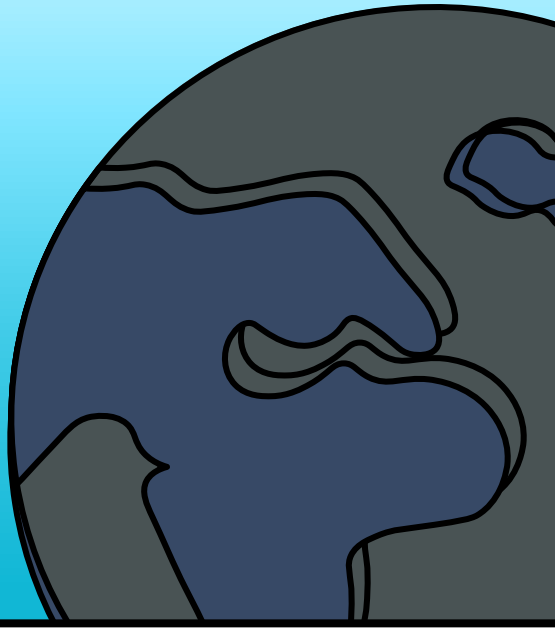
epis ThinkTank
international foreign affairs & security politics

Issue V
November 2024
epis-thinktank.de

SHIFT OF PERSPECTIVE



INTERVIEW WITH WERNER FASSLABEND

Former Minister of Defence

Proliferation of Satellite Mega-Constellations

What does the rise of satellite mega-constellations mean for Europe's strategic autonomy? As the space industry shifts to commercial dominance, mega-constellations like Starlink offer global connectivity but also pose strategic risks. This article explores how Europe's dependence on non-EU satellite infrastructure could undermine its security and analyses the EU's response, including the development of IRIS², a sovereign constellation project. Discover the challenges and opportunities Europe faces in securing space autonomy amidst growing US and Chinese influence in low Earth orbit.

Sovereignty in Cyberspace

Is an international consensus on cyber-sovereignty possible? As cyber-attacks surge globally, the urgency for defining state sovereignty in cyberspace has intensified. This article explores the difficulties of regulating this domain, addressing issues like anonymity, the rapid pace of technological evolution, and conflicting state jurisdictions. By examining cyberspace alongside traditional domains like airspace and maritime zones, it assesses whether current laws suffice or if a novel legal framework is required, offering critical insights for navigating cyber-sovereignty's complex landscape.

Table of contents

Commentary

Guest Contribution

Interview

Columns

FOREWORD

Theodor Himmel

Theodor Himmel (born 1998 in Berlin), studied law at the University of Cologne and an Erasmus semester at the Aristotle University of Thessaloniki. During his studies, he got involved in politics, completed an internship with a parliamentary group in the German parliament and participated in the 30th VIS Moot in Vienna, the PAX Moot in Paris and various Model United Nations conferences. He is currently pursuing an LL.M. in international procedural law at Leiden University. At EPIS, he edits the magazine as editor-in-chief, focusing on international foreign and security policy.

Alvin Karl Bürck

Alvin Karl Bürck is pursuing a MSc in International Political Economy at the London School of Economics and Political Science after graduating with a BA in Political Science from the University of Konstanz.

Pablo Mathis

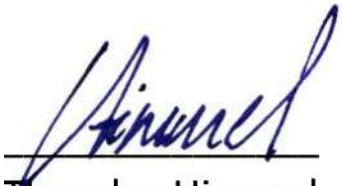
Pablo Mathis is currently pursuing an MA in War Studies at King's College London. He holds a BSc (Hons.) in Security Studies from Leiden University.

EPIS Magazine Foreword

One needs to shift the perspective. By the literal meaning, having a perspective means to have seen through something; to have thought about it from start to finish. Yet, in a complex world, things do not have just a start and a finish - not just a beginning and an end, not just a front and a back, not just one perspective. To truly understand, one must also look at what is unfolding beside it. A shift, a change, a turn: another view on things. How does the situation change from a different perspective? Are other conclusions needed? How do we respond to them? In articles and additional guest contributions, we gather insights from shifting perspectives on various topics. This is the focus of the fifth issue of the EPIS Magazine.

We thank all contributors to this issue. Emile Berthet explores Europe's pursuit of autonomy in the satellite industry, examining how dependence on mega-constellations challenges its security landscape. Chloe Young delves into the intricate issue of cyber sovereignty, considering the implications of state jurisdiction in an increasingly digital world. Jonathan Barry examines the Arctic's evolving geopolitical significance, once seen as a zone of peace but now a focal point for global power competition. Mara Sandru evaluates the EU's Temporary Protection Directive, questioning whether current frameworks for managing refugee crises provide the needed resilience for long-term support. Zell and Groenheijde offer a timely reflection on former Dutch Prime Minister Mark Rutte's potential impact as NATO's Secretary General, while David Stadin considers Sweden's NATO membership and its strategic impact on European defence. Anton Meier analyses shifts in the nuclear balance of power, exploring how advancements in artificial intelligence may alter deterrence dynamics. Vitaliy Venislavskyy, Ferdinand Wegener and Dmytro Sochnyev discuss the transformative potential of artificial intelligence in warfare in their piece. Lastly, Ralph Thiele provides a guest contribution on the Muslim Brotherhood as a hybrid actor, and we present an interview with Werner Fasslabend, Austria's former Minister of Defence, sharing insights into Austria's evolving role in European security.

I am especially thanking my editorial colleagues Alvin Karl Bürck and Pablo Mathis for leading the drafting of this issue, as well as our designer Cira Scherenberger for filling our contents in a nice looking layout. Finally, my thanks go to our growing number of readers and supporters. This issue is dedicated to you, and we hope you enjoy this shift of perspectives.



Theodor Himmel
Editor-in-chief and chairman of
EPIS Thinktank e.V.

GREETINGS FROM EURODEFENCE

Manuel de la Cámara

Manuel de la Cámara has been Ambassador of Spain to Turkey and Azerbaijan, Brazil, and Finland aswell as Deputy Ambassador to Russia, Deputy Permanent Representative to NATO, Head of the Commercial Office at the Spanish Embassy in Washington, and Director General for Security and Disarmament and North America at the Spanish MFA. Serving the Board of Directors of Eurodefense-Spain, he leads the Mediterranean and Migration Observatories of the EURODEFENSE network.

This new issue of the EPIS Magazine arrives at a pivotal moment in the global political landscape. The United States presidential election is just a few weeks away, with candidates Donald Trump and Kamala Harris locked in a tight race according to recent polls. The political atmosphere is highly polarized, and the election's outcome will have far-reaching consequences both domestically and globally.

The Russo-Ukrainian War, Europe's largest conflict since WWII, began with Russia's 2014 annexation of Crimea and escalated in February 2022 with a full-scale invasion. It has caused widespread destruction, casualties, displacement, and alleged war crimes, leading to ICC arrest warrants for Russian officials. The war has transformed European security, and revitalized and expanded NATO to include Finland and Sweden. It exposed Europe's energy vulnerabilities and prompted unprecedented EU unity in sanctioning Russia and supporting Ukraine. However, political fatigue is growing in the West, particularly in the U.S., where a potential Trump presidency could threaten support. Putin is betting on this waning resolve to achieve his objectives.

War in the Middle East rages on, with two main actors: Israeli Prime Minister Benjamin "Bibi" Netanyahu and the so-called "Axis of Resistance", formed by Iran and its proxies in the region. A year after suffering the worst terrorist attacks in their history, Israelis have not been able yet to overcome the trauma caused by those attacks. The war in Gaza continues and Hamas is weakened but not eliminated, the remaining hostages have not been freed and the military operations are now extended to Lebanon, a country Israel partially occupied between 1978 and 2000, with a brief incursion in 2006. Direct confrontation between Israel and Iran seems unavoidable, but perhaps can be contained. Stunning successes like the elimination of most of Hizbollah's leadership have dampened the domestic rejection of Bibi, if only temporarily.

But war is also going on in other parts of the world, from Sudan, Ethiopia, and the DR of Congo to Mali and Burkina Faso in the Sahel, and Myanmar in Asia. There are currently 56 armed conflicts worldwide, the highest number since WWII.

The "new Cold War" between China and the U.S and its allies in the Asia-Pacific region continues. The Biden Administration has made efforts to "decouple" from China economically by reducing U.S. economic dependence, especially in critical sectors. On its part, China is expanding its military and technological capacity and is trying to lure the so-called "global south" to support its quest for a revision of the Western sponsored rules-based international order.

In Venezuela, the incumbent President Nicolas Maduro proclaimed himself winner in the July 28, 2024, presidential elections, despite pre-election polls indicating that the opposition candidate Edmundo Gonzalez Urrutia was leading by more than 20 points. Maduro's régime has refused to publish the electoral records, engaged in violent repression of protesters, and sent Mr. Gonzalez into exile.

The new European Commission, taking office on December 1, 2024, faces a multitude of challenges, such as enhancing EU technological sovereignty, balancing climate goals with economic competitiveness, resolving international trade tensions, addressing rule of law issues in certain member states, managing the migration crisis, particularly in frontline states, and strengthening EU defense capabilities. The surge in irregular migration has become a primary concern for many EU citizens. The effectiveness of the New Pact on Migration and Asylum, scheduled for implementation in June 2026, will be crucial in addressing this issue.

These and many other topics will be addressed by the EPIS Magazine in this and future issues. I commend EPIS and EURODEFENSE for this fruitful and promising cooperation.

Manuel de la Cámara, EURODEFENSE ESPAÑA, October 2024

Proliferation of Satellite Mega-Constellations

Strategic Security and Defence Implications for the European Union

Emile Berthet

Emile Berthet holds a Master's degree in Crisis and Security Management from Leiden University. His academic interests lie in international relations and security, with a particular focus on Europe, the Asia-Pacific, and the defense implications of new technology development.

1. Introduction

Since the early 2010s, the space industry has undergone a significant transformation. The traditional dominance of government agencies in the sector has been challenged by the emergence of private U.S. companies such as SpaceX and Blue Origin, focused on developing innovative, low-cost space technology. This trend towards commercialisation has spread outside the United States, as countries such as China and India are increasingly investing in private space enterprises to develop their space capabilities (Pelton & Madry, 2020). Most notably, the privatisation of the space sector has fostered a reduction in space launch costs through technological advancements such as reusable rockets, cheaper manufacturing processes, and satellite miniaturisation (Young & Thadani, 2022). Today's expanded access to space is enabling the deployment of large networks of thousands of satellites in low earth orbit (LEO). Referred to as LEO constellations, such satellite systems are designed to provide high-speed internet across the globe (Hallex & Cottom, 2020). Perhaps the most well-known example is SpaceX's Starlink, an LEO constellation famous for its unprecedented commercial success. Although SpaceX is the only operator to offer broadband satellite internet to the consumer market as of 2024, numerous governments and private companies are racing to establish their own alternative service. In this context, the number of proposals for LEO constellations has grown considerably in the past few years, the most prominent of which include OneWeb, project Kuiper, LEO Lightspeed, and China's Guowang. Beyond mass-market connectivity, LEO satellite constellations demonstrate a significant potential for security and defence applications and could confer strategic advantages to their operators (Young & Thadani, 2022). Their proliferation therefore introduces new security and defence implications globally. Given the recent nature of these developments, academic literature about LEO constellations largely focuses on digital development, international security, and US national security implications. However, proliferated LEO constellations are also particularly relevant to the EU. In the current context of space militarisation and power competition between China, the US, and Russia, the bloc is facing pressure to develop autonomous security and defence capabilities in space, improve its launch capabilities, and protect its space assets from external threats (Council of the European Union, n.d). Within this scope, the following question is addressed: What are the implications of the proliferation of LEO satellite constellations for EU strategic autonomy in security and defence? This article begins with a background chapter before examining several constellations in development and their applications. The focus is first set on SpaceX's Starlink and US military LEO constellation programs. It then shifts to major LEO projects in China. Finally, these cases are analysed in relation to the EU's space capabilities, highlighting the overall implications for EU strategic autonomy in security and defence.

EU Strategic Autonomy:

The concept of EU strategic autonomy widely describes the ability of the European Union to act autonomously and protect its interests in diverse sectors such as trade, foreign policy, technology, defence, and security without being restrained by dependencies on foreign actors.

2. Background

2.1 Basics of Satellites

Before discussing the strategic relevance of LEO constellations, this section explains the basic technicalities of satellites. Since the launch of Sputnik 1 in 1957, various actors have deployed artificial satellites in orbit around Earth to perform specific missions. These missions typically fall into one of three categories, which

are communications, observation, or navigation. Communications missions provide radio, television, phone, or internet services. Earth observation missions collect measurements and images of the Earth's surface. Meanwhile, navigation missions enable users on the ground to determine their location. Because a single satellite can only cover a limited area of the Earth, satellites often operate in groups known as constellations. These configurations make it possible to undertake missions with global coverage from a given orbit (CBO, 2023; Voelsen, 2021). Satellites are usually launched into one of three main orbits: Low Earth orbit (LEO), at an altitude of 160 to 2000 km, Medium-Earth Orbit (MEO), from 2000 km to 35,786 km, and Geostationary Earth Orbit (GEO), at 35,786 km. LEO an

matching the earth's 24-hours rotation period (Figure 1) (CBO, 2023). Due to their larger field of view and their ability to deliver continuous coverage, GEO satellites are ideal for observation or broadcasting over large areas. Typically, a GEO constellation of only 4 satellites is needed to provide global coverage, ensuring lower launch and operating costs. For this reason, GEO satellites have been predominant in communications for the past 50 years. However, their high altitude means that signals take longer to travel from the earth and back, resulting in a longer latency. MEO satellites, as they stand, are prevalent in navigation missions as they can provide stronger signals across different earth latitudes (CBO, 2023; Young & Thadani, 2022). Lastly, LEO satellites are now being explored for several applications, as we will see shortly.

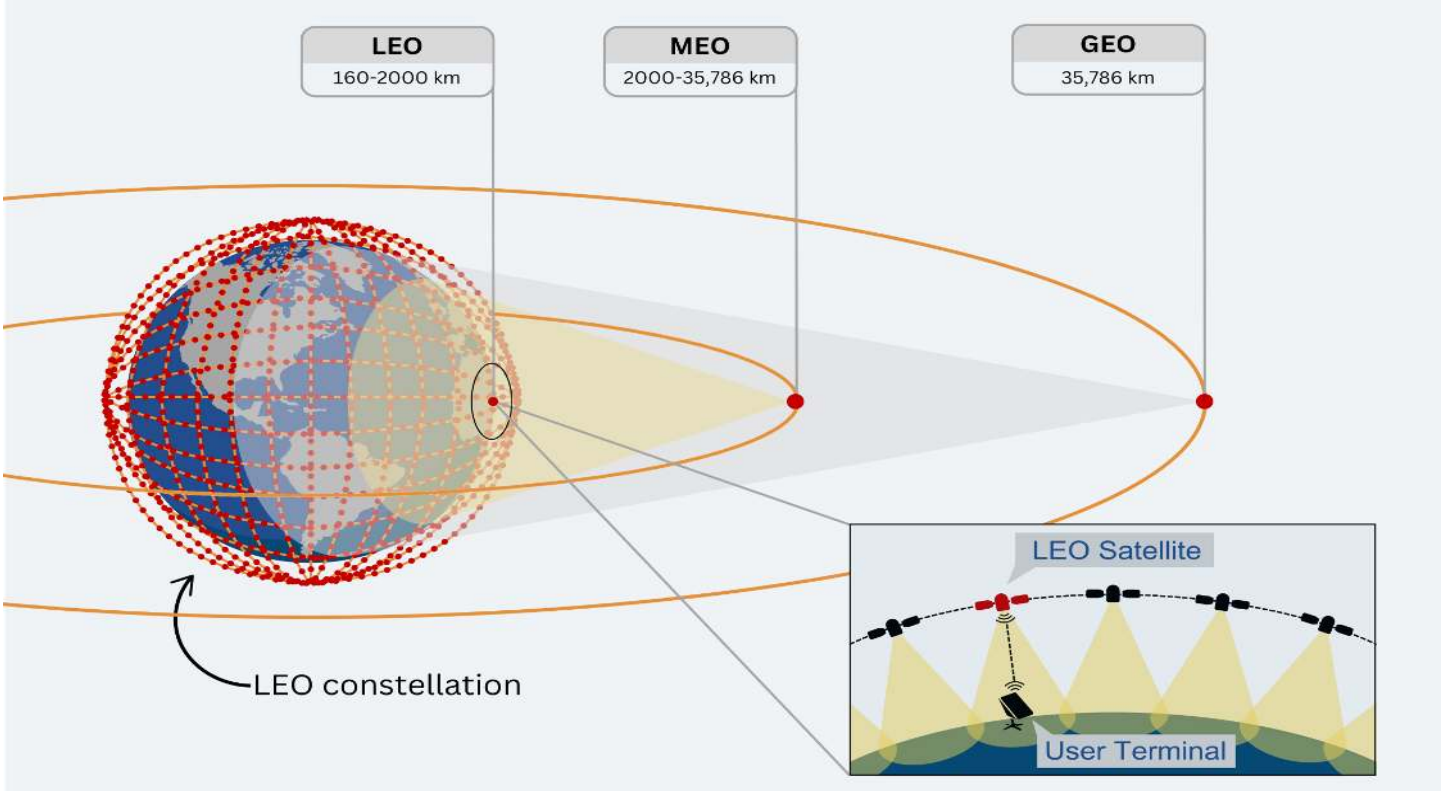


Figure 1: Orbits and LEO Constellations (own work)

MEO satellites are in constant motion relative to the surface. In particular, LEO satellites circle the earth multiple times per day, staying in view of a given location for about 10 minutes.

In contrast, GEO satellites remain permanently fixed above the same ground location by

2.2 Satellites as Critical Infrastructure and Key Defence Assets

Over the years, satellite services have become essential for numerous societal functions such as aviation, maritime traffic, weather forecasting,

agriculture, government communications, search and rescue, and broadcasting. The indispensable role that they exert in maintaining the functionality of other systems and societal functions places satellites in the category of critical infrastructures (CIs). As such, they are increasingly included in special national protection frameworks to safeguard national security (Froehlich, 2021; Schrogl, 2020).

It is important to distinguish between national security, which largely describes the ability of a state to protect its citizens from various threats, and defence, a specific aspect of national security focused on protecting the nation from external military threats (Osisanya, n.d.). Satellites have also long fulfilled defence applications, including providing secure military communications, navigation, targeting guidance, and perhaps most famously, reconnaissance. Reconnaissance satellites may monitor enemy military activities, intercept foreign communications, and detect ballistic missiles (Pelton & Madry, 2020).

2.3 Proliferation of LEO Mega-Constellations in the Age of Commercial Space

Breaking with the traditional dominance of GEO satellite systems in satellite communications, a growing number of companies are now developing LEO satellite constellations to provide global broadband internet services. As of 2023, around 33 percent of the global population remained offline, largely due to the lack of internet access in rural areas and least-developed countries (ITU, 2023). This digital divide is attributed to the limited coverage of ground-based internet infrastructure and GEO internet satellites. Despite handling the majority of global internet traffic, ground-based infrastructure is challenging and expensive to build in remote areas. Conversely, GEO satellites can transmit internet signals directly from orbit but are limited by low speed, high latency, and high service prices (Young & Thadani, 2022). Capitalising on mass-market appeal and economies of scale, LEO constellation operators intend to make significant profits by offering affordable, high-quality internet in underserved areas. Thanks to their low orbital altitude, LEO constellations can provide global coverage with download speeds reaching up to 250 megabits per second (Mbps), and as low as 25 milliseconds of latency – compared to 600 milliseconds for GEO satellites- (Starlink, n.d; Young & Thadani, 2022). However, because individual LEO satellites cover a smaller area, achieving similar coverage in LEO requires a significantly larger number of satellites (Figure 1). For instance, the Starlink constellation comprised more than 6000 satellites in September 2024 (Pultarova et al., 2024;). Due to their sheer scale, LEO constellations are often referred to as "mega-constellations" (Hallex & Cottom, 2020). Satellites are linked to one another using lasers, while user terminals on the ground continuously connect with the nearest passing satellite (Satariano et al., 2023).

The deployment of such large constellations today has been made possible by a combination of recent developments in the commercial space sector. From the 2000s, the emergence of a new US private aerospace industry known as NewSpace has set focus on developing low-cost space technology and improving access to space. Led by companies such as SpaceX and Blue Origin, NewSpace has brought about an increased number of launch providers and more efficient launch vehicles like the reusable Falcon 9 rocket, driving down the costs of space launch. (Pelton & Madry, 2020; Young & Thadani, 2022). A similar development of the commercial space sector is occurring outside the US, as nations like China are increasingly investing in private space enterprises to develop their own space industries. Reflecting these trends, the number of proposals for mega-constellations has grown considerably in the past few years (Figure 2).

Beyond providing commercial internet service, LEO constellations hold significant potential for security and defence applications.

Their Broadband capabilities enable the provision of timely military communications in any location worldwide and the relay of large amounts of intelligence data. If outfitted with specific satellite payloads, LEO constellations could also perform enhanced global remote sensing and missile detection tasks. Above all, their large numbers of easily replaceable satellites increase resilience against attacks. (Young & Thadani, 2022; Pelton & Madry, 2020). In light of the strategic advantages that LEO constellations could confer to nations and private entities that deploy them, their proliferation introduces new security implications globally.

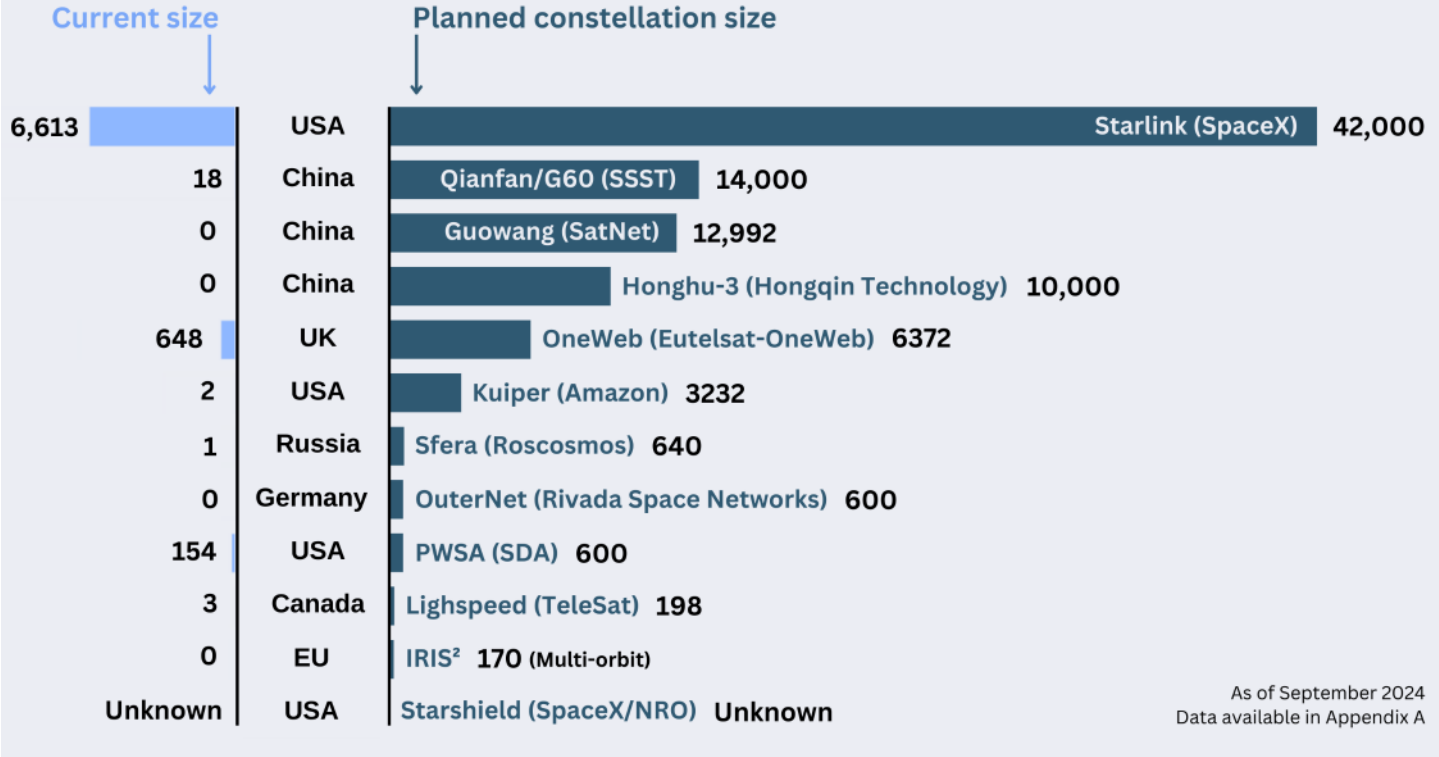


Figure 2: Current LEO Constellations in Development (own work, layout inspired by Voelsen (2021))

2.4 The Relevance of the Space Domain and LEO Constellations for EU Strategic Autonomy

Exemplified by the proliferation of LEO mega-constellations, rapid developments in the space domain have prompted reactions from the European Union in recent years, positioning EU space policy as an important element for achieving strategic autonomy. The concept of EU strategic autonomy widely describes the ability of the union to act autonomously and protect its interests in diverse sectors such as trade, foreign policy, technology, defence, and security without being restrained by dependencies on foreign actors (Helwig & Sinkkonen, 2022; Zhang et al., 2022). Today, space has become increasingly relevant to EU strategic autonomy within the fields of security and defence for several reasons. Since space infrastructures like satellites are essential enablers for numerous societal functions and military activities, developing homegrown space assets is critical to ensure autonomous security and defence capabilities. For instance, the existing Galileo MEO constellation provides an independent navigation system for civil and military applications, reducing member states' reliance on the US's GPS, Russia's GLONASS, or China's Beidou systems (Cellerino, 2023; Radhakrishnan et al., 2016).

Besides, the current geopolitical context of power competition between China, the US, and Russia – which each possess anti-satellite (ASAT) weapons – is fueling a race to develop advanced military capabilities in space. Lastly, the EU still lacks effective launch capabilities and risks being

increasingly dependent on external actors for its access to space (Harrison, 2024; Küsters et al., 2024; UN, 2023). Overall, these developments are pressuring the union to develop its security and defence capabilities in space, improve its launch capabilities, and protect its space assets from external threats.

To this end, the European Commission and the High Representative introduced the first-ever EU space strategy for security and defence in March 2023. Among others, the joint communication calls for the development of new EU launchers to ensure autonomous access to space. It also mentions the commission's intent to exploit upcoming LEO constellations for military capabilities. Crucially, it sets as an objective the deployment of IRIS², a sovereign multi-orbit constellation (Council of the European Union, n.d.; European Commission, 2023). These measures suggest that the bloc is carefully considering the global proliferation of mega-constellations as it lays down its plan for achieving strategic autonomy.

Against this backdrop, this article unravels the various implications that the said proliferation holds for EU strategic autonomy in security and defence. The subsequent sections discuss different LEO constellation initiatives and assess how they may impact the EU's ability to act autonomously and protect its interests in the two fields. The decision to focus on constellations from the US and China stems from the fact that both countries are currently at the forefront of LEO mega-constellations development (Figure 2). Moreover, the current debate on EU strategic autonomy is driven by the growing rivalry between the two geopolitical powers, which exposes the EU to security challenges and limits its ability to implement its foreign policy (Helwig & Sinkkonen, 202).

3. Discussion

3.1 Starlink and US Military Constellations

SpaceX's Starlink is the first commercially successful LEO mega-constellation. By May 2024, it provided high-speed internet to more than three million customers in 99 countries worldwide (Alvarez, 2024). Users connect to the constellation through a small terminal that can be set up in minutes and managed via an app.

