20NATO%20and%20Ukraine%20(Vakarin).pdf

“NATO’s Strategic Vision: Adapting for the Future through NATO Allied Command Transformation’s Initiatives”

https://www.act.nato.int/article/natos-strategic-vision-adapting-through-act-initiatives/

“Strategic-Raw-Materials-for-Defence-HCSS-2023-V2”

https://hcss.nl/wp-content/uploads/2023/01/Strategic-Raw-Materials-for-Defence-HCSS-2023-V2.pdf

“NATO Needs to Align on Supply of Critical Raw Materials”

https://www.rand.org/pubs/commentary/2024/06/nato-needs-to-align-on-supply-of-critical-raw-materials.html

“The U.S. Military and NATO Face Serious Risks of Mineral Shortages” https://carnegieendowment.org/research/2024/02/the-us-military-and-nato-face-serious-risks-of-mineral-shortages?lang=en

"Aluminium group calls for EU to go much further on Russian bans"
https://www.reuters.com/markets/commodities/industry-group-says-eu-should-go-much-further-bans-russian-aluminium-2023-12-08/

"2021-06-nato-ensec-coe-strategic-analysis-on-the-key-minerals-markets"
https://www.enseccoe.org/wp-content/uploads/2024/01/2021-06-nato-ensec-coe-strategic-analysis-on-the-key-minerals-markets.pdf

"Critical and strategic raw materials"
https://www.sgu.se/en/mineral-resources/critical-raw-materials/

"Euroviews. Europe's tough choice: Sanction aluminium or proceed with climate goals"
https://www.euronews.com/business/2024/10/17/europes-tough-choice-sanction-aluminium-or-proceed-with-climate-goals

"Defence-Critical Supply Chain Security Roadmap"
https://www.nato.int/nato_static_fl2014/assets/pdf/2024/7/pdf/240712-Factsheet-Defence-Supply-Chain-Ro.pdf

"How Russian hackers targeted NATO's Vilnius summit"
https://www.politico.eu/article/russia-hackers-targeted-nato-vilnius-summit-graphika/

"Strengthening Cyber Resilience: NATO's Cyber Coalition and Collective Defence"
https://www.act.nato.int/article/cyber-coalition-collective-defence/

"Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis"
https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

"NATO Cyber Defence"
https://www.nato.int/nato_static_fl2014/assets/pdf/2021/4/pdf/2104-factsheet-cyber-defence-en.pdf

"Securing Britain's and NATO's digital supply chains"
https://www.nato.int/docu/review/articles/2024/10/14/securing-britains-and-natos-digital-supply-chains/index.html

"Cyber defence"
https://www.nato.int/cps/en/natohq/topics_78170.htm

"Consensus decision-making at NATO"
https://www.nato.int/cps/en/natohq/topics_49178.htm

"NATO'S STRATEGY FOR A CHANGING WORLD IN 2024"
https://asociatia-alpha.ro/gidni/11-2024/GIDNI-11-Hist-a.pdf#page=85

"Priorities for N Priorities for NATO Partnerships in an an Era of Strategic Competition"
https://digitalcommons.ndu.edu/cgi/viewcontent.cgi?article=1008&context=inss-strategic-perspectives

"Surely but Slowly: NATO Adapts to Strategic Competition"
https://yalebooks.yale.edu/2024/08/14/surely-but-slowly-nato-adapts-to-strategic-competition/

"NATO Headquarters"
https://www.nato.int/cps/en/natohq/topics_49284.htm

"CIO Main Accountabilities"
https://www.nato.int/structur/recruit/2021/20211021-OCIO0012-main-accountabilities.pdf

"Strategic Cyber Threat Analyst vacancy 230121"
https://www.gov.pl/attachment/014fb406-6872-4e5d-b44f-3d0af1ba1c4b

"Warsaw Summit Communiqué"
https://www.nato.int/cps/cn/natohq/official_texts_133169.htm

"2021 Fact Sheet – Multi Corps Land Component Command Concept"
https://www.act.nato.int/wp-content/uploads/2023/05/2021_EiE_STLE_MCLCC.pdf