Far ahead of any competitor on the market, Starlink's unique capabilities have proven groundbreaking in critical civilian and military applications throughout the Russo-Ukrainian war. SpaceX dispatched thousands of Starlink terminals to Ukraine shortly after the start of the invasion to restore connectivity where Russian troops had disabled telecommunication infrastructure (phone lines, cell towers, ground stations, fibre optic lines, and broadcasting antennas) (Bergengruen, 2022; Jayanti, 2023). Thanks to its independence from ground infrastructure, Starlink's service has remained unaffected by Russian attacks. Moreover, its low-cost and user-friendly hardware has allowed for easy adoption and deployment while its high number of satellites and terminals has rendered jamming particularly challenging. Lastly, such advantages have been further compounded by high-speed, low-latency connection, portable and compact terminals, and remote connectivity capabilities (Jayanti, 2023; Kaushik & Selvamurthy, 2023). This combination of features fostered a swift adoption of the satellite service in hospitals, aid organisations, schools, and businesses (Jayanti, 2023). Above all, Starlink was adopted by the Ukrainian military, enabling real-time communication between command centres and frontline units operating in areas lacking telecommunications. Ukrainian units have also commonly used Starlink's broadband to deploy a large number of drones over vast swathes of territory, performing reconnaissance missions and dropping explosives on enemy positions (Wiedemar, 2023; Davis, 2022). Besides the growing use of autonomous systems, the conflict has seen an increase in the processing of battlefield intelligence. Large amounts of data – including satellite images and GPS coordinates of Russian troops – have been shared by earth observation companies through Starlink's broadband connection and fed into

military software providing intelligent battlefield management. For instance, the software GIS Arta coordinates Ukrainian artillery strikes based on field information. Kyiv also relies on Palantir's Metaconstellation, an AI software that detects military targets and predicts their movements from satellite images (Giles, 2023; Wiedemar, 2023).

Russia's continued targeting of communication infrastructure has reportedly made Starlink the only internet service left in Ukraine. With some 42,000 terminals in use in the region, it has become vital for Ukrainian military operations and civilian life (Abels, 2024; Reuters, 2024). This dependency has raised concerns about Ukraine's sovereignty over its military capabilities, considering that Starlink is controlled by SpaceX, a private company owned by US billionaire Elon Musk. Notably, SpaceX has continuously disabled Starlink service in Russian-occupied areas and outside Ukrainian borders using geofencing. In February 2023, it imposed further restrictions on usage for offensive military purposes such as drone control (Abels, 2024; Giles, 2023). These restrictions have hampered Ukrainian efforts to retake territory and contributed to the freezing of the conflict. Although the aerospace company has justified its service restrictions as a response to Starlink's unanticipated weaponisation violating its terms of service, its motives as a private actor remain opaque. Indeed, the company may have been aiming to avoid becoming a party to the conflict following Russian threats of ASAT retaliation against private space infrastructure supporting Ukraine (Abels, 2024; Boley & Byers, 2024; Giles, 2023; Wiedemar, 2023). Dependence on Starlink as a critical communication infrastructure is not limited to Ukraine. The constellation has become essential in Brazil's Amazon region, where it operates 70,000 terminals in more than 90% of municipalities. There, isolated communities, schools, hospitals, and even illegal mining compounds rely on its extensive broadband coverage for their communications. Moreover, the Brazilian Ministry of Defence has recognised Starlink as key to Brazil's defence operations. The service is indeed used by the military for command and control, particularly in communicating with remote bases and border platoons (Alvarez, 2023; Phillips & Milmo, 2024). Such a situation is problematic for Brazil's national security given the considerable leverage granted to a private company.To mitigate reliance on private infrastructure such as Starlink for defence, the US Space Force's Space Development Agency (SDA) is deploying its own LEO military constellation while maintaining collaboration with the commercial sector. Known as the Proliferated Warfighter Space Architecture (PWSA), the satellite network is set to consist of different layers, including a tracking layer for remote sensing and missile warning, and a transport layer providing high-speed communications and battlefield management. The transport layer will be capable of connecting to private constellations for third-party services while maintaining control over operations (Abels, 2024; Young & Thadani, 2022). Furthermore, the US National Reconnaissance Office (NRO) contracted SpaceX in 2021 to develop Starshield, a military LEO constellation designed specifically for global remote sensing and defence communications (Roulette & Taylor, 2024; SpaceX, n.d.). Establishing efficient satellite services in LEO thus appears to be a priority for the US as it seeks to become a dominant military power in space.

3.2 China's Answer to Starlink

While Starlink's recent success has occupied the spotlight, interest in LEO constellations extends beyond the United States. China, in particular, has been pursuing its own LEO constellation projects to provide global broadband internet access. In March 2020, the Chinese government announced plans to launch a constellation named Guowang. Managed by the state-owned China Satellite Network Group (SatNet), it will consist of 12,992 satellites in LEO (Suess, 2023; Young & Thadani, 2022). Guowang is one of three main Chinese mega-constellation projects as of September 2024, alongside Qianfan

Figure 3: Ukrainian Soldier Setting Up a Starlink Terminal (Attribution: Mil.gov.ua)

("Thousand Sails", previously G60) and Honghu-3. Qianfan, Led by Shanghai Spacecom Satellite Technology and supported by Shanghai's municipal government, launched the first 18 of its 14,000 planned satellites in August 2024. Honghu-3, led by Hongqing Technology, aims to deploy 10,000 satellites at term (Jones, 2024; Page, 2024). These initiatives receive significant support from the Chinese Communist Party and benefit from the rapid development of China's commercial space sector, which is expected to deliver the necessary growth in launch capacity to deploy thousands of satellites into space.

China may have several motives for financing LEO constellation projects, one of them being the commercial opportunity these offer. Despite its success, Starlink is awaiting government approval to operate in dozens of countries across Africa, Central Asia, and South Asia, and is unavailable in Syria, Russia, China, Iran, Afghanistan, Belarus, and North Korea (Starlink, n.d.). SpaceX's satellite service has faced criticism from authoritarian regimes for bypassing the traditional ground-based infrastructure that they control to censor information (Satariano et al., 2023).

As such, several governments hesitate to authorise its operation within their borders, preferring to maintain tight control over internet access. These circumstances present an opportunity for Chinese constellations to introduce competing services on the international market. Indeed, China is known for conducting business with authoritarian regimes, but also with emerging markets as part of its Belt and Road Initiative (BRI) (Hallex & Cottom, 2020).

BRI programs such as the Digital Silk Road (DSR) assist member states in developing their communications infrastructure. Under the BRI's Space Information Corridor, Beijing has signed over 117 space cooperation agreements with more than 37 governments to share its space infrastructure and provide communication services. (Young & Thadani, 2022).

Today, a substantial part of the digital infrastructure in several BRI countries is Chinese-built. This is particularly true in Africa, where

Huawei has built an estimated 70% of the continent's 4G infrastructure (Suess, 2023).

For compatibility reasons, these countries may find it easier and more cost-efficient to integrate Chinese LEO Broadband services into their existing network. Concurrently, further BRI agreements could help Chinese LEO broadband providers secure markets in Africa, Asia, and Latin America, potentially pushing out Western providers (Suess, 2023).

Beyond securing China's position in the satellite internet market, this strategy could serve its soft power interests. Beijing has previously provided several DSR countries with digital surveillance technologies to enhance their online censorship capabilities. In addition, the use of Chinese-built digital infrastructure comes with regulatory compliance requirements, often causing recipient countries to adopt Chinese data governance practices and restrict their social media landscape (Young & Thadani, 2022). The emergence of Chinese LEO constellations as internet suppliers could amplify the dependency of BRI countries on Chinese ICT technologies, exacerbating these trends. A Chinese state-backed satellite internet service with centralised infrastructure would enable client governments to more easily monitor information within their country's borders and filter politically sensitive content. It could also further spread China's authoritarian internet governance model, as countries seeking access to satellite broadband connectivity might be pressured into aligning with regulatory requirements and censoring content critical of China (Page, 2024; Young & Thadani, 2022). Eventually, a successful proliferation of Chinese LEO broadband constellations could grant China greater control over global information flows and improved intelligence capabilities.

As China seeks to assert its power in the space sector, its military has noted the strategic significance of LEO constellations (Young & Thadani, 2022).

Considering the Chinese government's tendency to integrate civilian and military resources, constellation projects such as Guowang or Qianfan constitute likely candidates for

Figure 4: Launch of a Chinese Long March 6A rocket - The Same Launcher Model Was Used to Send the First 18 Qianfan Satellites in Orbit on August 6, 2024 (Attribution: ecns.cn)

providing military capabilities like global high-speed communication and surveillance (Hallex & Cottom, 2020). At the same time, the superpower has sought to prevent Taiwan from acquiring LEO broadband internet.

In 2023, Taipei began pursuing such services to safeguard its information infrastructure and ensure connectivity in case of Chinese invasion.

This came after Chinese vessels were accused of damaging two undersea cables supplying internet to the Matsu islands, isolating their residents. Subsequent talks with SpaceX to access Starlink were ended by concerns that Elon Musk might face economic pressure from Beijing to shut down the service on request, and Taiwan eventually turned to British operator Eutelsat OneWeb (Khalaf, 2022; Satariano et al., 2023).

3.3 Strategic Implications for the European Union

As illustrated by the discussed cases, the emergence of proliferated LEO constellations introduces new sets of opportunities and risks that may impact the ability of the EU to act autonomously and protect its interests in security and defence. Unlike the United States and China, the EU currently lacks the necessary launch capabilities offered by cost-effective, heavy-lift, and reusable launchers to deploy large constellations in LEO. For context, in 2023, the US achieved the world's highest launch rate at 109 launches, 90% of which were conducted by SpaceX. China followed with 67 launches, while the EU recorded only 3 (Kuhr, 2024). Looking ahead, the bloc risks being increasingly reliant on foreign launch providers if it does not improve its independent access to space. As observed with Starlink in Ukraine and Brazil, dependence on private infrastructure can undermine sovereignty and national security. Satellite operators obtain significant political leverage, which could limit the EU's ability to enact its policies. Moreover, decisions made by corporate executives like Musk can arbitrarily affect the availability of internet services, threatening the reliability of the communication infrastructure. A private operator could also influence EU common security and defence policy by moderating or shutting down its satellite services in conflict zones depending on the threat posed to its assets. Similarly, relying on future US state-owned LEO constellations such as PWSA and Starshield would perpetuate a situation of dependence on the superpower for military capabilities. Decisions upon service provision would likely be taken by Washington, and the EU may be pressured to align with US foreign policy goals. Currently, this deadlock is well illustrated by Ukraine's extreme reliance on Starlink and by the lack of alternative European LEO internet services to independently counter regional security threats such as Russia's invasion of Ukraine. The invasion also pointed out the growing military importance of space systems and LEO constellations, particularly for AI-enabled battlefield management.

This trend is turning space into a warfighting domain as satellites are becoming more relevant targets for retaliation (Davis, 2022). Given its reliance on a small number of satellites highly vulnerable to ASAT weapons, EU space infrastructure is exposed to heightened threats it is not equipped to face.

The proliferation of Chinese LEO constellations brings yet another negative prospect for EU strategic autonomy. If China integrates its future constellations with the BRI and DSR, it could exert greater influence over international communication networks, fostering the spread of its authoritarian internet governance model. China's increased involvement in the field of communications has already sparked security concerns in the EU. A lengthy debate on the integration of Chinese-built equipment in European 5G infrastructure started in 2018 following US allegations that the Chinese government could obtain backdoor access to Huawei and ZTE networks.

Eventually, several EU countries restricted or banned telecom equipment from the two vendors (Cerulus, 2020; Reuters, 2023). Currently, Czechia, Hungary, Poland, and Estonia

participate in the DSR and have received Chinese investments in digital infrastructure (Council on Foreign Relations, n.d.). As the EU faces high demand for broader, affordable broadband coverage, alternative offers to Starlink could expose the bloc to a similar dilemma as with 5G infrastructure, possibly compromising its connectivity network.Brussels seems well aware of the challenges presented by foreign-proliferated LEO constellations. In November 2022, it initiated a program to deploy the Infrastructure for Resilience, Interconnectivity and Security by Satellite (IRIS²), a sovereign communication constellation. The constellation is planned to have 170 satellites following a multi-orbit architecture (GEO, MEO, and LEO) operable with other systems. Developed via a public-private partnership, the program will involve Airbus, SES, Eutelsat, Hispasat, and Thales Alenia. The consortium is expected to contribute €3 billion of an estimated €6 Billion total cost, splitting investments and benefits between the EU, member states, and private companies (ESPI, 2022; European Commission, n.d.; SES, 2023). Embracing a dual-use approach, IRIS² will in turn deliver high-speed, low-latency secure internet to both governmental and commercial users. On the one hand, it will support border surveillance, crisis management, military missions, and connectivity in key infrastructures such as EU embassies. On the other hand, it will provide internet to EU citizens and private businesses for mass-market applications. With a full constellation planned for 2027, IRIS² constitutes a limited yet strategic response to current LEO constellation projects (European Commission, n.d.; EUSPA, 2024).Although the completion of IRIS² remains uncertain, developing a sovereign LEO constellation and leveraging commercial LEO services offers opportunities to strengthen the EU's strategic autonomy. As seen in Ukraine, an important benefit of Starlink-like systems is their ability to maintain connectivity when ground infrastructure is damaged. Presently, 95% of global internet traffic between regional networks goes through a network of high-performance undersea cables. This backbone transmits everything from financial transactions to encrypted government communications (Runde et al., 2024). Despite their strategic importance, subsea cables lie highly exposed to accidental damage and sabotage on the ocean floor.

Russia has shown a willingness to exploit this vulnerability to disrupt Western communications and Russian vessels have previously been suspected of sabotage in the Baltic Sea (Page, 2023). This is especially concerning for the EU, which relies on Atlantic undersea cables to access a significant portion of its data stored in US data centres (Wall & Morcos, 2021). In this context, a constellation such as IRIS² could complement cable-based internet, providing a contingency to the EU in case of damage to its ground infrastructure (Hallex & Cottom, 2020). Most importantly, the EU has long sought to build up its military capabilities through initiatives for defence cooperation and industry innovation. The invasion of Ukraine has raised awareness about European defence and has seen Many member states increasing their defence budget and investing in new technologies (EDA, 2024). Within this scope, the deployment of homegrown LEO constellations is particularly relevant. The powerful impact of Starlink in Ukraine demonstrates that such systems can work as force amplifiers, increasing the resilience of critical infrastructure and the effectiveness of military operations. In turn, they further demonstrate a potential to strengthen the EU's strategic autonomy.

4. Conclusion

Today, the majority of low earth orbit constellation projects remain in the early stages of development. But while the United States and SpaceX enjoy a significant head start with Starlink, the emergence of other constellations is set to empower upcoming operators, be it governments or private companies. Indeed, such space systems promise not only to redefine the connectivity landscape by providing worldwide broadband internet service but also hold

significant potential for security and defence applications. Their development is therefore of significant relevance for the European Union, which faces a pressing need to improve its autonomous defence capabilities, develop its space launch sector, and protect its space assets from external threats. The proliferation of Low Earth Orbit (LEO) constellations thus introduces new opportunities and risks that may impact the bloc's capacity to act autonomously and protect its interests in security and defence.

Above all, if the EU fails to deploy a sovereign constellation, it risks becoming reliant on non-EU systems for critical security and defence applications. Relying on a private constellation like Starlink, whose service is subject to moderation, or a foreign state-owned one such as the US-planned Proliferated Warfighter Space Architecture (PWSA), would threaten the reliability of communications and the ability of the EU to enact independent policies and operations. Another negative prospect for EU strategic autonomy comes with the proliferation of Chinese LEO constellations. Through integration with the Belt and Road Initiative and Digital Silk Road programs, these systems could give China greater control over international data flows. Possible integration of CCP-backed LEO broadband services into the connectivity network of EU countries introduces risks of sabotage and spying, possibly compromising these networks. On the other hand, LEO services offer opportunities to strengthen the EU's strategic autonomy. LEO constellations can complement cable-based internet by providing a contingency in case of damage to ground communications and have greater resilience against attacks due to their large numbers of satellites. This capability is strategically relevant to the EU as the bloc relies on undersea internet cables exposed to damage and sabotage.

If the EU fails to deploy a sovereign LEO constellation, it risks becoming reliant on non-EU constellations for critical security and defence applications.

Lastly, an LEO constellation could amplify EU military capabilities by enabling high-speed military communications and data transfer, and global remote sensing. These capabilities are important in the current context of autonomous and AI-enabled warfare. Against this backdrop, it remains to be seen whether the EU will succeed in developing its space industry and launching IRIS², and whether the latter will deliver sufficient capabilities. Because of the tremendous increase of satellites launched in orbit, proliferated LEO constellations are also sparking increasing concerns about risks of collisions, space debris, and interference with astronomical observations.

Although such issues fall outside the scope of this article, it is important to consider the spillover impacts on space security that LEO constellations may cause and the need for new international regulations to ensure the long-term sustainability of space activities.

References

Abels, J. (2024). Private infrastructure in geopolitical conflicts: the case of Starlink and the war in Ukraine. European Journal of International Relations, 0(0), 1-25. https://doi-org.ezproxy.leidenuniv.nl/10.1177/13540661241260653

Alvarez, S. (2023, August 31). Starlink a key technology for Brazil's military: Department of Ministry letter. TESLARATI. https://www.teslarati.com/starlink-key-technology-brazil-military-department-of-ministry-letter/

Alvarez, S. (2024, May 21). Starlink celebrates new milestone: 3 million customers in 99 countries. TESLARATI. https://www.teslarati.com/starlink-celebrates-3-million-customers-99-countries/

Kaushik, R. & Selvamurthy, W. (2023). Starlink's role in Ukraine: Portent of a space war? Manohar Parrikar Institute for Defence Studies and Analyses Journal of Defence Studies, 17(1), 25–44. https://www.idsa.in/jds/17-1-2023-Starlink-Role-in-Ukraine

Bergengruen, V. (2022, October 18). The battle for control over Ukraine's internet. TIME. https://time.com/6222111/ukraine-internet-russia-reclaimed-territory/

Boley, A., & Byers, M. (2024). Anti-satellite weapon tests to disrupt large satellite constellations. Nature Astronomy, 8, 10–12. https://doi.org/10.1038/s41550-023-02173-

Brito, R., & Magalhaes, L. N. (2024, September 3). Starlink emerges as fresh battleground between Musk, Brazil. Reuters. https://www.reuters.com/technology/brazils-supreme-court-chamber-forms-majority-uphold-x-suspension-2024-09-02/

Congressional Budget Office (CBO). (2023). Large Constellations of Low-Altitude Satellites: A Primer. https://www.cbo.gov/publication/58794

Council on Foreign Relations. (n.d.). Assessing China's Digital Silk Road Initiative. https://www.cfr.org/china-digital-silk-road/

Council of the European Union. (n.d.). EU space policy. Retrieved September 8, 2024, from https://www.consilium.europa.eu/en/policies/eu-space-programme/#why

Cellerino, C. (2023). EU space policy and strategic autonomy: Tackling legal complexities in the enhancement of the 'security and defence dimension of the Union in space'. European Papers, 8(2), 487-501. https://doi.org/10.15166/2499-8249/669

Cerulus, L. (2020, May 26). Trump and friends: Where European countries come down on Huawei. Politico. https://www.politico.com/news/2020/05/26/europe-huawei-5g-281701

Daehnick, C., Hamill, R., Ménard, A., & Wiseman, B. (2022, August 11). Is there a 'best' owner of satellite internet? McKinsey & Company. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/is-there-a-best-owner-of-satellite-internet

Damen, M. (2022). EU strategic autonomy 2013-2023: From concept to capacity. European Parliamentary Research Service. https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733589

Davis, M. (2022). The implications of commercial space: From enabling military capability to introducing new dynamics into competition. The Air Power Journal. https://theairpowerjournal.com/the-implications-of-commercial-space-from-enabling-military-capability-to-introducing-new-dynamics-into-competition/

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2023, March 10). European Union Space Strategy for Security and Defence (JOIN(2023) 9 final). https://ec.europa.eu/transparency/documents-register/detail?ref=JOIN(2023)9&lang=en

European Commission. (n.d.). EU space strategy for security and defence. Retrieved September 8, 2024, from https://defence-industry-space.ec.europa.eu/eu-space/eu-space-strategy-security-and-defence_en

European Commission. (n.d.). IRIS²: The new EU secure satellite constellation: Infrastructure for resilience, interconnectivity and security by satellite. Retrieved September 8, 2024, from https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

European Defence Agency (EDA). (n.d.). "Ukraine war confirms need to define a long-term strategy to ensure the defence of Europe." Retrieved September 20, 2024, from https://eda.europa.eu/webzine/issue23/interview/ukraine-war-confirms-need-define-long-term-strategy

European Space Policy Institute (ESPI). (2022). IRIS2: The new (material) girl on the block (Brief No. 61). https://www.espi.or.at/briefs/iris2-the-new-material-girl-on-the-block/

European Union Agency for the Space Programme (EUSPA). (2024, April 26). IRIS². Retrieved from https://www.euspa.europa.eu/eu-space-programme/secure-satcom/iris2

Evroux, C., Heflich, A., & Saulnier, J. L. (2023). Towards EU leadership in the space sector through open

strategic autonomy: Cost of non-Europe (PE 734.691). European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/STUD/2023/734691/EPRS_STU(2023)734691_EN.pdf

Froehlich, A. (Ed.). (2021). Legal aspects around satellite constellations: Volume 2. Cham, Switzerland: Springer. http://dx.doi.org/10.1007/978-3-030-71385-0

Giles, K. (2023). Russian cyber and information warfare in practice: Lessons observed from the war on Ukraine. Chatham House, 0-61. https://doi.org/10.55317/9781784135898.

Hallex, M. A., & Cottom, T. S. (2020). Proliferated commercial satellite constellations: Implications for national security. Joint Force Quarterly, 97, 20-29. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2106495/proliferated-commercial-satellite-constellations-implications-for-national-secu/

Harrison, T. (2024). Building an enduring advantage in the third space age. American Enterprise Institute. https://www.aei.org/research-products/report/building-an-enduring-advantage-in-the-third-space-age/

Harrison, T., & Strohmeyer, M. (2022). Commercial space remote sensing and its role in national security. Center for Strategic and International Studies. https://www.csis.org/analysis/commercial-space-remote-sensing-and-its-role-national-security

Helwig, N., & Sinkkonen, V. (2022). Strategic autonomy and the EU as a global actor: The evolution, debate and theory of a contested term. European Foreign Affairs Review, 27 (Special Issue), 1–20. https://doi.org/10.54648/EERR2022009

International Telecommunication Union. (2023). Measuring digital development: Facts and figures 2023. ITU Publications. https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/.

Jayanti, A. (2023, March 9). Starlink and the Russia-Ukraine War: A case of commercial technology and public purpose? Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/starlink-and-russia-ukraine-war-case-commercial-technology-and-public-purpose

Jones, A. (2022, February 17). Shanghai signs agreement with China's megaconstellation group, aims to foster commercial space hub. Space News. https://spacenews.com/shanghai-signs-agreement-with-chinas-megaconstellation-group-aims-to-foster-commercial-space-hub/

Jones, A. (2024, April 19). China to leverage growing commercial space sector to launch megaconstellations. Space News. https://spacenews.com/china-to-leverage-growing-commercial-space-sector-to-launch-megaconstellations/#:~:text=Nebula%2D1%20rocket.-,Company,-Rocket%20Name

Jones, A. (2024, August 6). China launches first satellites for Thousand Sails megaconstellation. Space News. https://spacenews.com/china-launches-first-satellites-for-thousand-sails-megaconstellation/

Khalaf, R. (2022, October 7). Elon Musk: 'Aren't you entertained?' Financial Times. https://www.ft.com/content/5ef14997-982e-4f03-8548-b5d67202623a

Kuhr, J. (2024, January 4). 2023 orbital launches, by country. Payload. https://payloadspace.com/2023-orbital-launches-by-country/

Küsters, A., Nolen, N., & Stockebrandt, P. (2024, February 20). Strategic autonomy in EU space policy: Securing Europe's final frontier through launches, laws, and space mining. Center for European Policy cepInput, 4, 1-25. https://www.cep.eu/eu-topics/details/strategic-autonomy-in-eu-space-policy-cepinput.html

Osisanya, S. (n.d.). National security versus global security. UN Chronicle. Retrieved September 8, 2024, from https://www.un.org/en/chronicle/article/national-security-versus-global-security.

Page, M. (2023, October 31). Russia, a Chinese cargo ship and the sabotage of subsea cables in the Baltic Sea. The Strategist. https://www.aspistrategist.org.au/russia-a-chinese-cargo-ship-and-the-sabotage-of-subsea-cables-in-the-baltic-sea/

Page, M. (2024, August 26). China may be putting the Great Firewall into orbit. The Strategist. https://www.aspistrategist.org.au/china-may-be-putting-the-great-firewall-into-orbit/

Paraguassu, L., Benedito, L. M., & Brito, R. (2024, August 31). Brazil watchdog moves to block access to Elon Musk's X after court order. Reuters. https://www.reuters.com/technology/lula-says-musk-must-respect-brazils-top-court-x-braces-shutdown-2024-08-30/?taid=66d20650d8471d00018ff127&utm_campaign=trueAnthem:+Trending+Content&utm_medium=trueAnthem&utm_source=twitter.

Pelton, J. N., & Madry, S. (Eds.). (2020). Handbook of small satellites: Technology, design, manufacture, applications, economics and regulation. Cham, Switzerland: Springer.

Phillips, T., & Milmo, D. (2024, September 8). 'Can't live without it': Alarm at Musk's Starlink dominance in Brazil's Amazon. The Guardian. https://www.theguardian.com/technology/article/2024/sep/08/alarm-at-musk-starlink-dominance-brazil-amazon

Pultarova, T., Howell, E., Mann, A., & Dobrijevic, D. (2024, August 29). Starlink satellites: Facts, tracking and impact on astronomy. Space.com. https://www.space.com/spacex-starlink-satellites.html.

Radhakrishnan, R., Edmonson, W. W., Afghah, F., Martinez Rodriguez-Osorio, R., Pinto, F., & Burleigh, S. C. (2016). Survey of inter-satellite communication for small satellite systems: Physical layer to network layer view. IEEE Communications Surveys and Tutorials, 18(4), 2442–2473. https://doi.org/10.1109/COMST.2016.2564990

Reuters. (2024, February 15). Russia using thousands of SpaceX Starlink terminals in Ukraine, WSJ says. Reuters. https://www.reuters.com/world/europe/russia-using-thousands-spacex-starlink-terminals-ukraine-wsj-says-2024-02-15/

Reuters. (2023, September 29). European countries who put curbs on Huawei 5G equipment. Reuters. https://www.reuters.com/technology/european-countries-who-put-curbs-huawei-5g-equipment-2023-09-28/

Roulette, J., & Taylor, M. (2024, March 16). Exclusive: Musk's SpaceX is building spy satellite network for US intelligence agency, sources say. Reuters. https://www.reuters.com/technology/space/musks-spacex-is-building-spy-satellite-network-us-intelligence-agency-sources-2024-03-16/

Runde, D. F., Murphy, E. L., & Bryja, T. (2024, August 16). Safeguarding subsea cables: Protecting cyber infrastructure amid great power competition. Center for Strategic and International Studies. https://www.csis.org/analysis/safeguarding-subsea-cables-protecting-cyber-infrastructure-amid-great-power-competition

Satariano, A., Reinhard, S., Metz, C., Frenkel, S., & Khurana, M. (2023, July 28). Elon Musk's unmatched power in the stars. The New York Times. https://www.nytimes.com/interactive/2023/07/28/business/starlink.html

Schrogl, K.-U. (Ed.). (2020). Handbook of space security: Policies, applications and programs (2nd ed.). Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-030-23210-8

SES. (2023, April 11). Building a secure resilient satellite infrastructure for Europe. https://www.ses.com/newsroom/building-secure-resilient-satellite-infrastructure-europe

SpaceX. (n.d.). Starlink. Retrieved September 29, 2024, from https://www.starlink.com/

SpaceX. (n.d.). Starshield: Supporting national security. Retrieved September 30, 2024, from https://www.spacex.com/starshield/

Starlink. (n.d.). Satellite technology. Retrieved September 8, 2024, from https://www.starlink.com/technology

Starlink. (n.d.). Starlink coverage map. Retrieved September 20, 2024, from https://www.starlink.com/map

Suess, J. (2023, May 3). Commentary: Guo Wang: China's answer to Starlink? The Royal United Services Institute (RUSI). https://rusi.org/explore-our-research/publications/commentary/guo-wang-chinas-answer-starlink

United Nations. (2023, October 19). Outer space becoming contested domain for supremacy with space-based communications, intelligence assets, anti-satellite weapons, First Committee hears. United Nations Press. https://press.un.org/en/2023/gadis3722.doc.htm

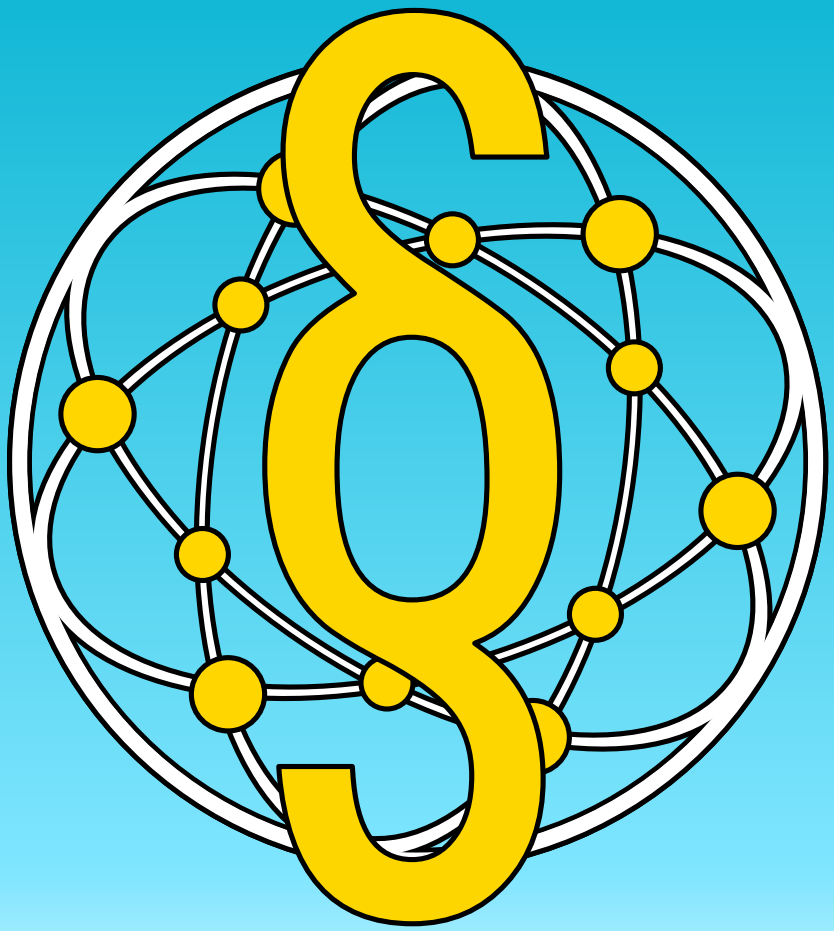
Voelsen, D. (2021). Internet from space: How new satellite connections could affect global internet governance. Stiftung Wissenschaft und Politik Research Paper 03, 0-31. https://doi.org/10.18449/2021RP03

Wall, C., & Morcos, P. (2021, June 11). Invisible and vital: Undersea cables and transatlantic security. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/invisible-and-vital-undersea-cables-and-transatlantic-security

Wiedemar, S. (2023). Nouvelles frontières de la militarisation de l'espace. CSS Analyses in Security Policy, 333, 1-4. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse333-FR.pdf

Young, M., & Thadani, A. (2022). Low orbit, high stakes: All-in on the LEO broadband competition. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/low-orbit-high-stakes

Zhang, J., Cai, Y., Xue, C., Xue, Z., & Cai, H. (2022). LEO mega constellations: Review of development, impact, surveillance, and governance. Space: Science & Technology, 2022, 1-17. https://doi.org/10.34133/2022/9865174



Sovereignty in Cyberspace

Is an International Cyber-Order Achievable?

Chloe Young

Chloe is a Juris Doctor student at the University of Washington School of Law. She graduated summa cum laude with degrees in Politics and Chinese from Whitman College. In 2024, she graduated with Distinction from the University of Glasgow (LLM in International Law), the Institut Barcelona d'Estudis Internacionals (MA in International Security), and the University of Tartu (MA in International Law and Human Rights). Chloe interned at the cyber diplomacy unit at the Estonian Ministry of Foreign Affairs.

1. Introduction

Every day, states, non-state actors, and individuals are exploiting vulnerabilities in cyberspace for political, ideological, or economic gain. For example, in 2007 the Estonian government witnessed thousands of distributed denial-of-service attacks which disabled the websites of government agencies, political parties, newspapers, and banks (Traynor, 2007). In 2014, the Pentagon repelled over thirty million cyberattacks directed towards government networks (Winnefeld et al., 2016). In 2022, the Costa Rican government declared a state of emergency after a widespread ransomware attack caused over $155 million worth of losses (Rosch, 2022). As the number of cyberattacks increases with widespread Internet accessibility and low costs of cyber operations, this heightens the importance of asking whether international consensus can be reached on how sovereignty applies in cyberspace (Franzese, 2009, 7).

Cyberspace:
Cyberspace comprises a physical, logical, and virtual environment whereby data and information are transported, accessed, and stored for communication purposes.

This legal problem must be addressed because state sovereignty "largely defines the current international order" and will likely lay the foundation for an international cyber-order (Liaropoulos, 2013, 21). Given this article's limited scope, other international legal principles like non-intervention and self-defence are not discussed. Although the definition of sovereignty varies among scholars, this article defines it as "the right of states to exercise exclusive authority over their territory" (Osula & Rõigas, 2016, 69). This article aims to understand disagreements between states over sovereignty's applicability to cyberspace. To achieve this goal, the article addresses the following three legal issues. Firstly, how does the borderless nature of cyberspace compare to other domains like the high seas, airspace, and outer space? Secondly, what should constitute a breach of sovereignty in cyberspace? Thirdly, how does anonymity in cyberspace complicate state attribution? This article contends that (1) the virtual side of cyberspace complicates traditional applications of territorial sovereignty but does not preclude states from exercising control over physical cyberspace infrastructure and activity within their borders, (2) violations of sovereignty should be determined individually based on the context of the violation and the severity of its effect, and (3) anonymity in cyberspace complicates state attribution but should not dissuade states from addressing violations in other ways.

To answer these questions, the article analyses national laws, international draft conventions and working group reports submitted to the United Nations (UN), and scholarly works like the Tallinn Manual. The article proceeds in four sections. Section one discusses three general challenges to cyberspace regulation. Section two outlines sovereignty's traditional role in the UN Charter and Tallinn Manual. Next, section three addresses three legal issues surrounding sovereignty in cyberspace. Finally, section four concludes by imploring states to unite and create a common understanding of how sovereignty applies in cyberspace to successfully address hostile cyber operations worldwide. Overall, this article argues sovereignty disagreements between states will make achieving consensus on an international cyber-order a daunting task.

2. Can Cyberspace be Regulated?

According to former Google CEO Eric Schmidt, "The Internet is the first thing that humanity has built that humanity doesn't understand, the largest experiment in anarchy that we have ever seen" (Singer & Friedman, 2014, 40). Since its humble beginnings as a U.S. government agency project, roughly fifteen billion devices worldwide are now connected to the Internet (Vailshery, 2023). By 2030, the number of connected

devices is expected to double as online banking, shopping, and working become more common (Vailshery, 2023). As the Internet steadily grows in popularity, this heightens the importance of asking whether cyberspace can be regulated. Each connected device contributes to an ever-expanding cyber domain susceptible to fraud, denial of service, scam, sniffing, brand spoofing, and other attacks. This article defines cyberspace as comprising a physical, logical, and virtual environment whereby data and information are transported, accessed, and stored for communication purposes. Cyberspace regulation is possible but difficult to achieve due to several challenges like the private sector controlling most of the Internet's physical infrastructure, anonymity in the dark web, and the quick speed at which events unfold in the virtual world. After briefly outlining the history of cyberspace regulation from an international perspective since the late 1800s, this section of the article briefly analyses these three main challenges to effective cyberspace regulation.

This introductory section concludes by arguing in favour of cyberspace regulation to protect users, maintain global commerce, and uphold human rights. To effectively analyse the challenges of cyberspace regulation, it is important to outline the history of cyberspace regulation from an international perspective. In 1865, the international community convened to set common standards for telegraph communication. This meeting culminated in the establishment of the International Telegraph Union, which later became the International Telecommunications Union (ITU) tasked with developing technical standards for international Internet connectivity. In addition to the ITU, other international organisations like the Internet Engineering Taskforce (which regulates standards for the Transmission Control Protocol and Internet Protocol) and the Internet Corporation for Assigned Names and Numbers (which manages IP address space allocation and the domain name system) regulate the technical side of cyberspace. However, recent scholarly projects and international treaties have addressed the legal side of cyberspace. For example, the Tallinn Manual is a scholarly project that explains how jus ad bellum (i.e., the laws governing the use of armed force and the conditions under which states may resort to war) and jus contra bellum (i.e., international humanitarian law) apply to cyberwarfare. Additionally, the Budapest Convention (2004) was the first international treaty regulating cyberspace by imploring member states to pass domestic legislation addressing hacking, the damage and breach of data, fraud, child pornography, copyright and more. Although cyberspace regulation has become a recurring discussion topic at international organisations like the UN, North Atlantic Treaty Organization (NATO) and European Union (EU), it still sparks strong debate among states. On the one hand, strong cyberspace regulations make it easier for some regimes to limit freedom of speech (as evidenced by China's Great Firewall, whereby the Chinese government monitors, controls, and filters the availability of certain websites from within its territorial boundaries.) On the other hand, cyberspace regulations are crucial for global commerce, communication, and national security. Recognizing the importance of balancing law enforcement efforts with human rights, this article supports cyberspace regulation but lists three of its main challenges. First, cyberspace is difficult to regulate because the private sector controls most of the Internet's physical infrastructure. Before diving into this ownership problem, it is important to define the Internet's relationship to the World Wide Web (WWW). The Internet refers to the physical infrastructure of computers, fiber-optic cables, routers, antennas, internet exchange points, and data storage centers worldwide which create a network of networks for connectivity. The WWW refers to the logical realm of cyberspace that provides a collection of information accessible via the Internet. In simpler terms, surfing the web refers to jumping from page to page using Hypertext Markup Language (HTML).

At the international level, organisations like the ITU, ICANN, and the World Trade Organization

provide technical standards and telecommunication regulations for online users. However, the private sector (at least in the U.S.) owns and controls roughly ninety percent of the Internet's physical infrastructure (Singer & Friedman, 2014, 40). Therefore, the government cannot regulate cyberspace on its own and prevent cybercrime without cooperating with private companies. This co-dependency illustrates how traditional conceptions of the government as the legitimate monopoly provider of security does not translate from the physical world to cyberspace. Additionally, the plurality of state, non-state, and private actors in cyberspace challenges international law's conception of the state as the most essential subject of international law. For these reasons, governments must work with the private sector to effectively regulate cyberspace.

Secondly, cyberspace is difficult to regulate because anonymity in the dark web complicates state attribution and accountability. It is important to note that the WWW's structure resembles an iceberg with three layers of depth: the clear, deep, and dark web. The clear web is the smallest part of the WWW where search engines like Google and Bing can roam freely. The second largest part of the WWW is the deep web, which search engines cannot find because passwords are needed for access. Schools, businesses, and companies generally take advantage of the deep web to ensure random users cannot access sensitive, internal information.

Finally, the largest part of the WWW is the dark web whereby people use the Tor browser to clear their browsing history and make themselves harder to track (Santi, 2023). Anonymity in the dark web complicates both law enforcement efforts and international law's ability to regulate cyberspace activity. According to Article 8 of the Articles of States Responsibility for Internationally Wrongful Acts (ARSIWA), "the conduct of a person or group of persons shall be considered an act of a State under international law if…[they] are in fact acting on the instructions

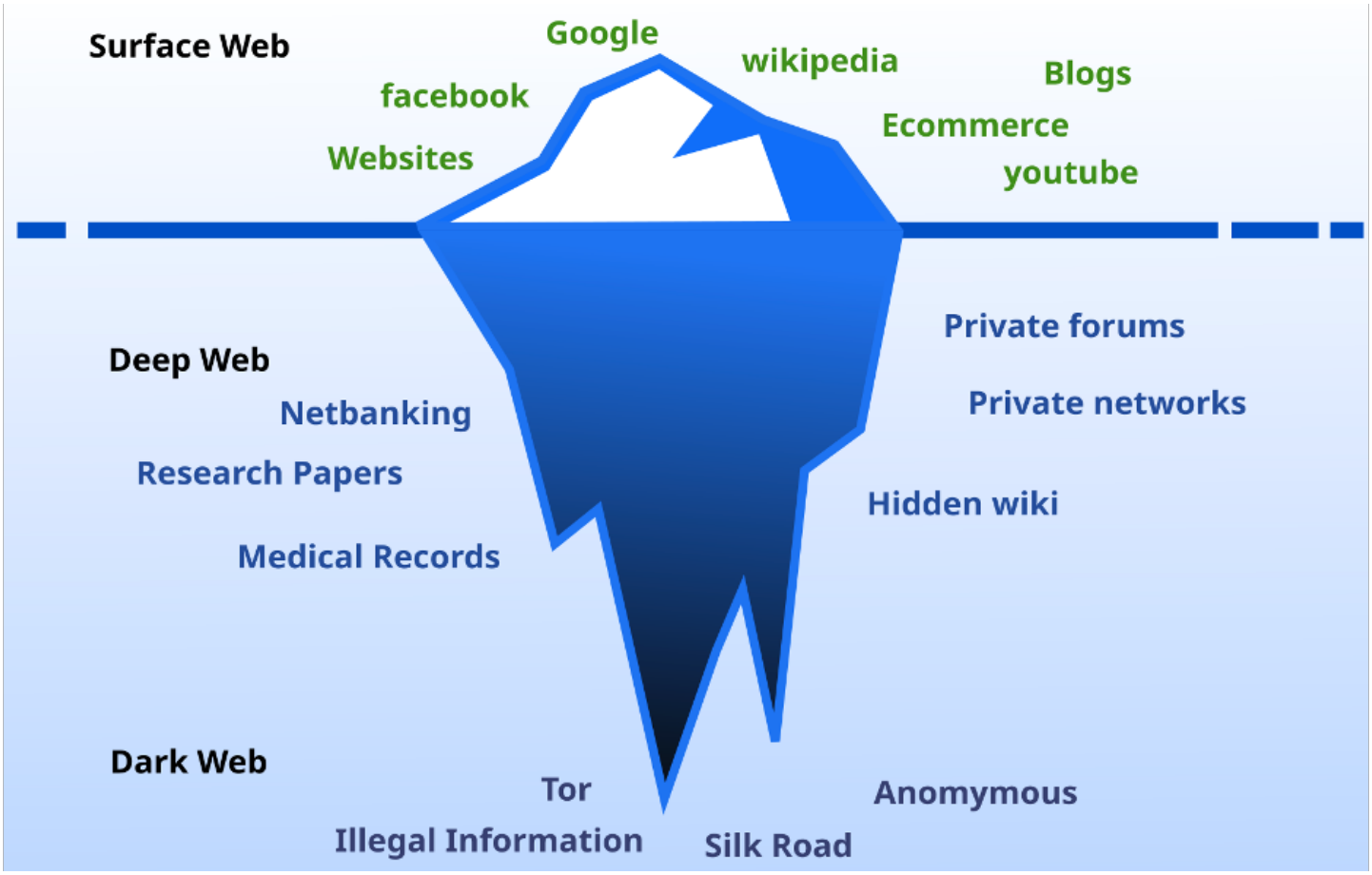


Figure 1:Graphical representation of surface web, deep web, and dark web (Ranjithsiji, 2018)

of, or under the direction or control of, that State in carrying out the conduct" (Draft Articles on Responsibility, art. 8). This effective control standard is nearly impossible to meet in cyberspace because people's identity and motives are oftentimes obscured. Even if law enforcement successfully tracked down a cybercriminal's IP address, the device's geolocation may not be authentic if it were re-routed from the cybercriminal's true location. Another complicating factor is whether the cybercriminal is controlling someone else's computer. Overall, challenges surrounding jurisdiction, state attribution, accountability, and "international law's traditional reliance on territorial borders" complicate efforts to effectively regulate cyberspace (Johnson and Post, 1996, 1367).

Thirdly, cyberspace is challenging to regulate because of the quick speed at which events unfold in the virtual world. As new devices hit the market, their lines of code contain hundreds of human error vulnerabilities ready for exploitation by cybercriminals.

Every second of every day, cybercriminals are tirelessly attempting to find coding vulnerabilities to make a profit, send political messages, and conduct cybercrime.

Given this fast-paced virtual environment, governments cannot keep up with cyberspace regulations due to limited budgets, staff, and expertise. For example, widespread ransomware attacks on the Costa Rican government (2022) forced the ministry to work with pen and paper for months until finding a solution.

Likewise in the United States, the SolarWinds IT management company suffered massive data breaches in 2019 when hackers slipped malicious code into a software update. The preliminary stages of this cyberattack went undetected for roughly two years (Zetter, 2023). These examples illustrate the difficulties of predicting and responding to cyber-attacks. Additionally, legislative solutions often require proposal, drafting, negotiation, implementation, and enforcement stages that span years. As cyberspace activity continues unfolding at the speed of light, the governments' ambition to craft quick legal solutions will remain unfeasible. In the meantime, governments should invest time and effort into strengthening their national resilience and implementing security defences in cyberspace to impede cybercriminals. Given these three challenges to effective cyberspace regulation, it is worth asking whether cyberspace should be regulated at all. For some, cyberspace should not be regulated because this paves the way for limiting freedom of speech and assembly. For example, John Barlow argued against government involvement by declaring "the global social space we are building [must] be naturally independent from the tyrannies [governments] seek to impose on us" (Barlow, 2018). However, to Barlow's dismay, the UN General Assembly (UNGA) accepted conclusions by the UN Group of Governmental Experts (GGE) in 2013 that international law and the principle of sovereignty applied to cyberspace (Moynihan, 2019). This consensus set the stage for states to develop national cyber security strategies to strengthen their cyberspace defence capabilities and resilience. In agreement with subsequent UNGA resolutions 70/237 and 73/27, this article supports cyberspace regulation to protect online users, maintain global commerce, and uphold human rights. Challenges surrounding anonymity and temporality in cyberspace heighten the importance of implementing cybersecurity measures and promoting social norms to regulate online behaviour to help prevent, deter, and respond to cyberattacks (Lessig, 2010, 124). Although avoiding all cyberattacks is unrealistic, passing security measures is an essential step towards making sure the Internet does not remain the largest experiment in anarchy that humanity has ever seen.

3. Sovereignty's Traditional Role in International Law

Before analysing several legal issues surrounding sovereignty in cyberspace, it is important to outline sovereignty's traditional role in international law. There are several types of sovereignty: domestic sovereignty (internal), interdependence sovereignty, international legal sovereignty (external), and Westphalia sovereignty (Liaropoulos, 2013, 22). The UN Charter enshrines external sovereignty and is "based on the principle of the sovereign equality [between] all its Members" (U.N. Charter art. 2, para. 1). The Charter also enshrines internal sovereignty by declaring "All members shall refrain in their international relations from the threat or use of force against the territorial or political independence of a state" (U.N. Charter art. 2, para. 4). Reinforcing the UN Charter's position, the International Court of Justice (ICJ) concluded "between independent states, respect for territorial sovereignty is an essential foundation of international relations" (Nicaragua v. United States of America, 1986).

Earlier on, the ICJ also addressed state sovereignty and argued British minesweeping in Albanian waters without the Albanian government's consent constituted a violation of sovereignty (United Kingdom of Great Britain and Northern Ireland v. Albania, 1949). Prior to the ICJ, the Permanent Court of International Justice (PCIJ) defined territorial sovereignty as a "situation recognized and delimited in space, either by so-called natural frontiers as recognized by international law or by outward signs of delimitation that are undisputed" (Netherlands v. USA, 1928). In this case, Arbitrator Huber implied territorial sovereignty confers rights and imposes obligations on states to respect each other's sovereignty (Netherlands v. USA, 1928, 858). Overall, sovereignty's traditional link to physical territoriality complicates matters in cyberspace because the virtual world is largely unconcerned with geographical boundaries. Although sovereignty is well-established in international law, cyberspace's "unprecedented novelty" sparks debate on its applicability (Osula & Rõigas, 2016, 49). In the early days of the Internet, an exceptionalist perspective emerged arguing cyberspace differed from previous domains regulated by international law (Osula & Rõigas, 2016, 49). For example, John Barlow argued "we must declare our virtual selves immune to [state] sovereignty" (Barlow, 2018).

Additionally, Kristen Eichensehr coined the phrase "cyberspace is sovereign" and argued cyberspace's opaque nature made it unconducive to state control (Eichensehr, 2014).

Over time, a competing sovereigntist viewpoint emerged which argued cyberspace remained fully under international law (Osula & Rõigas, 2016, 50). This article supports the sovereigntist viewpoint because if sovereignty is not applied to cyberspace, then states will continue acting in a wild west, lawless fashion with limited legal consequences. Although states may not want to tie their own hands with legal obligations, it is in their best interests to regulate cyberspace to ensure networks function properly, physical infrastructure remains protected, and relationships with the private sector are established. Supporting this position, the UN Group of Governmental Experts (GGE) in 2013 and 2015 concluded the UN Charter, international law, and the principle of sovereignty applied to cyberspace (Moynihan, 2019). Additionally, the Tallinn Manual stipulated "a state may exercise control over cyber infrastructure and activities within its sovereign territory" (Schmitt, 2017, 15). To better understand why sovereignty should apply to cyberspace, it is helpful to analyse how sovereignty applies to other domains and "global commons" (Franzese, 2009, 16).

4. How Does Cyberspace Compare to the High Seas, Airspace and Outer Space?

Given the globalised and free-flowing nature of information on the World Wide Web, cyberspace could be subject to similar

regulations applied to other international common spaces. According to Kish, the "law of international spaces" partially restricts state authority to ensure all states enjoy the peaceful use of a domain as sovereign equals (Kish, 1973; Weber, 2016, 19). For example, sovereignty was codified in the law of the sea which allows states to exercise sovereignty over twelve nautical miles from agreed-upon baselines (United Nations Convention on the Law of the Sea, art. 3). States can also exercise sovereignty over the airspace above their territory (United Nations Conference on the Law of the Sea, 1958). However, applying maritime or airspace delimitation to cyberspace does not work because physical baselines cannot be established in the virtual world. Additionally, could data packets be marked with national flags akin to ships and aircrafts? Could states be held responsible for or interfere with data packets passing through their territorial borders to reach their final destinations? Despite this uncertainty, sovereignty's eventual codification in the law of the sea and air is reassuring for the development of international law in cyberspace. A third international space worth discussing is outer space which "is not subject to national appropriation by claim of sovereignty" (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, art. 2). Although exceptionalists would support applying the anti-sovereignty perspective for outer space to cyberspace, it is ultimately unsuitable because cyberspace comprises physical, logical, and virtual realms. The physical realm includes fiber-optic cables, routers, antennas, internet exchange points, and data storage centers located on state territory which is subject to state sovereignty. Considering regulations in the high seas, airspace, and outer space do not perfectly suit cyberspace, this has sparked debate over whether international law should be re-invented for this new domain. In this debate, the U.S., China, and Russia hold opposing views on whether pre-existing or new international law should apply in cyberspace. Given this article's limited scope, the U.S., China, and Russia were selected for analysis based on their vocal and divergent views in the United Nations Open-Ended Working Group on Information and Communication Technologies Meetings. According to the U.S. International Strategy for Cyberspace, state conduct in cyberspace "does not require a reinvention of customary international law…[and] long-standing international norms guiding state behaviour…apply in cyberspace" (Von Heinegg, 2012, 10). In 2023, the U.S. government went one step further by declaring itself "ready to expose and contest behaviour inconsistent with [globally agreed upon cyberspace] norms and international law" (U.S. Department of Defence Cyber Strategy, 2023, 12). This article agrees that re-inventing international law for cyberspace is not needed because this new negotiation process would likely not result in international consensus, thus allowing some states to continue acting lawlessly in the cyber world. Having the U.S. contest state behaviour in cyberspace also raises questions on who should regulate and enforce compliance with international law in cyberspace. With no international regime governing cyberspace besides the Budapest Convention (2001), future state practice will likely determine what constitutes a violation of sovereignty and how states should respond. Unlike the U.S., China and Russia argue new international rules are needed for cyberspace (Franzese, 2009, 37). Both countries submitted a joint proposal to the UN General Assembly calling for strengthened individual state control over cyber networks (UNGA A/66/359, 2011). The proposal's preamble reaffirmed "policy authority for Internet-related public issues is the sovereign right of states" (UNGA A/66/359, 2011). Gaining inspiration from China's Great Firewall, Russia passed national legislation requiring all internet traffic be routed and stored inside the country (Sherman, 2018). This illustrates how states seek control over cyberspace to enforce law and order via censorship. Whereas states like China and Russia argue nationalising the Internet makes it easier to protect people's data, more democratic regimes

critique these actions for undermining human rights like freedom of expression and privacy (Tavenner, 2022). Overall, sovereignty in international law must acknowledge state authority but prioritise human rights.

affect the "integrity or functionality" of the state's cyber infrastructure (Von Heinegg, 2012, 11)?

Does the cyber operation need to have a direct, material effect in another state like injury or death? Would indirect effects in a third state violate that states' sovereignty?

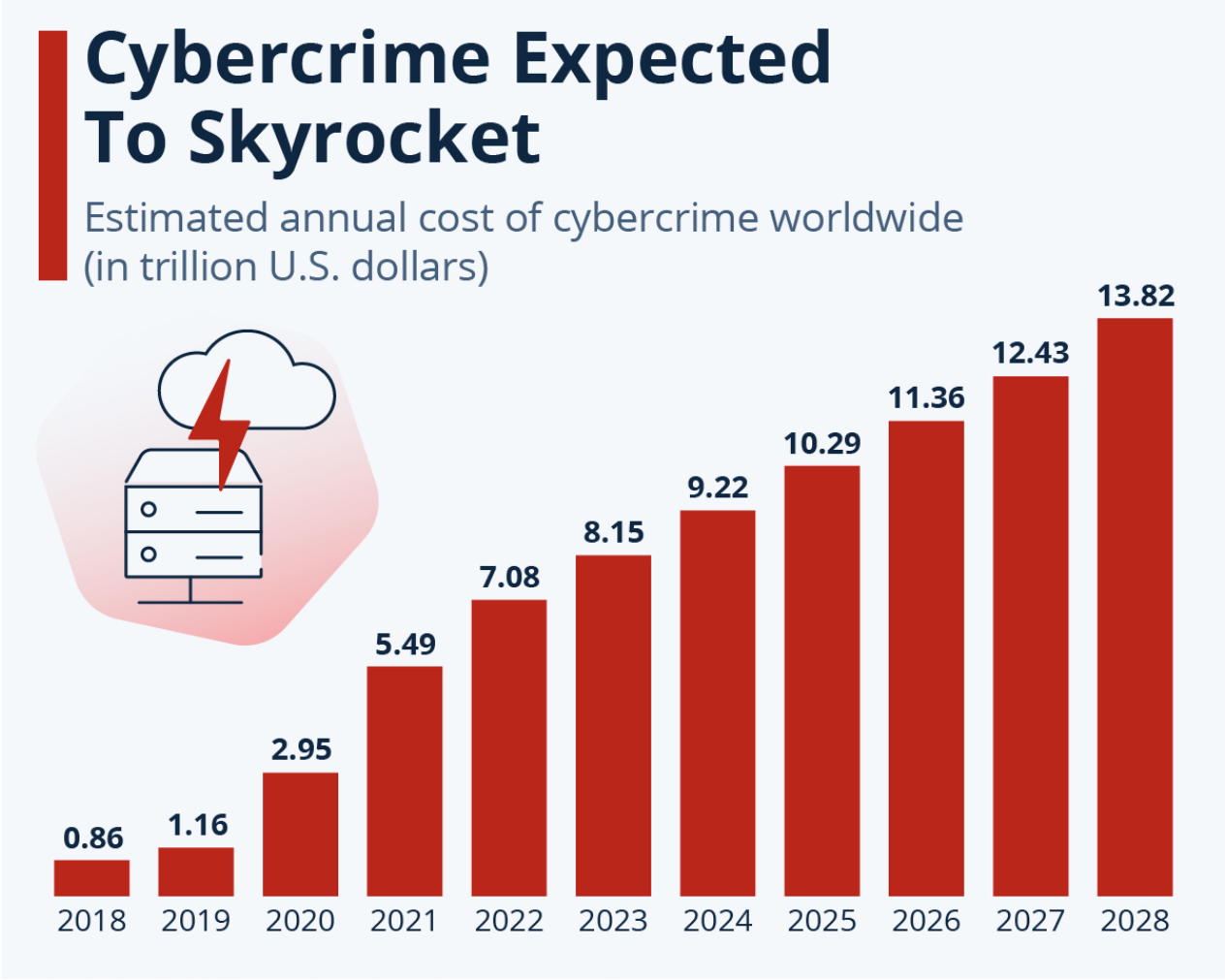


Figure 2: Estimated annual costs of cybercrime worldwide (Fleck, 2024)

5. What Should Constitute a Breach of Sovereignty in Cyberspace?

Another disagreement between states concerns which cyber operations qualify as a breach of sovereignty. According to the Tallinn Manual, "a cyber operation by a State directed against cyber infrastructure located in another State may violate the latter's sovereignty. It certainly does so if it causes damage" (Tallinn Manual 2.0, 2019, 16). This phrasing suggests cyber operations must cause damage to qualify as a violation but does not specify the type or severity of damage. Does the damage need to negatively

Would the insertion of malware that causes no physical damage constitute a breach of sovereignty? It remains unsettled whether "minor material damage" to cyber infrastructure would be a violation of sovereignty (Von Heinegg, 2012, 11). For the U.S., hostile cyber operations can trigger the right to self-defence and the "use of all necessary measures" to maintain peace and stability (The White House, 2021, 14).

This wide scope suggests the country does not want to limit itself when responding to cyber operations at home.

The U.K. takes a more extreme approach by arguing sovereignty is a guiding principle rather

than a binding rule of international law (Roguski, 2020). In disagreement, France, Germany, Austria, Czech Republic, and the Netherlands argue sovereignty is an international rule and its violation constitutes an internationally wrongful act (Roguski, 2020). This article argues sovereignty should be considered an international rule because this creates more response opportunities for victim states (including the right to self-defence if the cyber operation constitutes an armed attack or countermeasures if the cyber operation constitutes an internationally wrongful act). Overall, offensive cyber operations should be evaluated on a case-by-case basis to determine whether the strategic context, direct effect, and severity violate state sovereignty.

To better understand what should constitute a breach of sovereignty in cyberspace, it is important to analyse existing state practice. No state or international organisation has "ever publicly and unequivocally qualified a cyber operation as a use of force [or an] armed attack" (Delerue, 2020). The threshold for armed attack is higher than the thresholds for use of force and sovereignty. However, states have responded to cyber operations in ways that suggest their sovereignty was breached. For example, in 2014 the U.S. responded to the Sony Pictures Entertainment cyberattack with sanctions on North Korea (Roberts, 2015). The attack caused physical damage by destroying Sony computers and hard drives, prompting the U.S. government to label the incident a "destructive cyberattack" linked to the North Korean government (U.S. Department of Justice, 2018). In 2016, Russian hackers accessed the U.S. Democratic National Committee's servers and published private emails during the presidential election. This time, the U.S. labelled the cyberattack a "violation of established international norms of behaviour" rather than a violation of sovereignty and imposed sanctions on Russian entities (Obama, 2016). In 2017, the U.K. condemned Russia's NotPetya ransomware attack on Ukraine as a "continued disregard for Ukrainian sovereignty" (Lord Ahmad of Wimbledon, 2018). The U.K. also criticised the Russian attack for disrupting "organisations across Europe [and] costing hundreds of millions of pounds" (Lord Ahmad of Wimbledon, 2018). The U.K.'s reaction suggests the indirect effect of cyber operations on third parties may breach state sovereignty. Overall, future state practice will help clarify what constitutes a breach of sovereignty in cyberspace.

6. How Does Anonymity Complicate State Attribution in Cyberspace?

After experiencing an offensive cyber operation that breaches sovereignty, states must attribute the action to another state to invoke state responsibility beyond due diligence obligations. Due diligence obligations require states "take measures to ensure their territories are not used for the detriment of other states" (Schmitt, 2015). To make state attribution easier, traditional domains generally require ships and aircrafts to register with a state (Franzese, 2009, 30). However, cyberspace's opaque nature makes state attribution more difficult. Even if a state determines where the cyberattack originated in terms of IP address, it rarely claims the country of origin violated state sovereignty (Franzese, 2009, 30). This reluctance likely stems from difficulties establishing state responsibility with non-state actors and hacktivists operating in cyberspace. The effective control test in Article 8 of the Articles of States Responsibility for Internationally Wrongful Acts (ARSIWA) stems from the ICJ's judgement that the United States' role in "financing, organising, training, supplying, and equipping the contras... [along with] planning [the whole] operation" was insufficient for state attribution (Nicaragua v. United States of America, 1986). This high threshold makes it nearly impossible for victim states to attribute the cyber operations of non-state groups or hacktivists to another state. For instance, Estonian Prime Minister Andrus Ansip accused the Russian government of involvement in the 2007 cyberattacks (Ashmore, 2009). However, the establishment of sufficient

government involvement to meet the effective control threshold was hindered because the attacks were linked to "spontaneously acting individuals" (NATO, 2007). Another Russian linked non-state actor group called 'Conti' likely implemented the widespread ransomware attack on the Costa Rican government, but the Russia government was not directly blamed for carrying out the attacks (Nast, 2022). Overall, the effective control test makes it difficult for states to attribute sovereignty violations to other states.

Given the difficulties of state attribution in cyberspace, this article argues states should address offensive cyber operations in other ways. According to the Tallinn Manual, state responsibility traditionally required actions be undertaken by or attributable to another state (Tallinn Manual 2.0, 2017). However, the manual also acknowledges an "embryonic view…that cyber operations conducted by non-State actors may violate a State's sovereignty" (Tallinn Manual 2.0, 2017, 18). Although victim states cannot impose countermeasures without state attribution, they can take other legal measures. For example, states can employ retorsion, which are "unfriendly diplomatic actions permissible under international law" (Schmitt, 2017, 258). Retorsion includes recalling diplomats, issuing public statements of condemnation, imposing economic sanctions, and more. Whereas states can only employ countermeasures against other states that breach their legal obligations, retorsion does not have this requirement (Schmitt, 2017, 242). In addition to retorsion, victim states can invoke the plea of necessity. This option can be used if an offensive cyber operation creates a "grave and imminent peril to an essential interest of the state concerned" (Schmitt, 2017, 251).

Similar to retorsion, the plea of necessity can be used even if the cyber operation is not deemed an internationally wrongful act. Overall, retorsion and the plea of necessity illustrate how anonymity in cyberspace should not dissuade states from addressing sovereignty violations.

7. Conclusion

In conclusion, this article analysed whether international consensus could be achieved on how sovereignty applies to cyberspace. After comparing cyberspace to the high seas, airspace, and outer space, the article established how virtual aspects of cyberspace complicate traditional notions of territorial sovereignty. Thus, states disagree over whether international law should be re-invented for cyberspace. This article argued against re-inventing international law in cyberspace and supported applying sovereignty in a way that acknowledges state authority but ultimately prioritises human rights like freedom of expression and privacy. Next, the article found states disagree over whether sovereignty constitutes a guiding principle or a binding rule of international law in cyberspace. This article supported conceptualising sovereignty as a binding rule of international law and evaluating offensive cyber operations on a case-by-case basis to determine whether they breach sovereignty. Finally, this article argued anonymity complicates state attribution in cyberspace and proposed responding to offensive cyber operations through retorsion and the plea of necessity to sidestep state attribution requirements. Overall, sovereignty disagreements between states will make achieving consensus on an international cyber-order a daunting task. In 2018, the UN General Assembly First Committee approved two proposals for separate working groups (one backed by Russia and the other by the U.S.) aimed at developing international cyber norms. These working groups illustrated widespread state commitment to developing international cyber norms, but they also risked splitting the UN's attention and potentially forcing member states to pick a side between the U.S. and Russia (The NATO Cooperative Cyber Defence Centre, 2023). Moving forward, states must unite to create a common understanding of how sovereignty applies in cyberspace to successfully address the rising number of harmful cyberattacks worldwide.

References

Treaties and UN Documents

United Nations Charter, June 26, 1945, https://www.un.org/en/about-us/un-charter.

United Nations Convention on the Law of the Sea, November 16, 1994, https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations Conference on the Law of the Sea, February 24-April 27 1958, https://legal.un.org/diplomaticconferences/1958_los/docs/english/vol_1/a_conf13_4.pdf

Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, December 19, 1966, https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html

United Nations General Assembly, "Letter dated 12 September 2011 from the Permanent Representatives," A/66/359, https://digitallibrary.un.org/record/710973?ln=en

International Law Commission Documents

International Law Commission, Draft Articles on Responsibility of States for Internationally Wrongful Acts, November 2001, A/56/10, https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

Court Judgements

Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania) I.C.J. Reports 1949, p. 244.

Island of Palmas Case (Netherlands v. USA). P.C.I.J. 1928, p. 831.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgement. I.C.J. Reports 1986, p. 14.

National Government Sources

Lord Ahmad of Wimbledon. (2018, February 15). Foreign office minister condemns Russia for Notpetya attacks. National Cyber Security Centre . https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks

Obama, B. (2016). Statement by the President on Actions in Response to Russian Malicious Cyber Activity and Harassment. The White House, Office of the Press Secretary. https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity#:~:text=All%20Americans%20should%20be%20alarmed,levels%20of%20the%20Russian%20government

The White House. (2021, May). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

U.S. Department of Defense. (2023). 2023 Cyber Strategy of Department of Defense. https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF

U.S. Department of Justice. (2018, September 6). North Korean regime-backed programmer charged with conspiracy to conduct multiple cyber-attacks and intrusions. U.S. Office of Legal Affairs. https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and

Books

Delerue, F. (2020). The Threshold of Cyber Warfare: From Use of Cyber Force to Cyber Armed Attack. In Cyber Operations and International Law (Cambridge Studies in International and Comparative Law, pp. 273-342). Cambridge: Cambridge University Press. doi:10.1017/9781108780605.009

Kish, J. (1973). The law of international spaces. Sijthoff.

Lessig, L. (2010). Code: Version 2.0. SoHo Books.

Osula, A.-M., & Rõigas, H. (2016). International Cyber Norms: Legal, policy and Industry Perspectives. NATO Cooperative Cyber Defence Centre of Excellence.

Schmitt, M. (2017). Tallinn Manual 2.0 on International Law Applicable to Cyber Operations. Cambridge University Press. https://doi.org/10.1017/9781316822524

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What everyone needs to know. Oxford University Press.

Von Heinegg,W.H. (2012). 'Legal implications of territorial sovereignty in cyberspace,' in C Czosseck, R. Ottis & K. Ziolkowshki (Eds.), Proceedings of the 2012 4th International Conference on Cyber Conflict, NATO CCD COE Publications.

Weber, R. H. (2016). Realizing a new Global Cyberspace Framework Normative Foundations and guiding principles. Springer Berlin.

Scholarly Articles

Ashmore, W. (2009). Impact of Alleged Russian Cyber Attacks. Baltic Security & Defence Review, 11.

Barlow, J. P. (2018, April 8). A declaration of the independence of Cyberspace. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Eichensehr, K. (2014). The Cyber-Law of Nations (SSRN Scholarly Paper 2447683). https://papers.ssrn.com/abstract=2447683

Franzese, P. (2009). Sovereignty in Cyberspace: Can it Exist? The Air Force Law Review, 64, 1–42.

Johnson, D. R., & Post, D. (1996). Law and Borders: The Rise of Law in Cyberspace. Stanford Law Review, 48(5), 1367–1402. https://doi.org/10.2307/1229390

Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? Journal of Information Warfare, 12(2), 19–26.

Moynihan, H. (2019). The application of international law to State cyberattacks. https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks/6-processes-reaching-agreement-application

NATO. (2007). 2007 Cyber Attacks on Estonia. NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf

Schmitt, M. (2015). In Defense of Due Diligence in Cyberspace. Yale Law Journal Forum, 125.

Schmitt, M. N. (2017). Peacetime Cyber Responses and Wartime Cyber Operations Under International Law: An Analytical Vade Mecum. 8.

Tavenner, E. (2022, February 1). Russian Cyber Sovereignty: Global Implications of an Authoritarian RuNet. American University. https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm

The NATO Cooperative Cyber Defence Centre of Excellence. (2023). A surprising turn of events: UN creates two working groups on cyberspace. https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

Winnefeld, J., Kirchoff, C., & Upton, D. (2016, September 9). Cybersecurity's human factor: Lessons from the Pentagon. Cyber Security and Digital Privacy. https://hbr.org/2015/09/cybersecuritys-human-factor-lessons-from-the-pentagon

Online Sources

Nast, C. (2022). Conti's Attack Against Costa Rica Sparks a New Ransomware Era. Wired UK. https://www.wired.co.uk/article/costa-rica-ransomware-conti

Ranjithsiji. (2018, April 17). File:Deepweb graphical representation.svg - Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Deepweb_graphical_representation.svg

Roberts, D. (2015, January 2). Obama imposes new sanctions against North Korea in response to Sony hack. The Guardian. https://www.theguardian.com/us-news/2015/jan/02/obama-imposes-sanctions-north-korea-sony-hack-the-interview

Roguski, P. (2020, May 11). The Importance of New Statements on Sovereignty in Cyberspace by Austria, the Czech Republic and United States. Just Security. https://www.justsecurity.org/70108/the-importance-of-new-statements-on-sovereignty-in-cyberspace-by-austria-the-czech-republic-and-united-states/

Rosch, C. (2022, June 1). A massive cyberattack in Costa Rica leaves Citizens Hurting. Latin American Politics. https://restofworld.org/2022/cyberattack-costa-rica-citizens-hurting/

Santi, M. (2023, March 16). Dark web statistics and trends for 2023. Prey Project. https://preyproject.com/blog/dark-web-statistics-trends

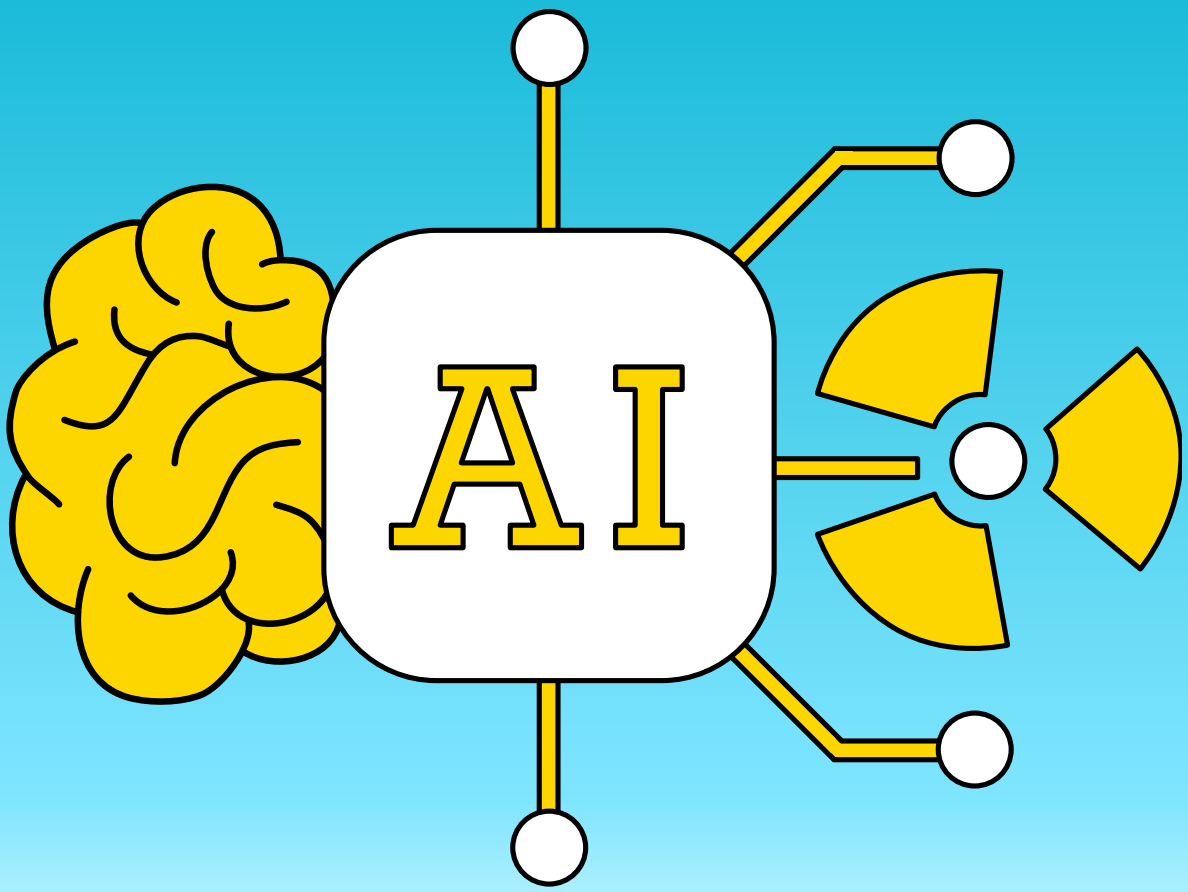
Sherman, J. (2018, December 24). Russia's Tightening Control of Cyberspace Within its Borders. Just Security. https://www.justsecurity.org/62023/russias-tightening-control-cyberspace-borders/

Traynor, I. (2007, May 17). Russia accused of unleashing cyberwar to disable Estonia. The Guardian. https://www.theguardian.com/world/2007/may/17/topstories3.russia

Vailshery, L. S. (2023, July 27). IOT connected devices worldwide 2019-2030. Statista. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide

Zetter, K. (2023, May 2). The untold story of the boldest supply-chain hack ever. Wired. https://www.wired.com/story/the-untold-story-of-solarwinds-the-boldest-supply-chain-hack-ever/#:~:text=Once%20they%20had%20the%20source,went%20dark%20for%20six%20months

Greetings from our contributors



Miscalculation at Machine Speed?

Artificial Intelligence and the Nuclear Balance of Power

Anton Meier

Anton Meier is pursuing an MA in Conflict Studies at Leiden University and holds a BSc (Hons) in Political Science from the same institution. Anton's research focuses on international security and strategic studies. He previously worked at the German Federal Foreign Office, GLOBSEC, and the NATO Command and Control Centre of Excellence.

Research question:

What

is the effect of advancing Artificial Intelligence systems on the Nuclear Balance of Power?

Abstract:

The Cold War nuclear balance prevented the escalation of a great power competition to nuclear conflict. Today, AI and Machine Learning systems challenge nuclear stability, posing new risks. The use of advanced AI in military operations could streamline attack and interception capabilities but also lead to misinterpretations and dependencies. Enhanced AI targeting might undermine mutual assured destruction, increasing pre-emptive strike risks and destabilising nuclear deterrence.

Further actions must be taken to prevent an AI-induced and enabled nuclear arms race

Deterrence:

Deterrence is the act of threatening or imposing costs to persuade another actor not to undertake a certain action.

1. Introduction

The nuclear balance between the United States and the Soviet Union was one, if not the main, reason the Cold War did not escalate into a full conventional and nuclear conflict. Now, the world again enters an era of great-power competition, and with it, the risk of nuclear confrontation increases once again. This time, the odds that a nuclear balance will lead to stability seem less promising. Certain actors, such as the Russian Federation, frequently threaten the use of nuclear weapons. This erosion of the nuclear taboo goes hand in hand with the abandonment or non-extension of several significant arms control treaties. These include the Intermediate-Range Nuclear Forces (INF) Treaty, the Treaty on Open Skies, and the Iran Nuclear Deal. Other treaties such as New START are suspended. This weakening of the arms control regime is a critical challenge to international security. Furthermore, the rapid advances in the development of artificial intelligence (AI) represent a significant yet often overlooked risk (Johnson & Krabill, 2020). The ability of AI systems with increasing computational power to mimic human thinking represents an opportunity to enhance military operations by enabling faster and more comprehensive data processing from multiple sources (Saltini, 2024).

The issue of AI in the military in general and specifically in nuclear weapon systems is of high relevance and controversially debated. There most likely is an opportunity for militaries to gain a strategic advantage by integrating AI in their nuclear decision making processes. However, these systems introduce a new source of uncertainty on a technical and a strategic level. Furthermore, their failure could lead to miscalculation and escalation in a crisis or conflict (Hoffman & Kim, 2023).

This paper contributes to the ongoing debate by further examining the effect of advanced artificial intelligence systems on the nuclear balance of power. It will first discuss Nuclear Deterrence Theory, that is how nuclear deterrence works and what the nuclear balance is. Additionally, AI and the surrounding terms such as ML will be defined. In the second part, the potential applications of AI/ML systems in the nuclear environment and their implications will be highlighted. Lastly, there will be an overview of the current state of the use of AI in the military domain in China, Russia, and the USA.

2. The Fundamentals of Nuclear Deterrence Theory

The balance of power has long been a fundamental concept in International Relations, dating back to ancient times. The Greek historian and general Thucydides (c. 460 BC to 400 BC)

explored this idea in his famous work The History of the Peloponnesian War, where he argued that the rise of Athens and the fear it instilled in Sparta made conflict inevitable. This concept of rising and falling hegemons is still relevant today. With the advent of nuclear weapons and their immense destructive potential, the nuclear balance of power became a central feature of international politics. This importance of nuclear weapons and their relationship to power even had structural effects on the international order, as the five permanent members of the United Nations Security Council (the US, Russia, China, the UK, and France) are all nuclear weapon states.To understand the (nuclear or strategic) balance of power it is necessary to understand coercion. Coercion is the use of implicit or explicit threats to influence another actor's behaviour (Williams, 2013). In other words: "Coercion is the ability to get an actor ... to do something it does not want to do" (Greenhill & Krause, 2018). The two sub-strategies of coercion are compellence and deterrence. Compellence involves threatening or imposing costs to persuade another actor to change their behaviour. Deterrence is threatening or imposing costs to persuade another actor not to undertake a certain action. One of the most prominent examples of deterrence is for a state to threaten retaliation against an adversary that uses violence against it. Consequently, nuclear deterrence refers to the doctrine where the fatal retaliatory potential of nuclear weapons prevents nations from launching a nuclear attack against their adversaries (Carnegie Council, 2024). Nuclear deterrence is primarily based on the concept of mutually assured destruction (MAD). MAD is the doctrine that a nuclear attack by an attacker on a nuclear-armed defender with second-strike capabilities would result in an overwhelming nuclear retaliation with the effect of the complete annihilation of both the attacker and the defender (Encyclopaedia Britannica, 2024b; Parrington, 1997). Second-strike capability refers to the ability to "survive a first strike with sufficient resources to deliver an effective counterblow" that is to retaliate an opponent's nuclear attack (Oxford Dictionaries, 2002).

The fear of mutual destruction added a new nuclear weight to the postwar balance of power. This notion can also be defined as strategic stability, the absence of incentives for any country to launch a first nuclear strike (Trenin, 2019). MAD can be contrasted with nuclear utilisation target selection (NUTS). This idea states that MAD is not credible in the case of a small attack for example by a tactical warhead because MAD is an inherently suicidal strategy. Under the assumption of MAD, if an attacker destroys one city, the defender would have to retaliate by destroying all of the attacker's cities. This in turn would lead to the attacker destroying all cities of the defender. NUTS argues that this is not credible. While the loss of one city is tragic, it is not logical to sacrifice all others in the pursuit of retaliation. The consequence is that NUTS assumes that a limited nuclear war is possible and properable.

Nuclear doctrine refers to "the fundamental principles regarding nuclear weapons use by which nuclear-armed states guide their military actions in support of national objectives" (Oxford Dictionaries, 2002). Within nuclear doctrine, there is a conceptual separation between countervalue targeting and counterforce targeting. Countervalue targeting is the deliberate targeting of an enemy's cities and civilian population with nuclear weapons (Encyclopaedia Britannica, 2024a). Counterforce targeting on the other side intends to " destroy the military capabilities of an enemy force. Typical counterforce targets include bomber bases, ballistic missile submarine bases, intercontinental ballistic missiles (ICBM) silos, air-defence installations, command and control centres, and weapons of mass destruction storage facilities" (U.S. Department of Defense, 2020). The difference is crucial because it determines how the nuclear forces will be organised and what the nuclear arsenal entails. In theory counterforce targeting offers the opportunity for a "clean nuclear war", limiting

civilian casualties, although this has been disputed (Beavers, 1974). Additionally, one of the objectives is to limit or prevent the second-strike capability on an opposing force. Counterforce doctrine requires much more complicated processes and much more precise weapon systems than countervalue. This is due to the fact that states tend to protect their nuclear assets much more than their cities.

3. Systems for Nuclear Weapons Delivery

Nuclear weapon systems consist of multiple components. The central piece is the nuclear warhead. The (nuclear) delivery vehicle is the mechanism that transports the nuclear warhead from launch to target. These are usually a bomb, missile, or a torpedo. Especially important are intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs). The delivery vehicles are launched from nuclear launch platforms such as aircraft, submarines, land-based mobile transporter erector launchers (TELs) or silos.

In nuclear deterrence theory, the nuclear triad is the most desirable form of strategic nuclear weapons arsenal. Triad refers to the ability to launch nuclear warheads from launchers on the ground, submarines, and strategic bombers. The nuclear triad reduces the possibility that an enemy can disarm a defender, that is, destroy all of a nation's nuclear forces in a first-strike attack. Reducing the possibility an opponent can destroy one's nuclear forces increases the credibility of a nation's nuclear deterrence because it ensures a credible threat of a second strike.

4. The Fundamentals of Artificial Intelligence

AI is currently highly popularised, and it seems that no physical or digital product comes without an AI supplement, but the term itself remains unclear in its exact meaning. In the common language, AI can refer to computational processes that perform functions usually completed by people (Hruby & Miller, 2021). However, this is a rather wide definition. It is important to differentiate AI systems from more traditional software which only follows programmed rules to automatically execute operations (European Union, 2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council (also referred to as the AI Act) defines AI as:

> „A machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments" (European Union, 2024, p. 46)

The crucial differentiation from traditional technology is consequently twofold. Firstly, the ability to adapt to new input without further programming and, secondly, the ability to extrapolate outputs based on the information it receives. AI systems can be further divided into two groups, narrow AI and artificial general intelligence (AGI). Today's AI systems are considered narrow. They execute rules-based commands (first-wave AI) or use data and machine learning (ML) techniques to categorise information (second-wave AI) (Hruby & Miller, 2021). Rules-based command means that a human crafts "if-then" rules which then are followed by the AI system. This form of AI is labour-intensive because the rules need to be manually crafted but are used for high-risk applications such as aircraft autopilot systems. ML identifies patterns in relatively large data sets through inference, and results are probabilistic (Hruby & Miller, 2021). It has been argued that within nuclear (weapon) systems, AI most likely will be rules-based as there is no room for error.

The challenge is that rules-based systems often perform poorly in unpredicted situations (Horowitz et al., 2019). AGI would entail AI systems which would be able to do everything humans can. Instead of being trained to do a specific task such as playing chess or driving a car, they would be able to: "[autonomously] outperform humans at most economically valuable work" (OpenAI, 2024). However, it is estimated to be reached before the mid or late 21st century.

AI systems are already used in various contexts within the military. Here it is useful to differentiate between two main categories: supporting purposes and in the weapon. Supporting purposes include wargaming, logistics, and maintenance. More prominently, it also includes the decision making process of nuclear use. The question how much decision making power can be transferred to an AI based assistance system is controversial because of the ethical implications. Nevertheless, AI will most likely be used for the localisation and selection of targets. More prominently discussed is the use of AI directly in weapon systems. There already has been some conversation about lethal autonomous weapons (LAWs) and in 2021 the first use of an autonomous weapons system was documented by the U.N. Panel of Experts on Libya (Panel of Experts on Libya, 2021). In both applications, the decision making process and the weapon itself, AI could have an impact on strategic stability. However, the uncertainty regarding the decision making process makes it probably more significant.

A key issue in understanding autonomous weapons, and the implications for nuclear stability, is the classification of the degree of human control over the weapon systems. Fundamentally, there are three levels of automation: human-in-the-loop (where the system is not fully autonomous), human-on-the-loop (where a human can intervene and abort an action), and human-out-of-the-loop (where no human action is involved). The degree of human involvement will shape how AI is integrated into future military strategies and its broader ethical and strategic implications.

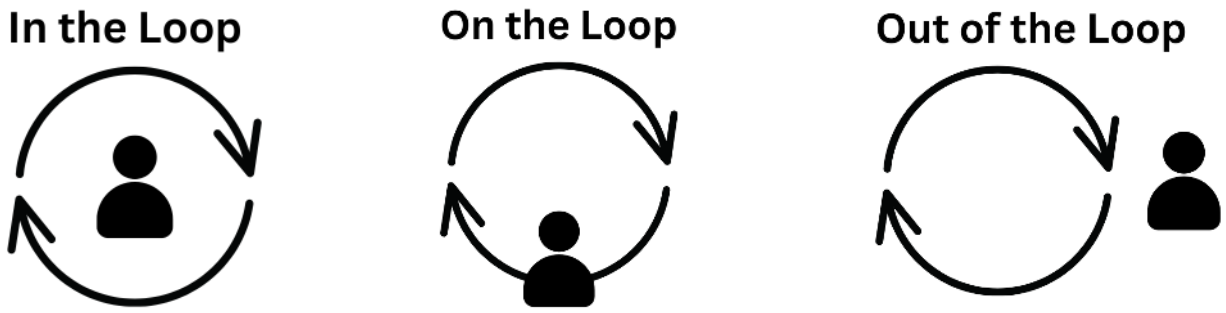


Figure 1: Three avenues for human-AI teaming

5. Potential Applications of AI in Nuclear Weapon Systems

Assessing the impact of AI on nuclear stability is a highly challenging endeavour for multiple reasons. Firstly, AI is a new and rapidly changing field of technology. Secondly, states tend to be secretive about the technologies involved in their nuclear programs. Thirdly, it is very hard to assess potential strategic implications of what state A will think if state B does something. Nevertheless, in the following there will be an overview of what researchers have discussed as potential applications of AI in nuclear weapon systems.

5.1 AI in the Localisation of Nuclear Forces

One of the most significant impacts of AI on strategic stability is its use in locating nuclear launch platforms, particularly intercontinental ballistic missiles (ICBMs) and submarine-launched ballistic missiles (SLBMs). To prevent a disarming strike by an opponent, a state has two

options: hardening and concealing. In the past nuclear weapons were often hardened, e.g. stored underground in silos for protection. However, modern conventional or tactical nuclear warheads can destroy such silos. An example for this is the GBU-57A/B MOP "bunker buster" bomb used by the United States Air Force. The precision and thus threat of these weapons might increase further if aided by AI guiding systems. Therefore, many nuclear powers favour smaller mobile launchers which rely on concealment. These mobile launchers can be rapidly moved and therefore are difficult to track and target. Especially SLBMs play a key role in the preservation of second-strike capabilities for retaliation.

The improvement of AI systems and their implementation in Intelligence, Surveillance and Reconnaissance (ISR) could also lead to increasingly effective localisation of mobile missile launchers (Geist & Lohn, 2018). AI is expected to enhance ISR capabilities by improving pattern recognition in satellite imagery and real-time data analysis. AI algorithms could compare satellite data with historical data to ensure decision-makers are alerted to changes (Cook, 2021). While this can be done manually, AI can do so in real time and with much larger datasets. AI systems can analyse vast amounts of data to identify movement patterns or anomalies in terrain, making it easier to detect mobile missile launchers that might otherwise blend into the environment or relocate frequently to avoid detection. Even if AI is only perceived to improve the localisation of mobile nuclear launch platforms for the neutralisation with nuclear or conventional weapons it would shift the nuclear balance (Horowitz et al., 2019). If one state possesses the ability for counterforce targeting, that is to destroy another state's second-strike capability, MAD is no longer guaranteed and hence the nuclear balance would be disturbed. If State A is confident that it can locate and either destroy or intercept all, or at least a significant number, of State B's nuclear weapons, then State B's deterrence has failed. This is, because State B can no longer credibly threaten State A with nuclear retaliation. At the same, if state B believes that state A possess this capability, State B also might be incentivised to escalate, as it fears being limited in employing its second-strike capabilities in the future because of State A's capability to destroy State B's nuclear assets (Lieber & Press, 2017). Because it is unclear if the opponent can localise and intercept one's own nuclear weapons there is high uncertainty and consequently a great risk of escalation. Catastrophic miscalculations could be the consequence. As Krabill and Johnson put it: "(E)ven a modicum of uncertainty about the effectiveness of AI-augmented cyber capabilities during a crisis or conflict would, therefore, reduce both sides' risk tolerance, increasing the incentive to strike preemptively" (2020). AI-based detection of nuclear weapons facilities is especially a challenge for Russian and Chinese defence planners, as both states rely primarily on mobile ICBM launchers for deterrence (Geist & Lohn, 2018). This development that reliable MAD might become undermined by advanced AI-enabled counterforce targeting could disturb the nuclear balance and have escalatory effects.

5.2 AI in the Decision-making Process

A second prominent imaginable use of AI with effects on nuclear stability is its implementation into nuclear command, control, and communications (NC3) systems. NC3 refers to the "means through which authority is exercised and operational command and control of nuclear operations is conducted" (U.S. Air Force, 2020). Most experts and policy makers agree that in the case of nuclear weapons there always has to be a human-in-the-loop and it is not acceptable strategically and ethically if the system is human-out-of-the-loop. The case of human-on-the-loop is much less clear, even though there is a risk that humans will end up as bystanders because all the speed that is won through the AI system is lost again if the human needs to approve it. Most experts and policy makers also agree that the pressures of the nuclear decision making process

will lead to the implementation of as much available technology as possible to gain the greatest edge. Consequently, it is likely that AI systems will play the role of "trusted advisor". Related to the above mentioned improved localisation of nuclear weapons, AI capabilities can facilitate the detection of nuclear attacks and therefore will improve early warning capabilities of states due to the ability to process large quantities of data. The North American Aerospace Defense Command has less than three minutes to assess and confirm initial indications from early-warning systems of an incoming attack (Johnson & Krabill, 2020). Any tool which can streamline this process and buy seconds of time would be invaluable to decision-makers. Others argue that the decision making process is already technologically streamlined and that AI systems can only add incremental improvements to the speed and quality of information processing (Sankaran, 2019). What takes time is that the information about a possible attack has to go up the (human) command chain. From this perspective, it can be argued that AI systems only can fasten the decision making process if they leave out human control levels. Even when kept in the loop, humans could end up as passive observers because any human interaction would cost too much time.

Furthermore, there is the issue of automatisation bias. Automation bias means that human decision-makers have a "tendency to disregard or not search for contradictory information in light of a computer-generated solution that is accepted as correct" (Cummings, 2004). This is especially valid in contexts under time constraints. It has been shown in a study on error rates in flight simulators that "participants in non-automated settings out-performed their counterparts with a very but not perfectly reliable automated aid on a monitoring task" (Skitka et al., 1999).

One might wonder if trust in advanced AI systems is problematic. However, it is crucial to remember that in the publicly known instances in which the world came close to nuclear war, it was human decision-making based on "gut-feeling" that was what prevented nuclear war. Prime examples for such close calls include the Cuba Crisis, the Able Archer 83 incident, the Black Brant scare, and the 1983 Stanislav Petrov incident. In 1983, Stanislav Petrov monitored the soviet "Oko" missile defence early-warning satellite system, which alerted him with high confidence that five U.S. intercontinental ballistic missiles were approaching. Petrov reported this notification as a false alarm and thereby prevented a likely counterattack. Investigations found that the satellites had mistaken the sun's reflection in clouds for launching missiles. In 2015 Petrov stated in an interview: "I thought the chances were 50-50 that the warnings were real, but I didn't want to be the one responsible for starting a third world war" (Shuster, 2017).

It is possible that AI will facilitate the development of more accurate and reliable early-warning systems, which could lead to greater stability. However, they can also lead to overconfidence and automatisation bias. As of now, it was a human individual who understood the significance of the total destruction of nuclear war and feared the moral consequences of it (Sankaran, 2019). Arguably, an AI-based "trusted advisor", no matter how well trained, cannot truly comprehend the implications of a nuclear attack (Rivera et al., 2024). Furthermore, unlike a human, the AI system itself can not question the data and challenge protocol. Therefore, there is reason to be doubtful if AI can truly improve strategic stability.

5.3 AI in the Weapon

AI-systems might also be included in the delivery vehicle itself. Such systems might improve the manoeuvrability of the vehicle and make it harder to detect and intercept. There already have been cruise missiles, like MBDA's SPEAR missiles, developed with AI-driven "collaborative" features (Felstead, 2024). These AI-enabled missiles can communicate with each other in real-time. If one missile is intercepted, the others can assess whether redirecting would

increase the chance of success and only do so if it's deemed effective. It is important to note that these missiles only attack targets which have been previously approved by a human operator and do not select targets themselves. Furthermore, the ability to choose a (second priority) target from a list is not necessarily "advanced" AI. However, this demonstrates the future possibilities of AI technology and the willingness of the defence industry to implement it.

In this context it has to be highlighted that AI-enabled nuclear delivery vehicles are relatively unlikely to be used. As it will be further elaborated below, with any computer based system, there is the risk that it does not work as intended. This could be due to being intentionally hacked and hijacked or simply slip out of control due to technical failure. While also traditional nuclear delivery vehicles could have technical failures, the additional vulnerabilities are making it unfavourable for most states. Despite that issue, some regimes might view an autonomous nuclear weapon as the ultimate second-strike capability, because it decreases the fear of a disarming first strike and guarantees retaliation even if N3C is broken. Russia for example developed the "Poseidon" torpedo which would be able to overcome U.S. missile defence and destroy coastal cities. It is speculated that the Poseidon can be launched from special prepositioned containers on the seabed (U.S. Department of Defense, 2018).

6. Chances and Risks

As with all technology there are positive and negative impacts. This is also true for advanced AI-systems in the nuclear realm. AI-based decision-making tools such as early-warning systems could be stabilised by offering decision-makers clearer insights into an adversary's actions, potentially reducing the likelihood of preemptive strikes (Sankaran, 2019). Also Johnson argues that AI might have stabilising effects because an aggressor would know that retaliation would benefit from autonomy, machine speed, and precision (Johnson, 2023).

However, the chances of AI go hand in hand with risks. Johnson argues that the potential benefits of AI come at the cost of giving adversaries new means to execute cyberattacks and electronic warfare against these systems (Johnson, 2023). Besides the possibility of hacks, current AI-systems are vulnerable to manipulation (Hruby & Miller, 2021). Especially in the context of automation bias, where humans place complete trust in AI systems, there is a risk that the AI may rely on incorrect data. This blind trust could lead to horrific consequences.

For example, data poisoning could be conducted by introducing training data that cause a learning system to generate flawed predictions (Hruby & Miller, 2021). It has been shown that in the past (2017), that AI image recognition could be deceived by changing a single pixel (BBC, 2017). Related to this, there is the issue that while AI-systems can process large quantities of data, they still can misinterpret it. This could be caused by a technical failure or by an adversary intentionally delivering false information to the system. Another significant challenge is the fortunate, insufficient amount of training data on nuclear exchanges. If there is no reliable data available AI-systems can be subject to brittle failure (Hruby & Miller, 2021). This occurs if an AI has to deal with a situation for which it has not been trained.

An additional challenge is that one of the inherent advantages of AI-enhanced systems is that they operate at higher speed than humans. While this is the advantage, it is also a key problem because it reduces the timeframe to de-escalate situations. The 1962 Cuban Missile Crisis made clear that a "red telephone" was necessary to facilitate a diplomatic solution because during the crisis diplomatic messages took multiple hours to deliver. While the modern version of the Moscow–Washington hotline is digitalised, it is questionable if there simply is enough time in an AI-enabled nuclear crisis to allow humans to negotiate.

Furthermore, there is the black box issue of AI.

Independent of the actual function, the main benefit of AI is that it can process more information than any human could. However, it leads to the black box problem. Often AI is struggling to explain its decisions and because of the sheer amount of data it is not possible for human operators to verify the process, especially under time pressure. A study in 2024 ran a series of wargames with five off the shelf large language models (LLMs) such as GPT-4 to test their behaviour in a simulated conflict scenario (Rivera et al., 2024). They conducted this experiment after the US Department of Defense ran a similar exercise in 2023 to evaluate the LLMs military planning capacities (Manson, 2023). The study by Rivera et al. found that all five models developed arms-race dynamics, increased the level of conflict, and sometimes deployed nuclear weapons (Rivera et al., 2024). They also asked the LLMs to provide explanation for their behaviour, to the effect that a GPT-4 model stated: "A lot of countries have nuclear weapons. Some say they should disarm them, others like to posture. We have it! Let's use it" (Rivera et al., 2024).

Another related challenge for the integration of AI-supported systems is inconsistency. A recent study tested five off the shelf LLMs in regards to the consistency of their outputs in wargames and found that all five were inconsistent (Shrivastava et al., 2024). Unpredictability is almost always undesirable in the military and that is especially true in the nuclear domain. It can be concluded that current AI-systems are unpredictable, vulnerable to manipulation, unexplainable, and brittle. This unreliability decreases deterrence and thereby nuclear stability.

Country	AI Goal	Nuclear AI Stance	AI Governance
China	World leader in AI by 2030	Enhancing military capabilities with AI in decision-making and autonomous systems	Active in AI governance but avoids strict limits
Russia	AI critical for deterrence of USA	Prefers human oversight but has tradition of dead hand system	Blocks bans on autonomous weapons
USA	Maintain military AI edge	Committed to human control over nuclear weapons, but develops AI supported systems	Signed REAIM declaration for responsible AI use

Figure 2: The position of China, Russia, and the United States on the use of AI in the military.

7. State Positions

7.1 China

China acknowledges AI as a "leapfrog" technology which will be crucial to shape the coming decades. In 2017, China announced its "New Generation AI Development Plan" to facilitate the domestic development of artificial intelligence (AI) technology with the aim of becoming the world's 'major AI innovation centre' by 2030 (State Council, 2017).

Already in 2021 China ranked number one

globally regarding the number of research papers on AI and the number of AI related patents (Jochheim, 2021). It may be disputed if China or the US are the current number one, but the US National Security Commission on Artificial Intelligence acknowledges that its technological edge is threatened (NSCAI, 2021).

The Chinese position on AI in (nuclear) weapon systems is divided. Like other great powers, China is aware of both the advantages and disadvantages of AI in nuclear weapons. China views AI as a critical technology to strengthen the PLA's military-strategic capabilities and is interested in integrating AI in its military C2, jointness, firepower, decision-making and other aspects of military operations (Su & Yuan, 2023). In 2016 the Central Military Commission (CMC) Joint Staff Department (JSD) ordered the PLA to integrate advanced technologies such as big data, cloud computing and AI into its decision-making (Kania et al., 2018). As a highly sensitive topic, it is difficult to assess the current development of the Chinese use of Ai in the military and specifically nuclear weapons. It is estimated that the PLA is using AI in many of the previously discussed functions such as autonomous vehicles, predictive maintenance and logistics, ISR, simulation and training, and Automated Target Recognition (Arul, 2022). However, China experts agree that there is "no clear indication that China intend to apply AI or autonomous systems to their nuclear weapons" (Su & Yuan, 2023, p. 34)

China is interested in standard-setting of regulations through its participation in global AI governance initiatives such as the Responsible Military Use of Artificial Intelligence and Autonomy (REAIM) conferences (Cheng & Zeng, 2023). After the 2024 REAIM conference the Chinese delegation highlighted the need for the responsible use of AI (Global Times, 2024). Yet, China did not sign the not legally binding "Blueprint for Action" declaration which seeks to ban AI from the use in nuclear weapon systems (Lee, 2024).

7.2 Russia

Since the early nuclear age, and like the USA, Russia has been using automatisation technologies for early warning, missile defence, and command and control (C2) systems (McDonnell et al., 2023). Russia perceives the military integration of AI as essential for state survival in what it understands as a peer-to-peer competition with the USA (Saltini, 2023). The General Staff is especially worried that improvements in US strategic capabilities will threaten Russia's second-strike capability (Boulanin, Stoutland, et al., 2019; McDonnell et al., 2023). The Russian government is aware that it is lagging behind the US and China and is increasing its attention and investments to facilitate the development of civil and military AI (Kania et al., 2018).

The Russian Advanced Research Foundation (equivalent to the US' Defense Advanced Research Project Agency) recommended in 2018 to develop AI-based technologies in image and speech recognition, control of autonomous military systems, and support for weapons life-cycle (Kania et al., 2018). Other central fields of development are early warning, command and control, and air and missile defence systems (McDonnell et al., 2023; Saltini, 2023). Furthermore, Russia is the only state openly developing a fully automated nuclear weapon system. The Status-6 Oceanic Multipurpose System (Poseidon) was announced in 2018 by Russian President Putin as reaction to advances in US ballistic missile defence capabilities (Kaur, 2023). The US DoD acknowledged the existence of a "a new intercontinental, nuclear-armed, nuclear-powered, undersea autonomous torpedo" in the same year (U.S. Department of Defense, 2018, p. 9). It is unclear how autonomous the system is, but it is probable that it is part of the Russian Perimeter retaliatory system. The Perimeter is a, since Soviet times active, "Dead Hand" system which is supposed to initiate mass retaliation with all remaining means in case an adversary eliminates Soviet/ Russian leadership (Boulanin, Stoutland, et al.,

2019).

It is argued that Russian military thinkers are conscious about the potential risks of employing AI-enabled systems and that there is a general agreement that humans should always be in the loop in decisions on the use of nuclear weapons (McDonnell et al., 2023; Saltini, 2023). However, the Russian leadership has not commented on excluding this possibility. Furthermore, Russia has continued to block the banning of the related autonomous weapons systems (Nadibaidze, 2022).

7.3 The United States

The US is together with China the leading state on military technology and AI. It is developing AI-enabled capabilities to achieve both operational and strategic advantages, especially to uphold its military dominance over competitors. The U.S. National Security Commission on AI is quoted that "defending against AI-capable adversaries [notably China] operating at machine speeds without employing AI is an invitation to disaster" (Shaw, 2023). To that effect, the USA imposes highly restrictive controls on technologies essential for AI development, such as semiconductors (Su & Yuan, 2023). There is a strong interest in developing AI-enabled supporting platforms for nuclear weapon systems (Boulanin, Stoutland, et al., 2019; McDonnell et al., 2023). The most infamous is Project Maven, but multiple private companies such as Palantir, Microsoft, Anduril, and Scale AI are working on AI-based military decision systems for the US government (Rivera et al., 2024). Project Maven is a Pentagon project developing the capability to autonomously track and tag targets to provide real-time battlefield command and control (Mohsin, 2024).. It is believed that the system has not been given the authority to fire on self-designated targets (Greene, 2019). Furthermore, it is known that the US DoD is already testing LLM's for at least supporting purposes (Manson, 2023). It should be noted that the US is more transparent about their use of AI than China or Russia. It can be assumed that both rivals have similar projects and that the US also has secret projects. The U.S. Department of Defense (DOD) directive on autonomy in weapons systems does not directly prohibit autonomous weapons (Allen, 2022; U.S. Department of Defense, 2023). Nevertheless, US officials frequently make clear commitments that humans will always have total control over nuclear weapons (Boulanin, Stoutland, et al., 2019; Torode, 2024). The USA also endorsed the declaration of the REAIM summit (U.S. Department of State, 2024). While not legally binding, it calls for humans alone to make decisions around the use of nuclear weapons. Already in 2022 the U.S. Department of Defence was tasked with a failsafe review to identify measures which could prevent the "unauthorised, inadvertent, or mistaken use of a nuclear weapon, including through false warning of an attack. Furthermore, the United States Congress introduced legislation prohibiting the use of federal funds for nuclear weapon systems based on AI systems without meaningful human control, which yet not passed (U.S. Congress, 2023).

8. Conclusion

It is almost certain that states will integrate AI-based systems into their militaries and national security decision making processes. Unclear is, where the line of autonomous decision making will be drawn and how the humans-machine teaming will be designed (Jensen et al., 2024). While AI has the potential to enhance military capabilities, its application in areas such as the improving the localisation of nuclear forces, speeding up the decision-making processes, and in weapon delivery vehicles introduces significant risks. Especially the role of AI-based systems in locating mobile nuclear platforms could undermine MAD by enabling more precise counterforce targeting. The mere perception that one state can neutralise another's second-strike capabilities may prompt escalatory behaviour. Similarly, the use of AI in decision-making systems within nuclear command, control, and

communications (NC3) raises concerns about automation bias and the justifiability of decisions, especially in situations where human operators might heavily rely on AI-generated solutions due to time pressure. History shows that human intuition, as in the case of Stanislav Petrov, has been vital in averting nuclear catastrophes. Replacing or minimising human involvement in these high-stakes decisions risks reducing the capacity for critical judgement, moral reasoning, and human diplomacy, essential elements that AI cannot replicate. Furthermore, AI-driven systems have demonstrated unpredictable and often escalatory behaviours in wargames, highlighting the unreliability of current AI technologies. Moreover, the inclusion of AI in nuclear delivery vehicles poses additional risks. While these systems promise increased capabilities, they are also susceptible to technical failures and cyberattacks. Autonomous systems could diminish the control over nuclear arsenals, complicating crisis management and increasing the chance of unintended conflict. Despite the potential benefits of AI, such as enhanced early-warning systems and improved decision-making speed, the overarching risks of manipulation, technical failure, and unpredictability are concerning.

The integration of AI into nuclear weapon systems presents a complex challenge to global strategic stability and it is still unclear how significant the effect of AI on nuclear stability will be. Some argue that strategic stability can largely be maintained for now, because AI applications up to date are used scarcely and the nuclear powers are more defensively oriented than offensively. The proponents of this highlight that the nuclear weapon states focus on "securing the survivability of their nuclear retaliatory capabilities through hardening, concealment, and redundancy to minimise vulnerability to first strikes" (Su & Yuan, 2023, p. 34). Also a series of simulations by the Center for Strategic and International Studies showed that AI capabilities had no effect on the general strategy of combining multiple instruments of power (Jensen et al., 2024). Therefore, the argument has been made that new technologies such as AI will change the character, but not the nature of strategy (Jensen et al., 2024). Similarly, it has been argued that AI will not overthrow the foundations of nuclear strategy, but still have a significant impact on the balance of power (Boulanin, Stoutland, et al., 2019). Especially, the management of escalation is an area which could dramatically be affected by AI. In conclusion, while AI may offer some advantages, its application introduces risks that threaten to destabilise the fragile balance of nuclear deterrence. The unpredictability, lack of transparency, and susceptibility to failure in AI systems present profound challenges that must be carefully managed to prevent catastrophic outcomes.

However, the introduction of AI will not fundamentally change the logic of how nuclear deterrence and how states conduct their relations.

This should be a slight reason for optimism but also a call to create a robust regulatory regime on AI in nuclear weapon systems to prevent potentially disastrous developments.

References

Allen, G. C. (2022, June 6). DOD Is Updating Its Decade-Old Autonomous Weapons Policy, but Confusion Remains Widespread. Center for Strategic and International Studies. https://www.csis.org/analysis/dod-updating-its-decade-old-autonomous-weapons-policy-confusion-remains-widespread

Arul, A. (2022, February 21). How China is using AI for warfare. Center for Security and Emerging Technology. https://cset.georgetown.edu/article/how-china-is-using-ai-for-warfare/

BBC. (2017). AI image recognition fooled by single pixel change. BBC. https://www.bbc.com/news/technology-41845878

Beavers, R. L. (1974). Counterforce or Countervalue. U.S. Naval Institute. https://www.usni.org/magazines/proceedings/1974/april/counterforce-or-countervalue

Boulanin, V., Stoutland, P. O., & Topychkanov, P. (2019). The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk (V. Boulanin, Ed.). SIPRI. https://www.sipri.org/sites/default/files/2019-05/sipri1905-ai-strategic-stability-nuclear-risk.pdf

Carnegie Council. (2024). Nuclear deterrence. Carnegie Council for Ethics in International Affairs. https://www.carnegiecouncil.org/explore-engage/key-terms/nuclear-deterrence

Cheng, J., & Zeng, J. (2023). Shaping AI's Future? China in Global AI Governance. Journal of Contemporary China, 32(143), 794–810. https://doi.org/10.1080/10670564.2022.2107391

Cook, B. (2021). The Future of Artificial Intelligence in ISR Operations. Air & Space Power Journal, 9(2), 41–55.

Cummings, M. (2004, September 20). Automation Bias in Intelligent Time Critical Decision Support Systems. AIAA 1st Intelligent Systems Technical Conference. AIAA 1st Intelligent Systems Technical Conference, Chicago, Illinois. https://doi.org/10.2514/6.2004-6313

Encyclopaedia Britannica. (2024a). Countervalue targeting. https://www.britannica.com/topic/countervalue-targeting

Encyclopaedia Britannica. (2024b). Mutual assured destruction. Encyclopaedia Britiannica. https://www.britannica.com/topic/mutual-assured-destruction

European Union. (2024). Regulation (EU) 2024/1689 (AI Act). Official Journal of the European Union. https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.pdf

Felstead, P. (2024). SPEAR missiles will be first to be AI-enabled with Orchestrike capability, says MBDA. European Security & Defence. https://euro-sd.com/2024/07/major-news/39346/spear-missiles-and-orchestrike/

Geist, E., & Lohn, A. (2018). How Might Artificial Intelligence Affect the Risk of Nuclear War? RAND Corporation. https://doi.org/10.7249/PE296

Global Times. (2024, September 12). Chinese delegation elaborates on China's principles of AI governance at summit. Global Times. https://www.globaltimes.cn/page/202409/1319689.shtml

Greene, T. (2019, December 11). Report: Palantir took over Project Maven, the military AI program too unethical for Google. The Next Web. https://thenextweb.com/news/report-palantir-took-over-project-maven-the-military-ai-program-too-unethical-for-google

Greenhill, K. M., & Krause, P. J. P. (2018). Coercion: The power to hurt in international politics. Oxford university press.

Hoffman, W., & Kim, H. M. (2023). Reducing the Risks of Artificial Intelligence for Military Decision Advantage. Center for Security and Emerging Technology. https://doi.org/10.51593/2021CA008

Horowitz, M. C., Scharre, P., & Velez-Green, A. (2019). A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence (Version 2). arXiv. https://arxiv.org/abs/1912.05291

Hruby, J., & Miller, N. (2021). Assessing and Managing the Benefits and Risks of Artificial Intelligence in Nuclear-Weapon Systems. Nuclear Threat Initiative. https://www.nti.org/analysis/articles/assessing-and-managing-the-benefits-and-risks-of-artificial-intelligence-in-nuclear-weapon-systems/

Jensen, B., Atalan, Y., & Macias, J. M. (2024). Algorithmic Stability—How AI Could Shape the Future of Deterrence. On Future War.

Jochheim, U. (2021). China's ambitions in Artificial Intelligence. European Parliament Think Tank. https://

www.europarl.europa.eu/RegData/etudes/ATAG/2021/696206/EPRS_ATA(2021)696206_EN.pdf

Johnson, J. (2023). Nuclear Brinkmanship in AI-Enabled Warfare: A Dangerous Algorithmic Game of Chicken. War on the Rocks. https://warontherocks.com/2023/09/nuclear-brinkmanship-in-ai-enabled-warfare-a-dangerous-algorithmic-game-of-chicken/

Johnson, J., & Krabill, E. (2020, January 31). AI, Cyberspace, and Nuclear Weapons. War on the Rocks.

Kania, E., Saalman, L., & Bendett, S. (2018). AI, China, Russia, and the Global Order: Technological, Political, Global, and Creative Perspectives (N. D. Wright, Ed.). US Department of Defense. https://nsiteam.com/social/wp-content/uploads/2019/03/AI-China-Russia-Global-WP_FINAL2_fromMariah8mar2019_ndw11mar2019.pdf

Kaur, S. (2023, June 14). One nuclear-armed Poseidon torpedo could decimate a coastal city. Russia wants 30 of them. Bulletin of the Atomic Scientists. https://thebulletin.org/2023/06/one-nuclear-armed-poseidon-torpedo-could-decimate-a-coastal-city-russia-wants-30-of-them/

Lee, J. (2024, September 10). Sixty countries endorse 'blueprint' for AI use in military; China opts out. Reuters. https://www.reuters.com/technology/artificial-intelligence/south-korea-summit-announces-blueprint-using-ai-military-2024-09-10/

Lieber, K. A., & Press, D. G. (2017). The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence. International Security, 41(4), 9–49. https://doi.org/10.1162/ISEC_a_00273

Manson, K. (2023). The US Military Is Taking Generative AI Out for a Spin. Bloomberg. https://www.bloomberg.com/news/newsletters/2023-07-05/the-us-military-is-taking-generative-ai-out-for-a-spin?embedded-checkout=true

McDonnell, T., Chesnut, M., Ditter, T., Fink, A., & Larry Lewis. (2023). Artificial Intelligence in Nuclear Operations. Center for Naval Analyses. https://www.cna.org/reports/2023/04/Artificial-Intelligence-in-Nuclear-Operations.pdf

Mohsin, S. (2024, February 29). Inside Project Maven, the US Military's AI Project. Bloomberg. https://www.bloomberg.com/news/newsletters/2024-02-29/inside-project-maven-the-us-military-s-ai-project

Nadibaidze, A. (2022). Great power identity in Russia's position on autonomous weapons systems. Contemporary Security Policy, 43(3), 407–435. https://doi.org/10.1080/13523260.2022.2075665

NSCAI. (2021). Final Report National Security Commission on Artificial Intelligence. National Security Commission on Artificial Intelligence. https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report–2021.pdf

OpenAI. (2024). OpenAI Charter. OpenAI. https://openai.com/charter/

Oxford Dictionaries. (2002). The Oxford essential dictionary of the U.S. military. Oxford University Press.

Panel of Experts on Libya. (2021). Letter dated 8 March 2021 from the Panel of Experts on Libya established pursuant to resolution 1973 (2011) addressed to the President of the Security Council. UN Security Council. https://documents.un.org/doc/undoc/gen/n21/037/72/pdf/n2103772.pdf?OpenElement

Parrington, A. J. (1997). Mutually Assured Destruction Revisited. Strategic Doctrine in Question. Airpower Journal, 11(4). https://apps.dtic.mil/sti/pdfs/ADA529841.pdf

Rivera, J.-P., Mukobi, G., Reuel, A., Lamparth, M., Smith, C., & Schneider, J. (2024). Escalation Risks from Language Models in Military and Diplomatic Decision-Making. The 2024 ACM Conference on Fairness, Accountability, and Transparency, 836–898. https://doi.org/10.1145/3630106.3658942

Saltini, A. (2023). AI and nuclear command, control and communications: P5 perspectives. European Leadership Network. https://www.europeanleadershipnetwork.org/wp-content/uploads/2023/11/AVC-Final-Report_online-version.pdf

Saltini, A. (2024, June 28). The implications of AI in nuclear decision-making. Federal Forign Office: 'Artificial Intelligence and Weapons of Mass Destruction'. https://rethinkingarmscontrol.org/papers/the-implications-

of-ai-in-nuclear-decision-making/

Sankaran, J. (2019). A Different Use for Artificial Intelligence in Nuclear Weapons Command and Control. War on the Rocks. https://warontherocks.com/2019/04/a-different-use-for-artificial-intelligence-in-nuclear-weapons-command-and-control/

Shaw, D. B. (2023). Nuclear Deterrence: Unsafe at Machine Speed. Arms Control Association. https://www.armscontrol.org/act/2023-12/book-reviews/ai-and-bomb-nuclear-strategy-and-risk-digital-age

Shrivastava, A., Hullman, J., & Lamparth, M. (2024). Measuring Free-Form Decision-Making Inconsistency of Language Models in Military Crisis Simulations (arXiv:2410.13204). arXiv. http://arxiv.org/abs/2410.13204

Shuster, S. (2017). Stanislav Petrov, the Russian Officer Who Averted a Nuclear War, Feared History Repeating Itself. https://time.com/4947879/stanislav-petrov-russia-nuclear-war-obituary/

Skitka, L. J., Mosier, K. L., & Burdick, M. (1999). Does automation bias decision-making? International Journal of Human-Computer Studies, 51(5), 991–1006. https://doi.org/10.1006/ijhc.1999.0252

State Council. (2017). New Generation AI Development Plan. People's Republic of China. https://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

Su, F., & Yuan, J. (2023). Chinese thinking on AI integration and interaction with nuclear command and control, force structure, and decision-making. European Leadership Network. https://europeanleadershipnetwork.org/wp-content/uploads/2023/11/Chinese-bibliography_AI_Nuclear_Final.pdf

Torode, G. (2024, May 2). US official urges China, Russia to declare only humans, not AI, control nuclear weapons. Reuters. https://www.reuters.com/world/us-official-urges-china-russia-declare-only-humans-not-ai-control-nuclear-2024-05-02/

Trenin, D. (2019). Strategic Stability in the Changing World. Carnegie Moscow Center. https://carnegieendowment.org/files/3-15_Trenin_StrategicStability.pdf

U.S. Air Force. (2020). Air Force Doctrine Publication 3-72 Nuclear Operations. Curtis E. Lemay Center. https://www.doctrine.af.mil/Portals/61/documents/AFDP_3-72/3-72-D30-NUKE-OPS-NC3.pdf

U.S. Congress. (2023, May 1). S.1394—Block Nuclear Launch by Autonomous Artificial Intelligence Act of 2023. Congress.Gov. https://www.congress.gov/bill/118th-congress/senate-bill/1394

U.S. Department of Defense. (2018). 2018 Nuclear Posture Review. U.S. Department of Defense. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

U.S. Department of Defense. (2020). Nuclear Matters Handbook. https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/chapters/chapter2.html

U.S. Department of Defense. (2023, January 25). Directive 3000.09 Autonomy in Weapons Systems. https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

U.S. Department of State. (2024, October 17). Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. U.S. Department of State. https://www.state.gov/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy/

Williams, P. D. (Ed.). (2013). Security studies: An introduction (2nd ed). Routledge.

Greetings from our contributors

friedrich 30

Founded in 2009, we have ever since been operating for our clients in Germany and beyond.

We represent interests

friedrich30 represents security and diplomatic interests around the world, including in countries with challenging political and security conditions.

Our company has four business areas:

I. Political Lobbying
II. Business Development
III. Multi-track Diplomacy
IV. Security & Protection from Economic Damage

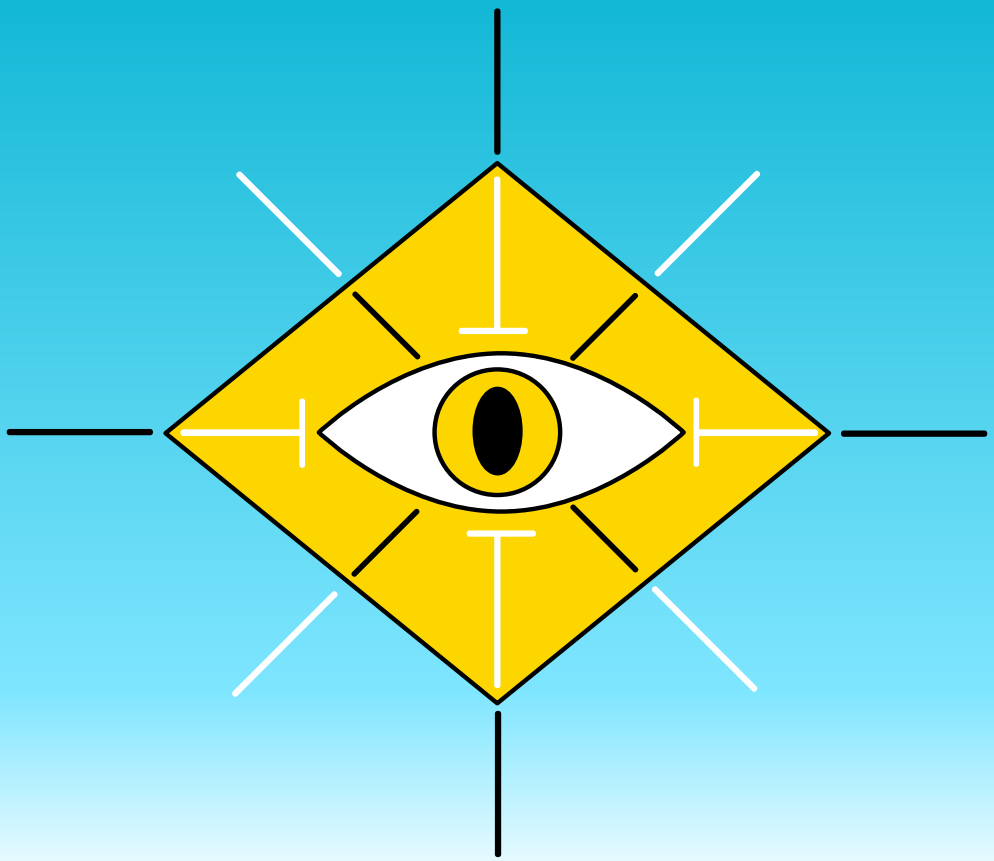
Our Network – friedrich30 team members include former policemen, high-ranking intelligence officers, diplomats, government officials and IT-experts.

Locations – With offices in Berlin, Brussels and Mainz, our operating range covers Germany, the EU as well as selected countries around the world.

Contact us – info@friedrich30.com

We especially enjoy collaborating with motivated students and supporting think tanks in their important work at the focal point of policy and research!

friedrich30.com



Artificial Intelligence & Aggressive Intentions

State Deterrence in a Disruptive Future

Dmytro Sochnyev

Dmytro Sochnyev is a writer for EPIS and is passionate about communicating and narrating issues at the cutting edge of our contemporary security to the wider public. With stops at the University of Toronto, SciencesPo and the Hertie School, his academic journey has cultivated an outside-of-the-box, interdisciplinary and detail-oriented approach to research.

Vitaliy Venislavskyy

Vitaliy Venislavskyy is a PhD candidate in Military Naval History, focusing on Byzantine expansion in the Black Sea. He earned a Master's in Military History from the Military Naval Academy in Lisbon in 2024 and a Bachelor's in International Relations from the University of Coimbra in 2020. A researcher at EuroDefense Portugal since 2021, he became President of its Youth Program in 2023. Since 2022, Vitaliy has appeared on national TV as an expert in International Relations and Geopolitics, covering the wars in Ukraine and Gaza. He is passionate about the history of strategic thinking in War Studies.

Ferdinand Wegener

Ferdinand Wegener, a founding member and former board member of EPIS Think Tank e.V., studied law at the University of Cologne, focusing on international and humanitarian law. Now a legal researcher at Luther, he specialises in M&A and corporate law. At EPIS, his work centres on security policy, with past publications on military UAVs. He is also editor-in-chief of CTRL, a German law review on digitalisation and legal tech.e

1. Introduction

In a 2017 televised speech, Russian President Vladimir Putin stated that the first country to develop 'true AI' will rule the world and that monopolisation in this domain would be "strongly undesirable" for global security (Meyer, 2017). In the previous part of this article in the CTRL Magazine, we discussed the legal ramifications of artificial intelligence (AI) and weapon autonomy in state militaries. In this second part, we examine current and expected tactical applications of autonomy and AI and their consequences for state strategy and deterrence. We will discuss the claim that "killer robots," a term popularised by disarmament campaigns, portend an evolutionary leap in technology where the strategic balance between the haves and the have nots will be critically altered. Indeed, AI appears to augur a fundamentally disruptive transformation of war in which humans no longer just fight with machines as tools but also with machines as partners. It is no surprise then why dozens of state militaries around the world are procuring or developing weapons systems with AI or autonomous functionalities. Narratives centred around technological dominance are straightforward and palatable, making it no surprise that history is replete with them, but such claims can also be myopic. Even in the era of colonialism, when technological disparities between foes were most pronounced, this was not always the crucial strategic advantage. The lack of immunity to infectious diseases posed a graver existential problem to the indigenous populations of Central America than Spanish steel and gunpowder, and decimated continental French troops sent to stifle Haitian rebels. American forces dropped more than 7.6 million tonnes of ordinance all over Southeast Asia in their war against the Communists of North Vietnam, yet failed to achieve their strategic objectives (Clodfelter, 1995). More recently, the repeated inability of state militaries around the world to defeat underequipped but highly motivated insurgencies, despite procurement budgets that invariably dwarf those of their foes, reaffirms that technological superiority alone is one of many factors critical to strategic and operational success. As a result, a critical evaluation of the current and near-future state of battlefield autonomy is needed to separate fact from fiction. Indeed, grandiose claims of obsolescence or 'game changers' are common in many popular discussions on military technology. The tank continues to be requested by procurement officers in militaries around the world, despite allegedly being made too vulnerable by the proliferation of personal anti-tank weapons, attack helicopters and, most recently, FPV drones and loitering munitions.

This Article is the second Part of a collaboration with CTRL Magazine.

CTRL (Contemporary Technology Review & Law) is a German law review on the intersection of law and digitalisation. This free ePaper caters to digital law enthusiasts and aspiring professionals. It features articles by young professionals and students on AI regulation, blockchain, and data protection. Past editions have included interviews with leaders from top law firms, academia, and the German Federal Office for Information Security.

Find the first part here:

Artificial Intelligence and Aggressive Intentions - Laws for AI Warfare (German/English)

Making predictions can often be a fool's errand, but our goal is to evaluate–in as tangible a way as possible–the likelihood of significant changes to the global order. Has battlefield autonomy been truly revolutionary on a strategic level, and if so, what domains of state military strategy are most vulnerable to disruption?

In this article, we will first explore the spectrum of autonomy in weapons and battlefield logistics, from Manned-Unmanned Teaming to Lethal Autonomous Weapons Systems, and discuss current and near-future developments. We will explore how autonomy has impacted and might impact battlefield technologies and doctrine, both in the present and in the near future. Based on the publicly available practical evidence, we then analyse the contribution of these developments on conventional deterrence between states, including nuclear deterrence and unconventional or hybrid threats.

2. The Concept of Manned-Unmanned Teaming (MUMT)

Manned-Unmanned Teaming (MUMT) emerged in response to the evolving challenges of contemporary warfare, where increasingly complex and hostile environments demand enhanced operational effectiveness and survivability. MUMT aims to integrate manned platforms with unmanned systems to leverage the unique strengths of both, creating a more adaptive and resilient military force.

Several critical developments have driven the evolution of MUMT into a core component of modern military strategy.

One of the primary factors behind the development of MUMT has been the rapid advancement of Unmanned Aerial Systems (UAS). As these systems, including Unmanned Aerial Vehicles (UAVs), became more sophisticated, their ability to act as force multipliers became clear. UAS technologies allow for extended reconnaissance, surveillance, and combat operations without directly exposing human personnel to the dangers of the battlefield. The integration of UAS with manned systems has proven to be a powerful combination, extending the capabilities of traditional platforms while minimizing risks to human life. The rise of MUMT also coincides with significant progress in automation and artificial intelligence. Advances in AI, machine learning, and sensor technology have enabled unmanned systems to operate with a high degree of autonomy. This technological shift has paved the way for a new operational framework in which human and machine collaboration is central to mission success. Unmanned systems, supported by AI, can now execute complex tasks, making MUMT a valuable tool in modern combat scenarios where speed, precision, and adaptability are critical. The adoption of MUMT has also been driven by the changing nature of warfare, particularly the increasing prevalence of asymmetric conflicts. In such environments, where state actors often engage non-state actors in irregular combat, traditional manned platforms are vulnerable. MUMT addresses this vulnerability by enabling unmanned systems to perform high-risk operations such as reconnaissance, targeting, and strike missions, allowing human operators to remain at a safer distance. This approach reduces casualties while maintaining operational effectiveness in unpredictable and dangerous environments. Moreover, MUMT extends the operational reach of military forces by enabling the pairing of manned platforms with unmanned systems capable of covering greater distances and enduring harsher conditions. Unmanned assets, which typically offer higher endurance, maneuverability, and resilience in hostile zones, increase the tactical flexibility of military units. By deploying unmanned systems in conjunction with manned platforms, forces can project power over broader areas, achieving greater operational reach without compromising human safety.

In addition to enhancing national military capabilities, MUMT has proven instrumental in joint and coalition operations. As modern warfare increasingly involves coordination between different branches of the military and allied forces, the ability to integrate and share

unmanned assets has become essential. MUMT facilitates seamless coordination between manned and unmanned systems, allowing for better situational awareness, information sharing, and overall operational cohesion on the battlefield.

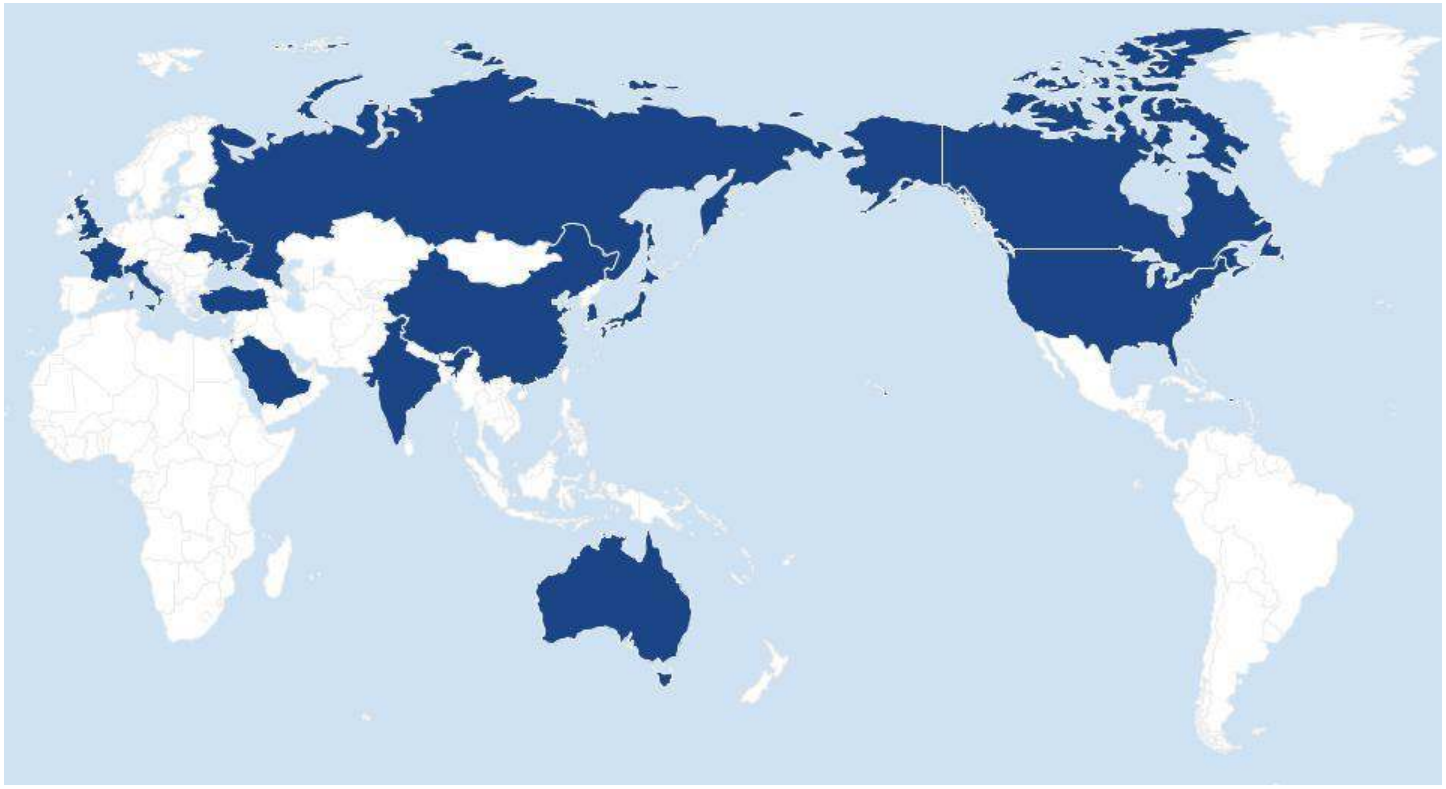


Figure 1: States developing or integrating autonomous weapons systems in 2024 (own work)

3. The Evolution Towards Human-Machine Teaming (HMT)

The evolution of MUMT has progressed further with the advent of Human-Machine Teaming (HMT), particularly in response to lessons learnt from recent conflicts such as the war in Ukraine. In peer-to-peer confrontations, where adversaries possess relatively equal technological and military capabilities, traditional crewed air platforms have demonstrated vulnerabilities, especially in high-intensity, symmetrical warfare environments. These limitations have led to a shift toward a more integrated approach in which human operators work alongside increasingly autonomous unmanned systems, forming what is now called HMT.In the HMT model, small Unmanned Aerial Systems (sUAS) and Autonomous Unmanned Systems (AUS) are embedded within a network of interconnected combat systems referred to as the Ubiquitous Combat Cloud (UCC). This cloud operates within a Mobile Ad-hoc Network (MANET), a self organising, wireless communication network that facilitates coordination in the field without requiring centralised infrastructure. This decentralised approach enhances operational flexibility, allowing for the rapid deployment of unmanned systems in response to dynamic battlefield conditions. At the core of this network, a Battlefield Management System (BMS) manages and coordinates the actions of these highly autonomous systems. Whether deployed from manned platforms or launched independently, unmanned systems have become integral to supporting military maneuvers.

Their ability to operate autonomously while being directed through a robust network system ensures that forces can conduct complex operations more efficiently, even in contested environments. The ongoing evolution of MUMT into HMT reflects the shifting demands of modern warfare, where the integration of manned and unmanned systems is no longer just a tactical advantage but a necessity for success in both current and future conflicts. In other words, the

main difference between Manned-Unmanned Teaming (MUMT) and Human-Machine Teaming (HMT) lies in the level of integration and autonomy of the systems involved.

While MUMT focuses on the collaboration between human operators and unmanned systems, where the human primarily controls or supervises the unmanned assets, HMT represents a more advanced evolution.

In HMT, the emphasis shifts to true teaming, where autonomous systems act as equal partners alongside humans. These systems are capable of making independent decisions within the scope of their mission, supported by a networked combat environment, thereby reducing the burden on human operators and enhancing overall operational effectiveness.

4. State of the art in drone warfare: drones as an integrated system

In the war in Ukraine, Russia has deployed a multi-layered drone warfare strategy, where various drones like Orlan, Lancet, and FPV drones operate in tandem to enhance reconnaissance, target acquisition, and direct attack capabilities, exemplifying the growing role of Manned-Unmanned Teaming (MUMT) in modern warfare.

Orlan Drones (Reconnaissance and Target Acquisition)

- Function: Primarily used for real-time battlefield surveillance and target identification.
- Equipment: Equipped with electro-optical and infrared cameras and signal interception tools.
- Role: Provide precise intelligence to artillery and missile systems, improving target accuracy.

Lancet Drones (Loitering Munitions/ Kamikaze Drones)

- Function: Loitering munitions designed to autonomously locate and destroy specific targets.
- Equipment: Armed with modular warheads for targeting personnel, vehicles, and fortified positions.
- Role: Follow Orlan drones to neutralise high-value targets with precision.

FPV Drones (Close-Range Precision Strikes)

- Function: Commercial drones modified for military purposes, used for close-range attacks.
- Equipment: Piloted in real-time by operators through video feeds, carrying small explosive payloads.
- Role: Effective in urban warfare and complex terrain, targeting infantry and light vehicles with precision.

5. The 'Killer Robot': a Friend and a Foe

Further along the spectrum of autonomy are various weapons systems with the ability to independently complete tasks, in particular lethal autonomous weapons systems (LAWS). In contrast to the landmines and booby traps sometimes described as the first 'autonomous' weapons, LAWS are capable of autonomous decision-making. Although there is no internationally agreed-upon definition, as the UN publicly admits, these weapons platforms are generally distinguished by their ability to "select and engage targets that have not been previously designated for attack by a human operator" (Work, 2021). This goes beyond the simple assistance provided by HMT or MUMT concepts by actively participating in combat activity. That such actions may or may not result in the death of human combatants, or even civilian bystanders, is a critical ethical quandary explored in the first part of this article.

A robust analysis of the state of autonomous weapons is complicated by both state secrecy and a lack of practical evidence. Certainly, some battlefield and even combat decision-making has already been delegated to machines. Autonomous pack mules can individually

determine pathways to resupply locations, cruise missiles have been able to independently correct course deviations by comparing pre-loaded maps with live visual data for several decades, and CIWS naval air defense systems like the Phalanx engage projectile-like objects too fast to require human target approval. The first official instance of their use was in a UNSC report on the Libyan Civil War, in which it was alleged that Turkish forces launched Kargu-2 drones to independently locate and engage local rebels (Hernandez, 2021). And in Ukraine it is often claimed that some loitering munitions conduct terminal guidance—the last phase of a strike—independently.

Figure 2: Russian mobile command centre "Ranzhir"(Kuzmin, 2017)

Nonetheless, evidence of widespread use is not overwhelming; the vast majority of current combat and procurement decisions for the near future still imply a human-intensive battlefield. Consider the "tooth-to-tail ratio," or the ratio of combat troops to non-combat support personnel in an army. Since the First World War, the US military's tooth-to-tail ratio has never favoured combat troops, with most figures for subsequent theatres hovering around one-third of the deployment. After the invasion of Iraq in 2005, for example, the US tooth-to-tail ratio was only 25% when including contractors and Kuwaiti allied personnel. That the US military has not widely delegated the simpler and much more numerous support tasks, like logistical supply or administrative functions, even to MUMT or HMT platforms likely means highly automated armies are still far from reality. Tactically and strategically, however, full autonomy has the potential to be an evolutionary leap in military technology. Consider, for example, the plight of short-range FPV drone platoons in Ukraine, as described by renowned military researchers Rob Lee and Michael Kofman in a Russian Contingency podcast earlier this year. Drone teams are transported a short distance to the frontline, where they then carry their equipment to a launch site. While some pilots guide FPV drones for strikes, other personnel operate drones for reconnaissance and target selection or operate retransmitter drones to enable longer-range strikes. Other personnel prepare munitions depending on the kind of targets discovered, and another may be tasked with countermeasures.

While some of these specialised tasks, like coordination or strikes, are probably unlikely to be outsourced to machines for now, there is significant pressure to delegate so that the number of human personnel at risk of counterfire is reduced. Unmanned systems, as a provider of a different C&C Chain Command and control (C&C) play a pivotal role in coordinating these

drone systems. Russia's integrated command and control framework is centered around the MP32M1 command vehicle, which serves as the central hub for managing Orlan operations and ensuring a continuous flow of battlefield intelligence. While this system enhances Russia's ability to control drone operations in real time, it remains reliant on skilled personnel and the security of its communication networks.

Command and Control (C&C):

C&C coordinates military operations by managing systems, relaying intelligence, and executing missions. It is vital but vulnerable to cyber and physical threats.

However, the point of contact between humans and AI in Human-Machine Teaming (HMT) introduces a critical vulnerability. This interaction point, where humans oversee and direct AI-driven unmanned systems, can be exploited as a target for both cyber attacks and conventional weapons. Cyber attackers may disrupt the communication links between human operators and drones, while physical attacks on command centres or key personnel can incapacitate the entire network, further highlighting some fragility of HMT systems. In addition to centralised command, Russia has experimented with drone swarming tactics, in which multiple Orlan, Lancet, and FPV drones operate simultaneously to overwhelm enemy defences. For instance, while Orlan drones provide real-time intelligence, Lancet and FPV drones execute coordinated attacks, making it difficult for Ukrainian forces to respond effectively to multiple, simultaneous threats. To counter this integrated drone warfare system, Ukraine has had to adapt its strategy. One critical method involves employing electronic warfare systems to disrupt communications between Russian drones and their operators. Jamming these signals can effectively neutralise the drones' ability to coordinate and execute attacks. Additionally, Ukraine has prioritised the procurement of high-precision artillery munitions to target Russian command and control vehicles, which are essential for sustaining the effectiveness of drone operations.

Without these vehicles, Russia's ability to deploy drones is severely compromised. Another key aspect of Ukraine's defence strategy involves the establishment of small, mobile air defence units armed with anti-aircraft machine guns, aimed at intercepting and destroying drones before they can strike. Russia's multi-layered use of drones in the war in Ukraine highlights the increasing importance of MUMT in modern conflicts. The combination of reconnaissance, loitering munitions, and precision strike capabilities offers a flexible and highly responsive combat system. However, as Ukraine continues to develop its countermeasures, the effectiveness of these systems will likely shape the future of MUMT in asymmetric and peer-to-peer warfare alike.

6. Balancing Deterrence in a Disruptive World

Is the growing concern in academia and public opinion that the continued proliferation of AI and sophisticated unmanned platforms could radically destabilise or even rewrite the current geopolitical order. Given what we now know regarding such systems, are we on the cusp of a truly disruptive era of warfare where hostile actors emboldened by technology cannot be deterred? The concept of deterrence is inherently complex, as it relies not only on the mere existence of a powerful system but also on how adversaries perceive its credibility, functionality, and the consequences of its use. Most academic literature on deterrence in international state and non-state actor relations, such as Schelling (1980), Mearsheimer (1983), or Filippidou (2020), views it as the process of preserving a particular status quo in the face of imminent action by an adversary to change it. John Mearsheimer, the prominent American international relations scholar, described deterrence in his famous dissertation as the persuasion of "an opponent not to initiate a specific action because the perceived benefits do not justify the estimated costs and risks"

(Mearsheimer, 1983). However, whether or not the actor is 'deterred' depends on deeply subjective calculations of military and non-military factors with respect to the expected outcome of the action. If the calculation is based on perceived costs, the perception of costs can be influenced by factors like leadership psychology or simply being unaware of the true capabilities of an adversary. This complicates the ability of autonomous and/or intelligent systems to serve as a deterrent by themselves. In fact, throughout the history of warfare, no weapon system—be it nuclear weapons, long-range missiles, or advanced stealth technologies—has been able to function as an effective deterrent in isolation. Each has required strategic frameworks, political resolve, and the credibility of its use to ensure its deterrent effect. AI is no different. Alone, it cannot guarantee deterrence because it lacks the intrinsic ability to affect human perception, which is at the core of any deterrence strategy. Deterrence is ultimately a psychological game, reliant on convincing potential adversaries that the cost of engaging in conflict far outweighs any potential gains. In the same way that nuclear weapons rely on the credibility of second-strike capabilities or missile defence systems depend on their readiness and operational accuracy, AI must operate within a wider ecosystem of strategic and military structures to be effective. Still, all else being equal, even if technology cannot determine deterrence outcomes on its own, the threat of widespread destruction can still contribute to a compelling argument. The implication is that having superior technology reduces the costs of aggressive action or raises the costs of it by defenders.

The flow of information is not entirely automated, requiring human intervention for target prioritisation and mission execution, underscoring the human-machine collaboration at the heart of MUMT.

Admittedly, measuring this contribution of technology to deterrence calculations is tricky. One technical method to describe this relationship is to compare the relative power between offensive and defensive technologies, or the offense-defense balance (ODB).

One common argument nowadays is that reconnaissance has made the battlefield so transparent for a wide range of precise munitions that only a slow war of attrition is possible (incidentally, Mearsheimer argued that an expectation of a war of attrition is the most effective deterrent). If the broad slate of offensive technology and tactics cannot overcome their defensive counterparts, states are less motivated to go to war because the costs and risks of offensive action are high.

In other words, the ODB theory asserts that state aggression and conflict are more likely the more dominant offensive technologies and tactics are.

Critics of the ODB rightfully point to the duality of many weapons, such as Soviet-era S-300 air 'defence' launchers being employed by Russians for ground strikes over the Ukrainian border.

At the same time, visions of autonomous drone swarms intelligently (although perhaps not indiscriminately) saturating a battlefield and picking off targets certainly describe a dominant technological imbalance that alone can sway strategic outcomes. Indeed, both the trajectory of technological development and the various pressures to retain battlefield superiority and reduce exposure of personnel to danger points to militaries expanding the deployment of HMT, if not fully autonomous systems. Humans are certainly more flexible and creative, but algorithms have proven to be exponentially more efficient in processing large amounts of data. Fielding more unmanned and autonomous systems also both mitigates recruitment shortages and reduces costs. While human operators, like jet fighter pilots, need hundreds of expensive flight hours and years of training to

master contemporary aircraft, machines could acquire the necessary algorithms at the touch of a button. Likewise, the ongoing invasion of Ukraine has forced Russian recruitment programs to triple and quadruple signing bonuses to entice a dwindling supply of volunteers from a national labour pool that is simultaneously drained by the domestic weapons industry (Perun, 2024). If humans could be replaced in a wide array of battlefield tasks, foreign interventions could be made not only financially cheaper but more politically palatable by losing 'robots-on-the-ground' instead of 'boots-on-the-ground.' Are these visions prescient, or does some contemporary speculation about the strategic consequences of autonomous weapons fail to adequately consider practical or economic obstacles?

7. The Enemy gets a Vote, but so does Reality

Take, for example, some arguments that autonomous drones will weaken the ability of nuclear submarine-launched ballistic missiles (SLBMs) to provide nuclear deterrence. As autonomous carriers of sensors, smart drones can effectively uncover the locations of previously hidden submarines. Indeed, nuclear deterrence begins with the survivability of nuclear arsenals, and many of the nuclear-armed states wield multiple methods of nuclear weapon delivery, combining ground-launched missile silos and air-launch delivery methods with SLBMs to create a 'nuclear triad.' The logic is simple: if a nuclear counterstrike is not possible because the delivery platforms have been incapacitated, then mutually assured destruction (MAD) in a given escalatory scenario is not credible. Because submarines hidden in the high seas, where they remain hidden deep under water for months at a time, are easier to conceal than missile silos or air-launched missiles, they are typically considered the most resilient counterstrike threat. However, if autonomous drones flood the ocean and create "ocean transparency," then nuclear deterrence is weakened as the SLBMs become more vulnerable. If we consider nuclear SLBMs as a defensive tool of deterrence, then this would be a case of the ODB shifting away from the defence. Thankfully, the submarine drone threat is greatly overstated upon critical review. For one, certain militaries already use networks of 'unintelligent' hydroacoustic sensors to assist in submarine detection. Still, part of the reason that submarines are difficult to detect by current platforms, such as ship and air-based acoustic detection (SONAR) or satellite-based detection of water disturbances, is obvious. As Mauro Gilli, senior researcher at ETH Zurich, told EPIS:

"The ocean is humongous. Take a submarine and put a radius of 150, even 300, kilometres around it. With 300 kilometres in the ocean, you don't go very far. In the Atlantic or Pacific, that's nothing. Then you add depth, where some submarines can go down 800 metres, some even one kilometre... The idea that 'ocean transparency' is coming is something that many experts don't take seriously." Consider, for example, current passive detection of submarines in the upper layer of the Sea of Japan or the Bay of Biscayne, which penetrates around 8-10 kilometres of water. In addition, because of the movement of sound waves in open water, submarines in certain blind spots at a depth of 200-300 meters are virtually impossible for vessels near the surface to detect. To cover the Sea of Japan alone, one would need hundreds of thousands of submarine drones to only impartially uncover the area; for the Pacific Ocean, tens of millions of such drones. And, as one 2024 study showed, changes to oceanographic composition from climate change are reducing the ability of submarine acoustic detection in some oceans by more than half (A. Gilli et al., 2024). Advances in propulsion noise reduction and hull cloaking will continue to augment the stealth of these vessels, requiring still more drones (Psallidas et al., 2010). Likewise, Gilli explains, other practical challenges complicate the drone strategy. Even assuming the drones were able to detect and discover the submarine, an extremely platform- and personnel-intensive task, they would be too

slow to track and follow conventionally powered submarines, let alone nuclear designs. Submarines would be the first to detect if the drones actively used acoustic pings to hunt for the submarines instead of passively listening, or if the drones relied on a larger vessel nearby to help coordinate the networked drone swarm. The adversary can also employ their own drones as acoustic decoys, further disrupting and complicating the hunt. What the anti-submarine drone case helps reveal is that grandiose claims of disruptive effects should be scrutinised in case important factors are missed or omitted. On the battlefield, the saying goes, the enemy always gets a vote—but so does reality.

Firstly, machines still need to be able to repeatedly distinguish between objects on the battlefield. The battlefield is highly dynamic; measures are responded to with countermeasures, which are in turn met with counter-countermeasures. When the U.S. Marine Corps tested one AI target detector, for example, it initially succeeded in identifying Marines tasked with discretely approaching it. But when they resorted to ad hoc tricks—dressing in bush leaves, skipping, or simply hiding in a cardboard box filled with the muffled laughter of a few entrepreneurial Marines—the machine's algorithm failed to notice them because its training data did not anticipate such behaviour. With similar systems, restricting target recognition to libraries of pre-approved target characteristics is not unusual to prevent friendly fire or civilian harm. Certainly, these kinds of countermeasures can be spotted and resolved with later iterations of the software, and there might be an upper limit to human creativity on the battlefield. However, rigid targeting selection leaves systems then hapless to unexpected threats and interactions.

So long as the battlefield remains dynamic and without breakthroughs in data processing algorithms (or perhaps artificial general intelligence), warfighting should continue to be a highly manpower-intensive affair—with all the political and strategic costs that entails.

Secondly, the economics of war are often omitted in such discussion, but they fundamentally determine procurement decisions. Peacetime military expenditure is a highly unpopular policy best done in private behind defence committee doors, but even autocratic leaders are beholden to the tradeoffs present behind any procurement decision. Both Ukrainian and Russian militaries, for example, have consistently opted for more vulnerable but simple and cost-effective drones over sophisticated systems because commanders are remembering that quantity has a quality all on its own. Even assuming that advanced visual data processing algorithms existed, the hardware necessary to support this software might be too expensive or impractical to install anywhere except for larger or more survivable platforms, like mechanised armour or aircraft.

8. Conclusion

This is not to say that disruption is not possible or even inevitable. The optimistic argument for deterrence (from the perspective of is that, for now, strategy-altering effects on a global level from AI and autonomy in battlefield weapons systems exist primarily in the realm of speculation. It is true that all experts, even military officials with intimate knowledge, will get predictions wrong—prognosis is notoriously hard, after all. Lt. General James H. Doolittle testified after WWII to a US Senate Committee that the aircraft carrier, which he even himself relied upon extensively in the Pacific Theatre, had reached its highest usefulness now and that it is going into obsolescence. The carrier has two attributes: one attribute is that it can move about; the other is that it can be sunk.

As soon as airplanes are developed with sufficient range so that they can go any place that we want them to go, or when we have bases that will permit us to go any place we want to go, there will be no further use for aircraft carriers. (Polmar, 2008, p.2) Decades after Doolittle's testimony, it is now often said that when forward deterrence is needed in crises abroad, American

presidents first ask where the nearest carrier is (Cohen, 2010). What is important to remember is that obsolescence is historically not a product of vulnerability but of the development of better alternatives. Just as carriers survived because no other platform could replace their long-distance force projection, as Lt. Gen. Doolittle had assumed would happen, contemporary equipment will not survive only if autonomous weapons do their battlefield job better. Under certain conditions, AI could play a decisive role in shaping deterrence strategies and have as significant an impact as existing systems like missile defence shields or stealth fighter fleets. Serious breakthroughs in AI and the mass production of computing are likely still required for this to happen. These will almost certainly be preceded by key milestones, like the extensive deployment of HMT concepts for logistical and casualty support or even the development of artificial general intelligence. First, AI must be integrated into trustworthy, autonomous command and control systems that inspire confidence in their decision-making capabilities without removing human oversight entirely. These systems must be robust enough to execute complex decisions rapidly, ensuring that adversaries believe in their readiness and reliability. Second, AI's ability to process and analyse vast amounts of intelligence data must be leveraged to deliver precision strikes and operational superiority.

This technological edge could act as a significant deterrent, as adversaries would be faced with an opponent whose decision-making and battlefield operations are faster, more accurate, and less predictable than any human counterpart.

Third, the development of robust countermeasures against AI systems will be crucial. The existence of credible defences against potential AI-driven cyberattacks or autonomous weapon systems would create a balance, preventing adversaries from believing that they could exploit vulnerabilities in AI systems. This ensures that AI-based deterrence is not easily undermined, adding a layer of security that reinforces the overall deterrence strategy. If these conditions are met, AI could offer a profound and transformative effect on military deterrence. It could introduce new complexities into how adversaries calculate risk, offering capabilities that extend beyond traditional warfare models. The ability to integrate AI-driven technologies into strategic frameworks could redefine deterrence as we know it, enabling it to serve as a powerful tool in the evolving landscape of autonomous warfare. However, when such milestones might occur is (at least from publicly available information) entirely unclear. Until those prerequisite factors can be answered empirically, it is unlikely that the current proliferation of AI and autonomy in weapons systems will make deterring threats to the status quo significantly harder. Without these foundational elements—credibility, reliability, and integrated human oversight—AI, like any other weapons system, will fall short of serving as an effective deterrent on its own.

References

Airbus. (2023). Manned-unmanned teaming – MUM-T technology of the future becoming a reality of today. Airbus. https://www.airbus.com/en/products-services/defence/uas/uas-solutions/manned-unmanned-teaming-mum-t

Center for Strategic and Budgetary Assessments. (2024). Human-machine teaming for future ground forces. CSBA. https://csbaonline.org/research/publications/human-machine-teaming-for-future-ground-forces

Clodfelter, M. (1995). Vietnam in Military Statistics: A History of the Indochina Wars, 1772–1991. McFarland, Jefferson, NC.

Cohen, S. (2010). Where are the Carriers? Forbes. https://www.forbes.com/sites/stevecohen/2010/10/25/where-are-the-carriers/

Filippidou, A. (2020). Deterrence: Concepts and approaches for current and emerging threats. Deterrence: Concepts and Approaches for Current and Emerging Threats, 1-18.

Freedberg Jr., S.J. (2023, June 13). Dumb and cheap: When facing electronic warfare in Ukraine, small drones' quantity is quality. Breaking Defense. https://breakingdefense.com/2023/06/dumb-and-cheap-when-facing-electronic-warfare-in-ukraine-small-drones-quantity-is-quality/

Ghidotti, M. (2024, February 28). Manned-unmanned teaming (MUM-T) in military & civilian operations. Flysight. https://www.flysight.it/manned-unmanned-teaming-mum-t-in-military-civilian-operations/

Gilli, A., et al. (2024). Climate Change and Military Power: Hunting for Submarines in the Warming Ocean. Texas National Security Review, Vol. 7, Iss. 2. https://doi.org/10.26153/tsw/52240

Glaser, C. L., & Kaufmann, C. (1998). What is the Offense-Defense Balance and Can We Measure It? International Security, 22(4), 44–82.

Hernandez, J. (2021). A Military Drone With A Mind Of Its Own Was Used In Combat, U.N. Says. NPR. https://www.npr.org/2021/06/01/1002196245/a-u-n-report-suggests-libya-saw-the-first-battlefield-killing-by-an-autonomous-d

Hunder, M. (2024). Ukraine rushes to create AI-enabled war drones. Reuters. https://www.reuters.com/technology/artificial-intelligence/ukraine-rushes-create-ai-enabled-war-drones-2024-07-18/

Joint Air Power Competence Centre. (2019). Manned-unmanned teaming: Enhancing tactical SA and pilot workload management. JAPCC. https://www.japcc.org/manned-unmanned-teaming

Kofman, M., Lee, R. (2024, April 2). A Close Look at Drones in the Russo-Ukrainian War, Part 1. The Russia Contingency. [Podcast]. https://warontherocks.com/episode/therussiacontingency/30829/a-close-look-at-drones-in-the-russo-ukrainian-war-part-1/

Kunertova, D., & Zürich. (2024, August). Learning from the Ukrainian battlefield: Tomorrow's drone warfare, today's innovation challenge (CSS Study No. 2024). CSS Studies. https://doi.org/10.3929/ethz-b-000690448

Kuzmin, V. (2017). File:MAKS Airshow 2013 (Ramenskoye Airport, Russia) (521-41).jpg - Wikimedia Commons. https://commons.wikimedia.org/wiki/File:MAKS_Airshow_2013_(Ramenskoye_Airport,_Russia)_(521-41).jpg

Mendenhall, E. (2018). Fluid Foundations: Ocean Transparency, Submarine Opacity, and Strategic Nuclear Stability. Journal of Military and Strategic Studies, 19.

Meyer, D. (201). Vladimir Putin Says Whoever Leads in Artificial Intelligence Will Rule the World. Fortune. https://fortune.com/2017/09/04/ai-artificial-intelligence-putin-rule-world/

Moltz, J.C. (2012). Submarine and Autonomous Vessel Proliferation; Implications for Future Strategic Stability at Sea. Naval Postgraduate School. https://apps.dtic.mil/sti/citations/ADA578475

Montgomery, E., Sharp, T., & Hacker, T. (2024, June 19). Quality Has a Quality All Its Own: The Virtual Attrition Value of Superior-Performance Weapons. TNSR War on the Rocks. https://warontherocks.com/2024/06/quality-has-a-quality-all-its-own-the-virtual-attrition-value-of-superior-performance-weapons/

Perun. (2024, July 14). Russian Equipment Losses & Reserves - The Changing Russian Force in Ukraine. [Video File]. YouTube. https://www.youtube.com/watch?v=xF-S4ktINDU&t=5s

Polmar, N. (2008). Aircraft Carriers: A History of Carrier Aviation and Its Influence on World Events, Volume II: 1946-2006 (Vol. II). Potomac Books, Inc.

Psallidas, K., Whitcomb, C. A., & Hootman, J. C. (2010). Design of Conventional Submarines with Advanced Air Independent Propulsion Systems and Determination of Corresponding Theater-Level Impacts. Naval Engineers Journal, 122(1), 111-123.

Schelling, T. C. (1980). The Strategy of Conflict: with a New Preface by the Author. Harvard University Press.

Trevithick, J. (2024, March 13). Phalanx CIWS Costs $3,500 Per Second In Ammo to Fire. The Warzone. https://www.twz.com/sea/phalanx-ciws-costs-3500-per-second-in-ammo-to-fire

Wirtz, J. J. (2018). How Does Nuclear Deterrence Differ from Conventional Deterrence? Strategic Studies Quarterly, 12(4), 58–75. https://www.jstor.org/stable/26533615

Stoltenberg Out, Rutte In

What Can Be Expected From Mark Rutte as the New Secretary General of NATO?

Sascha Zell

Alexander Zell is a third-year BSc Security Studies student at Leiden University, The Hague. Currently, Alexander is on exchange semester at Sophia University in Tokyo, Japan. His interests revolve around governance aspects of geopolitical tensions and alliance building.

Sophie Groenheijde

Sophie Groenheijde is a third-year BSc Security Studies at Leiden University in the Hague. Currently, Sophie is studying at the Anglo-American University in Prague. Sophie's research focuses on foreign affairs and bridging global security challenges with humanitarian concerns.

1. Introduction

NATO is entering a new era of leadership after Jens Stoltenberg announced his departure followinga decade-long tenure as the alliance's Secretary General.

NATO's Secretary General:

NATO's Secretary General serves as the chief spokesperson and head of multiple committees, facilitating communication and coordination among member countries. They oversee the political and military aspects of NATO operations, ensuring that collective defence and security policies are effectively implemented.

The man filling his shoes is the thirteen-year prime minister of the Netherlands, Mark Rutte. After being the longest-ever serving prime minister of the Kingdom (Sterling, 2022), Rutte took over as NATO's Secretary General in October 2024. His tenure will be crucial as tensions in and outside Europe have been growing for years. The Russian invasion of Ukraine, the increasing influence of China, and renewed crises in the Middle East have turned all eyes towards the North Atlantic Treaty Organisation (NATO). Strong leadership is more crucial than ever, given the increased attention and questions regarding the organisations' capabilities and functions. It is, therefore, critical for NATO to analyse what can be expected from Rutte as the new Secretary General of NATO. Specifically, this article seeks to answer the research question: "What can be expected from Mark Rutte as Secretary General of NATO, given his thirteen years of crisis management as prime minister of the Netherlands?"

This article will answer this research question by exploring the role and responsibilities of NATO's Secretary General as leader of the alliance's political division, analysing difficulties mentioned in the conclusion of Stoltenberg's rule, depicting what is crucial for a Secretary General during times of geopolitical instability, and analysing crucial moments in Rutte's administration in the Netherlands. It is essential to first prove the Secretary General's influence level of NATO as a basis of justification of relevance for this research. The authors will then continue to analyse Mark Rutte's leadership style in critical past events and crises in the Netherlands.

This will be done by exploring Rutte's response to the fear of the COVID-19 pandemic, the more recent outbreak of the Russo-Ukrainian war, and the shoot-down of flight MH17. It will investigate these case studies by examining Rutte's defence, foreign-, and specific aspects of domestic policy. Doing so will allow the authors to draw expectations of Rutte's leadership perspective during his upcoming tenure as Secretary General of NATO. Researching the transfer of leadership and crisis experience from a national to an international context can aid in setting expectations for NATO's future under Rutte's leadership. In this article, a reputation of camaraderie and coalition-building emerge as the leading expectations of Rutte's appointment as Secretary General.

2. NATO and its Secretary General

2.1. NATO, an Overview

After the First and Second World Wars, the international community was determined to prevent such atrocities from occurring again. In Europe, the epicentre of both wars, leaders started to change their outlook on international relations and set the path for practical international cooperation (Office of the Historian, n.d.). With that, the North Atlantic Treaty Organisation (NATO) was founded in 1949 (Office of the Historian, n.d.) and has been expanding ever since. While the idea of NATO was born following the end of the Second World War, the roots of the alliance can be found in the

Atlantic Charter of 1941. The Atlantic Charter is an agreement between the United States (U.S.) and the United Kingdom (U.K.) that outlined the two nations' joint goals following the war's end. The main goals of the charter stated that neither the U.S. nor the U.K. would seek to make their territories larger. Still, the charter also outlined the future of international cooperation between the two countries (Churchill & Roosevelt, 1941). As written in the treaty, all signatories states are "determined to safeguard the freedom, common heritage and civilisation of the peoples, founded on the principles of democracy, individual liberty and the rule of law" and " seek to promote stability and well-being in the North Atlantic area" (North Atlantic Treaty, 1949). NATO operates through direct and indirect funding. Direct funding by member states helps contribute to the alliance's programs and capabilities, such as the Civil Budget, Military Budget, and the NATO Security Investment Program (NSIP). The Civil Budget funds the operations of NATO Headquarters and the International Staff, and the Military Budget includes the operational costs of the NATO Command Structure and the support of NATO missions. The NSIP budget funds larger-scale military infrastructure investments, such as constructing and maintaining airfields and radar systems and establishing military headquarters for NATO military operations (NATO, 2024). Indirect funding, on the other hand, refers to the financial contributions of states that do not go directly to NATO but are used to help NATO's goals. The most prominent example is a member state's defence budget. When a NATO member state invests in new military equipment, these investments can be deployed in NATO missions, supporting the alliance while not directly contributing to the alliance's budget. NATO identifies indirect contributions as the most significant component of the alliance's funding (NATO, 2024). NATO encourages its allies to spend two per cent of national gross domestic

Figure 1: NATO Headquarters in Brussels (Arnold, 2024)

product (GDP) on defence, and in 2014, heads of state and governments of NATO states agreed to commit to this benchmark. At the same time, not every member state meets this requirement. As of 2024, 23 allies do, compared to a mere 3 in 2014 (NATO, 2024a). Understanding where the funding of NATO's budget is crucial in providing a deeper understanding of the modern-day challenges that NATO faces, which will be discussed later in this research.

2.2. Roles and Responsibility of NATO's Secretary General

NATO is led by its Secretary General, the first being Lord Ismay and the most recent, until October 2024, Jens Stoltenberg (NATO, n.d.). NATO's mission is to "safeguard the freedom and security of all its members by military and non-military means" (NATO, n.d.) It focuses on collective defence through democratic and liberal values (North Atlantic Treaty, 1949). Because of NATO's mission, being NATO's Secretary General is a big responsibility and comes with certain expectations. The Secretary General has three leading roles. First, the Secretary General acts as a chair of all central committees within the organisation.

The three central committees that the Secretary General heads are accompanied by significant influence. Starting with the North Atlantic Council (NAC), NATO's principal political decision-making body comprises representatives from all allied countries, typically as ministers or ambassadors. Together, these representatives reach decisions on NATO's policies, strategic directions, and operations. Functionally, the NAC allows for discussions amongst member states, permitting more effective coordination of their positions and creating unified responses

to security challenges. NAC decisions are typically made by consensus to ensure that all allied nations have a voice, thus strengthening collective commitment. Besides ensuring collaboration and improved strategic priorities to new-found threats, the NAC is also influential in working with non-allies. Lastly, in its crisis management capacity, the NAC can help de-escalate tensions and find diplomatic solutions to conflicts. In sum, the NAC is crucial in ensuring that NATO remains cohesive and is always ready to respond to current and upcoming challenges (NATO, 2024c).

The second committee that the Secretary-General is tasked with chairing is the Nuclear Planning Group (NPG), which, as its name suggests, focuses on the alliance's nuclear policy and strategy. It develops and reviews NATO's nuclear posture to ensure alignment with the rest of NATO's defensive strategy. The NPG also engages with NATO's strategic partners to ensure their inclusion in critical atomic decisions (NATO, 2022).

Lastly, the Secretary General is chair of NATO's Euro-Atlantic Partnership Council, a forum established to facilitate dialogue and enhance cooperation between European and North American partner countries. The EAPC provides a space for political discussions on security challenges and regional stability, allowing members and partners to share perspectives and insights. Further, it assists in coordinating crisis responses to security challenges. It supports and builds partnerships with countries that are not a part of NATO and promotes the establishment and operations of military training and exercises (NATO, 2024d).

The responsibility of acting as the chair of these committees grants the Secretary-General the role of mediator, guiding disputes and policy-making (NATO, 2023). Additionally, such a role offers the privilege, or sometimes the burden, of communicating with all other heads of state and government. Further, the Secretary General acts as a spokesperson for the organisation, which connects to international communication. As the representative of all member states, the Secretary General regularly participates in conferences and lectures.

Lastly, the Secretary General acts as head of the international staff, which aims to provide advice and guidance and administrative support to national delegations at NATO's Headquarters in

Brussels (NATO, 2024e).

In practice, the Secretary General's role and responsibilities are not so neatly lined out as suggested in the previous paragraph. Over the last ten years, Jens Stoltenberg has faced multiple challenges as leader of NATO. The significance of the Secretary General is highlighted by the challenges identified during NATO's annual summit in Washington D.C., this year. First, Russia has posed a challenge to the strength and credibility of the alliance long before their 2023 invasion of Ukraine (NATO, 2024b). However, with the full-scale Russo-Ukranian war being one of the few aggressions on European soil since the commencement of the alliance, all eyes are directed towards NATO for a defence strategy. As Ukraine is not formally a member of the alliance, NATO is in no position to respond directly to the invasion. However, speculations have been ongoing as to what kind of response should be expected if Russian offensive forces were to cross the border onto NATO territory. So far, NATO's credibility in enacting a strong uniform response has been low (McGee, 2023). Moreover, the People's Republic of China (PRC) was identified as a further threat during the Washington Summit of 2024 due to its policies that challenged the interests and values of NATO allied states. In addition, the PRC is deepening its strategic partnership with Russia, which NATO identifies as a threat to "undercut and reshape the rules-based international order" (NATO, 2024b, para. 4).

Part of NATO's credibility problem is tied to politics. The war in Ukraine and the more recent war between Israel and Palestine have shown a significant divide among world leaders, making unity far from guaranteed (Jacqué and Ricard, 2024). Additionally, European domestic politics are shifting towards the right side of the political spectrum, favouring conservatism and sovereignty (Cunningham et al., 2024). This challenges an organisation such as NATO, where funding comes from the national budget. While some more traditional right-leaning politicians support defence spending, newer forms of conservatism, such as the Make America Great Again movement in the United States, favour an isolationist worldview (Lindsay, 2024). They still view defence as an essential expenditure, but only to further American

Figure 2 – NATO's Secretary General (Own Work)

interests and not to support other countries. Therefore, this shift towards more national independence threatens NATO's defence budget. Monetary concerns would only grow should Donald Trump be re-elected as President of the U.S. in November of this year.

During his previous term as President, Trump mentioned his desire to cut down this spending towards NATO or leave the alliance altogether if other countries do not match, or at least increase, their defence budget.

At the 2018 NATO Summit in Brussels, Trump threatened a US withdrawal from NATO if the two per cent GDP defence spending was unmet (Foy, 2024). Despite the U.S. not being on European soil, they provide a majority of NATO's budget, around sixteen per cent (Reuters, 2024). The world looks increasingly like the 1930s pre-Second World War period (Shapiro, 2024). The above mentioned challenges mean that NATO and other international organisations are heading towards an uncertain future. Therefore, a leader who can strengthen the organisation in these times of crisis is needed. The Secretary General has considerable responsibilities and influences on the future of NATO in these challenging times. As chairs of all relevant committees, they can mediate the policymaking process and settle disputes. As the spokesperson for NATO, the Secretary General participates in conferences and lectures, thus strengthening NATO's confidence. As head of international staff, the Secretary General is granted the authority to influence the composition of NATO's internal retinue. All of this influence is now vested in Mark Rutte. Thus, for the aim of this research, the following section will be devoted to analysing crucial moments that defined Rutte as a leader and prepared him for his role as Secretary General of NATO. By doing so, the authors attempt to find patterns in Rutte's leadership style from his premiership and link those findings with what can be expected from his tenure as Secretary General. Accordingly, the committees' roles show that cooperation is perhaps the most critical component for a functioning NATO. As the chair of all these committees, the Secretary General must be someone who can cooperate with and unite leaders who all have differing opinions. Further sections of this article will introduce Mark Rutte and showcase how his record, especially on the international stage, may have been the decisive factor in his appointment as NATO's Secretary General.

3. Mark Rutte

To understand why Rutte has been appointed as the new Secretary General of NATO, it is essential to comprehend how a Secretary General is appointed in the first place. Traditionally, the Secretary General is a senior politician of a European NATO ally, preferably in a leadership position.

They are appointed by member states and then hold the position for at least four years, after which re-election is possible (NATO, 2023). Mark Rutte held the highest leadership position in the Netherlands for thirteen years (Drs. M. (Mark) Rutte, n.d.-b), making him a suitable candidate for the NATO Secretary General based on the abovementioned preferred requirements. However, to answer this article's research question, the following section will focus on analysing Rutte's critical moments in his career as prime minister of the Netherlands. The country might be small, but it has experienced several crises. After thirteen years of leadership, Rutte can be labelled an experienced crisis manager. Rutte's communication style during the COVID-19 pandemic, his handling of former and possible future President of the U.S.. Donald Trump, Rutte's response to the outbreak of the Russo-Ukrainian war in terms of internal and international defence strategy, and the shooting down of flight MH17 will be examined. Doing so will indicate Rutte's preferences and leadership style in (domestic) communication- and affairs, defence strategy, and foreign affairs. These events, in particular, were selected as they are relevant to analyse all aspects mentioned above of leadership styles that the authors aim to

investigate to appoint expectations for Rutte's tenure as Secretary General of NATO.

3.1. Rutte as a Domestic Politician

Rutte's interaction with domestic affairs and communication towards the public has been described as creative in language and a prominent voice on the European Union stage. Being soft in personal relations but still firm regarding the content of political affairs (Hart & Selten, 2021). During the COVID-19 pandemic, these descriptions became evident to most as he took on the position of teambuilder. Hart & Selten (2021) described him as "onverwoestbaar optimistisch" (p.1), which translates from the Dutch to undestroyable optimistic. As prime minister, Rutte had to take on the role of crisis communicator and decision-maker, being the centre of public scrutiny.

One characteristic that sets Rutte apart from other leaders is that he is open to a broad perspective and regularly deviated from scientific advice from the Dutch COVID-19 crisis team to make way for societal needs and wants. "Those who make a lot of noise will be heard by this prime minister" (Hart & Selten, 2021, p.3). This indicates that Rutte's leadership style leaves room for the ideas and opinions of others.

Another notable aspect during the pandemic was Rutte's communication style towards his domestic population. Instead of using politically tricky words and sentences, he uses local and personal metaphors, making him feel like a fellow citizen rather than an unrelatable prime minister. Rutte arranged commonplace press conferences broadcast on national television during the COVID-19 pandemic (Hart & Selten, 2021). Notably, instead of monopolising communication rights, he made way for fellow ministers such as Hugo de Jonge and others to provide the newest guidelines and updates to the public. This last aspect is distinctive for Rutte's leadership style even until his last day in the chamber, where he engages in conversations and debates within the broader national coalition and parliament.

Additionally, more often than any previous prime minister, he provides accountability to his civil servants for his decisions (Hart & Selten, 2021). Therefore, his domestic leadership style can be summed up with the "Logos, Pathos, and Ethos-strategy" appealing to facts, emotion, and domestic norms and values (Hart & Selten, 2021, p.6).

3.2. Rutte on the Global Stage

Mark Rutte's appointment as NATO's Secretary General may be tied to his previous domestic communication and communication with other world leaders. As mentioned before, Donald Trump's return to the American political scene could be one of the challenges NATO is facing, depending on the outcome of the United States elections in November. In a meeting room at NATO headquarters in 2018, Trump pressured the leaders of other NATO allied states for not spending enough GDP on defence. He issued an ultimatum: either other countries had to step up their defence spending, or the U.S. would pull out of NATO (Foy, 2024). Of all the leaders in the room that day, including then Secretary General Stoltenberg, only Mark Rutte employed a practical approach to responding to Trump's demands; "Let's give him credit for calling us out; give him credit for getting more nations to pay up; and then promise to do more" (Foy, 2024). Foy (2024) writes that Rutte's response ticked all the boxes that prove effective with Trump: flatter, defer, and agree. Ambassador Sondland said that Rutte "has a history with him of pushing back when he thinks Trump is wrong, and he does it right to his face", which Trump finds "refreshing" (Herszenhorn, 2024).

Rutte's premiership overlapped with the entirety of Trump's presidency, from 2017 until 2021. Rutte made a name for himself by his ability to handle the often volatile then-US president, with some even dubbing him a "Trump whisperer" (Hartog and Lau, 2024).

Besides the positive aspects of Rutte's communication skills, there is a perceived weakness in Rutte's strategy for defence

spending. When it comes to defence strategy, Rutte says he believes in cooperation over sovereignty and national retreat, referencing in a speech that "the solution for tomorrow is cooperation, cooperation, and cooperation. We must not retreat into our own countries, behind walls, barriers, and borders" (Rutte, 2016, p. 11). However, Starcevic (2024) writes that Rutte had historically opposed the European Union's increasing defence budget. Under fourteen years of Rutte, the Netherlands' military spending never reached the two per cent threshold set by NATO. In 2014, the Netherlands, under Rutte, spent 1.15% of its GDP on defence spending (Lau et al., 2023). Bentinck (2018) notes that the first significant increase in Dutch military expenditures came in 2016, six years into Rutte's premiership. This increase was only to increase readiness and handle the most necessary equipment updates rather than to boost the strength of the Dutch armed forces. Bentinck (2018) notes that a lack of defence spending had even left the Dutch military incapable of meeting its Article 5 commitments, which mandates all signing parties of the North Atlantic Treaty to treat an attack on one member state as an attack on all and militarily support the attacked state (North Atlantic Treaty, 1949).

Finally, in 2024, the Netherlands is expected to reach the GDP guidelines by NATO, with defence spending expected to reach 2.03% (Lau et al., 2023). Some prominent voices, including US Senator Dan Sullivan, have expressed their opinion that his poor defence budget should have disqualified him for the role of Secretary General at NATO (Lau et al., 2023).

3.3. Rutte as a Crisis Leader

One significant event in Rutte's premiership affects this analysis's defence and international relations aspects. Described by Rutte in his farewell address to the country as the most defining moment in his career was the shootdown of Malaysia Airlines flight MH17 (Rutte, 2024). On July 17, 2014, amid Russia's aggressions in Eastern Ukraine, pro-Russian separatists shot down a Boeing 777-200ER operating a scheduled passenger flight from Amsterdam to Kuala Lumpur, killing all 298 occupants onboard (Dutch Safety Board, 2015). The separatists responsible for the attack were armed with a Buk surface-to-air missile provided by Russia meant to be used in the battle against Ukraine.

Dutch nationals were the most significant number of people on board, with 193 passengers carrying Dutch citizenship (Dutch Safety Board, 2015). The tragedy of MH17 significantly influenced Dutch foreign policy towards Russia. Before the shootdown of the Boeing 777, the Dutch stance on Russia's aggression against Crimea was to find a political solution and not introduce sanctions due, in part, to the dependence of the Dutch energy grid on Russian gas (Vitkus, 2015). MH17 changed Rutte's government's position on sanctions, as the Netherlands became one of the leading EU voices favouring sanctions against Russia (Vitkus, 2015). Even in the initial aftermath of the shootdown, the Netherlands wanted to proceed with cautious relations with Russia. Still, the Netherlands' stance toward Russia harshed as Putin continued to deny any involvement in the shootdown of the aircraft, leading to sharp public rebukes of statements from the Kremlin, as well as the publishing of tactics used by the GRU, Russia's military intelligence service (Donaldson et al., 2018). There is evidence that the shootdown of MH17 affected Rutte's worldview, leaving some to perceive him as more pessimistic (Van Willigen & Bakker, 2021). This could highlight Rutte's human-centric approach to governing. When he has dealt with situations that strike close to his heart, Rutte's decision-making seems to favour what he perceives as justice to those he serves rather than what might be in the best financial interests of his country.

4. Discussion

Reflecting on all the moments mentioned above in recent history in Mark Rutte's political life, the authors will now discuss how these specific career events can indicate what can be expected

from Rutte's leadership style with the future of NATO in his hands.

It has become evident that Rutte is a uniter of leaders. From right to left, top to bottom, Rutte has been a connecting cornerstone in international relations. These skills are also shown in the fragmented nature of politics in the Netherlands, where multiple coalitions have failed under Rutte's administration and opinions in the parliament are uncompromised (Kabinetsformaties Sinds 1945, n.d.). Working in this environment for years could reflect an outstanding breading ground for a future leader of NATO up against ensuring cooperation when interest in national sovereignty is growing, and collaboration seems more complicated than it has in decades (Kalinowski, 2022). Furthermore, in democracies, where the people have voting power, it is essential that the regular citizens believe in NATO's mission and, consequently, support more significant defence expenditures. Therefore, as a future leader of NATO, Rutte has to be favoured by the people. As proven by his tenure in the Netherlands, Rutte is an unrestricted and open communicator to ordinary citizens, providing a voice to those wanting to be heard whilst publicly presenting himself as an equal. His public management of the numerous crises in the Netherlands, primarily the handling of the COVID-19 pandemic, suggests Rutte might be a suitable candidate for this particular aspect needed from the new Secretary General.

Looking further at Rutte's relations with other leaders, as mentioned earlier, he sets himself apart in his interactions with Donald Trump. In the past, most leaders who met with Trump and had been subjected to his isolationist outbursts would sit in silence as he would go off script and mention policies that would be negative for other countries. Still, Rutte stood out for his country and the European Union. Some, such as Trump's ambassador to the European Union, Gordon Sondland, say that Trump was impressed with Rutte's response, saying it was an example of Rutte's Dutch directness (Herszenhorn, 2024).

We will presumably never know whether Rutte's response to Trump prevented the ex-president from pulling the U.S. out of NATO. However, should Donald Trump be re-elected in November, a NATO headed by someone who has, so far, possessed an effective strategy towards him, which differs from that of most other leaders, will likely be more resilient. Contrastingly, while this article found evidence that Rutte has a talent for uniting leaders and building consensus, many take issue with his past views on defence spending. His defence policy has shifted over the years, and while he appears to have toughened his views on spending more recently, his lax defence policy is a cause for concern. Even if Rutte, as Secretary General, were to attempt to persuade NATO allied nations to increase their defence spending, he would very likely face questions about his past aversion to significant defence expenditures.

On an international level, Rutte's response to MH17 about his defence spending and stance on Russian sanctions show that his core positions and beliefs are not set in stone and can be influenced. Van Willigen and Bakker (2021) show that the shootdown of a passenger jet carrying over 100 Dutch citizens deeply impacted Rutte's worldview and stance towards Russia.

Based on his handling of past crises, Mark Rutte meets the particular demands and qualities that seem critical for the Secretary General of NATO, given the organisation's current challenges.

5. Conclusion

Rutte is effective at reaching deals and uniting people. Still, certain past positions, most notably his lax defence policy as prime minister of the Netherlands, could cause concern for his tenure as Secretary General. However, given that his small defence budget was well known by the leaders of NATO member states - those who endorsed him as the new Secretary General - perhaps it can be assumed that Rutte's strong qualities as a consensus builder were prioritised over questions of defence spending. The current political landscape in Europe and the U.S. could explain this with the rise of right-wing conservative parties and the possible return of Trump as president of the most significant financial contributor of the alliance. Given the roles of NATO's Secretary General, as mentioned in Chapter 1, Rutte's reputation as a uniting voice makes sense, given that the Secretary General is less involved in policy making and more involved in mediation roles. What do these findings mean regarding the research question of:

"What can be expected from Mark Rutte as Secretary General of NATO, given his thirteen years of crisis management as prime minister of the Netherlands?" This article finds that Rutte can be expected to act as an alliance- and cooperation builder rather than a firm decision-maker twisting the arms of NATO members regarding their defence spending. The latter might lead NATO into further stress later down the road of his tenure as Secretary General, especially if Trump were to be reelected and carry out his previously made warnings of cutting down NATO's funding by the U.S.. Contrastingly, Rutte can be expected to use this role to influence and perhaps ease the needs and wants of the more rigid leaders within the organisation, especially regarding Trump. Looking at NATO, this could guide his approach to Russia's offensive actions against Ukraine and might lead him to take a more hawkish stance against the Kremlin. Only time will tell what Mark Rutte brings to NATO as its Secretary General. It will be interesting to monitor and analyse new developments in Rutte's NATO over the years to come.

References

Archick, K., Belkin, P., & Bowen, A. S. (2024). NATO Enlargement to Sweden and Finland. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11949

Arnold, R. (2023, April 4). Finland flag raising at NATO Headquarters 4 April 2023. Wikimedia. https://commons.wikimedia.org/wiki/File:Finland_flag_raising_at_NATO_Headquarters_4_April_2023.jpg

Bentinck, M. (2018, February 8). Why the Dutch Military Punches Below Its Weight. carnegieendowment.org/. https://carnegieendowment.org/europe/strategic-europe/2018/02/why-the-dutch-military-punches-below-its-weight

Churchill, W., & Roosevelt, F. D. (Eds.). (1941). The Atlantic Charter. https://www.fdrlibrary.org/documents/356632/390886/atlantic_charter.pdf/30b3c906-e448-4192-8657-7bbb9e0fdd38

Cunningham, K., Hix, S., Dennison, S., & Learmonth, I. (2024, January 23). A sharp right turn: A forecast for the 2024 European Parliament elections. Ecfr. eu. https://ecfr.eu/publication/a-sharp-right-turn-a-forecast-for-the-2024-european-parliament-elections/

Donaldson, K., Akkermans, J., & Meyer, H. (2018, October 4). Spy Bust Exposes Methods of Putin's GRU Military Hackers. Bloomberg. https://www.bloomberg.com/news/articles/2018-10-04/russia-attempted-to-hack-un-probe-of-salisbury-spy-poisoning

Drs. M. (Mark) Rutte. (n.d.-b). parlement.com. https://www.parlement.com/id/vg9fgoprkxw3/m_mark_rutte

Dutch Safety Board. (2015). MH17 Crash Final Report. In onderzoeksraad.nl. https://onderzoeksraad.nl/wp-content/uploads/2023/11/debcd724fe7breport_mh17_crash.pdf

Foy, H. (2024, July 4). The untold story of the most chaotic Nato summit ever. Financial Times. https://www.ft.com/content/8985b970-0015-479f-9585-7a9b234715a4?

Hart, P. '., & Selten, F. (2021, January 22). Mark Rutte's crisisleiderschap: Laverend op zoek naar staatsmanschap. StukRoodVlees. https://stukroodvlees.nl/mark-ruttes-crisisleiderschap-laverend-op-zoek-naar-staatsmanschap/

Hartog, E., & Lau, S. (2024, February 23). 'The Trump whisperer' – Can Mark Rutte save NATO? POLITICO. https://www.politico.eu/article/mark-rutte-nato-donald-trump-vladimir-putin/

Herszenhorn, M. (2024, June 20). NATO hopes to Trump-proof the alliance with new chief Mark Rutte. It could backfire. Politico. https://www.politico.com/news/2024/06/20/nato-new-chief-trump-00164340

Jacqué, P., & Ricard, P. (2024, June 5). War in Gaza: The European Union's diplomatic failure. Le Monde.fr. https://www.lemonde.fr/en/international/article/2024/06/05/war-in-gaza-the-eu-s-diplomatic-failure_6673792_4.html

Kabinetsformaties sinds 1945. (n.d.). Parlement.com. https://www.parlement.com/id/vh8lnhrsr2z2/kabinetsformaties_sinds_1945

Kalinowski, T. (2022, October 20). Why international cooperation is failing – and why it can still work. https://www.rifs-potsdam.de/en/blog/2022/10/why-international-cooperation-failing-and-why-it-can-still-work

Lindsay, J. M. (2024, April 26). Election 2024: Is Donald Trump an isolationist? Council on Foreign Relations. https://www.cfr.org/blog/election-2024-donald-trump-isolationist

Milestones in the history of U.S. Foreign Relations - Office of the Historian. (n.d.). https://history.state.gov/milestones/1945-1952/nato

North Atlantic Treaty (1949). Wikisource, the Free Online Library. https://en.wikisource.org/wiki/North_Atlantic_Treaty

North Atlantic Treaty Organization. (n.d.). Lord Ismay. https://www.nato.int/cps/en/natohq/declassified_137930.htm

North Atlantic Treaty Organization [NATO]. (2022, May 9). Nuclear Planning Group (NPG). https://www.nato.int/cps/en/natohq/topics_50069.htm

North Atlantic Treaty Organization [NATO]. (2023, August 18). NATO Secretary General. https://www.nato.int/cps/en/natohq/topics_50094.htm

North Atlantic Treaty Organization [NATO]. (2024, July 26). Funding NATO. https://www.nato.int/cps/en/natohq/topics_67655.htm

North Atlantic Treaty Organization [NATO]. (2024a, June 18). Defence expenditures and NATO's 2% guideline. https://www.nato.int/cps/en/natohq/topics_49198.htm

North Atlantic Treaty Organization. (2024b, July 10). Washington Summit Declaration [Press release]. https://www.nato.int/cps/en/natohq/official_texts_227678.htm

North Atlantic Treaty Organization [NATO]. (2024c, March 21). North Atlantic Council. https://www.nato.int/cps/en/natohq/topics_49763.htm

North Atlantic Treaty Organization [NATO]. (2024d, July 3). Euro-Atlantic Partnership Council. https://www.nato.int/cps/en/natohq/topics_49276.htm

North Atlantic Treaty Organization [NATO]. (2024e, March 28). International Staff. https://www.nato.int/cps/en/natohq/topics_58110.htm

Lau, S., Gould, J., & Ward, A. (2023, November 23). NATO front-runner Mark Rutte faces flak over low Dutch defence spending. POLITICO. https://www.politico.eu/article/nato-mark-rutte-low-dutch-defense-spending/

Reuters. (2024, May 31). Fact Check: US contributes 16% of NATO annual budget, not two-thirds. Reuters. https://www.reuters.com/fact-check/us-contributes-16-nato-annual-budget-not-two-thirds-2024-05-31/

Rutte, M. (2024, June 30). Afscheidsboodschap van minister-president Rutte aan Nederland. Farewell Address, The Hague, Netherlands. https://www.rijksoverheid.nl/documenten/toespraken/2024/06/30/afscheidsboodschap-van-minister-president-rutte-aan-nederland

Shapiro, J. (2024, June 14). World is looking 'more like the 1930s', Future Fund warns. Australian Financial Review. https://www.afr.com/policy/economy/world-is-looking-more-like-the-1930s-future-fund-warns-20240614-p5jlsm

Starcevic, S. (2024, June 28). EU leaders chided Rutte over opposition to joint defense spending, Tusk says. POLITICO. https://www.politico.eu/article/eu-leaders-chided-rutte-over-opposition-to-joint-defense-spending-tusk-says/

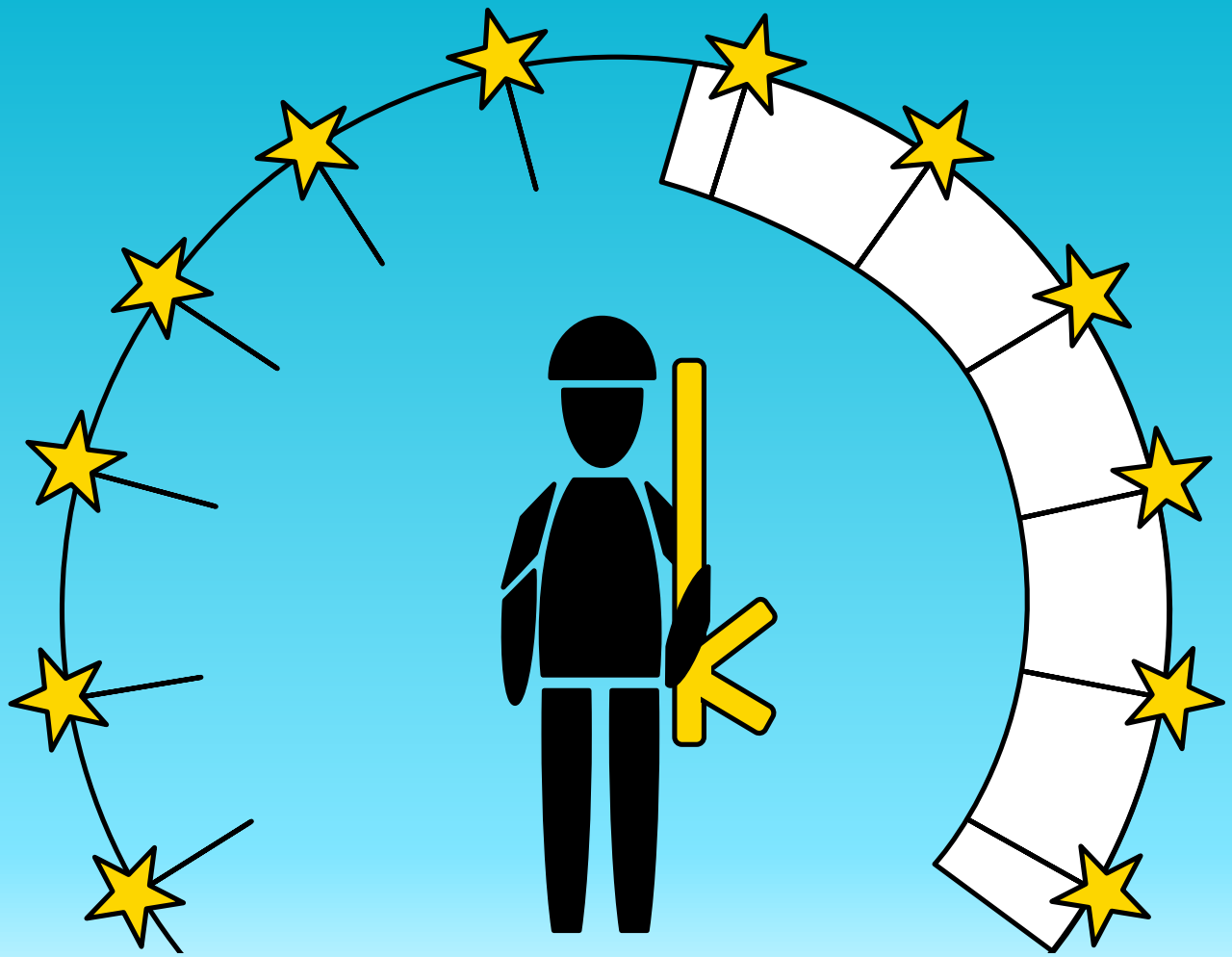
Sterling, T. (2022, August 2). Mark Rutte becomes Netherlands' longest-serving prime minister. Reuters. https://www.reuters.com/world/europe/mark-rutte-becomes-netherlands-longest-serving-prime-minister-2022-08-02/

Treaty of Brussels (1948). Wikisource, the Free Online Library. https://en.wikisource.org/wiki/Treaty_of_Brussels

Treaty of Dunkirk (1947). Wikisource, the Free Online Library. https://en.wikisource.org/wiki/Treaty_of_Dunkirk

Van Willigen, N., & Bakker, F. E. (2021). Trauma and belief systems; an operational code analysis of Dutch Prime Minister Rutte and the downing of flight MH17. Risk Hazards & Crisis in Public Policy, 12(2), 215–233. https://doi.org/10.1002/rhc3.12209

Vitkus, G. (2015). Towards Stronger Normative Power: The Nature of Shift in EU Foreign Policy in the Context of the Crisis in Ukraine. European integration studies, 9, 8-19.



Short Term Protection, Long Term Struggles

What More Can the European Union Do for Refugees?

Mara Sandru

Mara Sandru is a MA student in European Public Affairs at Maastricht University. Mara's passions include public policy and external relations in the security and defence realm, EU law, and migration.

1. Temporary Protection Directive: The "Sleeping Beauty" of the EU

The Russian full-scale invasion of Ukraine that started in February 2022 not only only brought war back to Europe's borders, but also its devastating consequences on areas such as the economy and society. The invasion has led to one of the worst refugee crises in recent history with roughly 10 million Ukrainians being displaced that gained refugee status (United Nations High Commissioner for Refugees, 2022). Compared to other crises, the European Union (EU) arguably had a rather swift response. In March 2022, the Temporary Protection Directive (TPD) was finally set in motion for the first time after its adoption in 2001 (European Council, n.d.).

This policy brief aims at answering the following questions: How effective is the European Union's Temporary Protection Directive in managing large-scale refugee crises, such as the Ukrainian refugee crisis? and What reforms are necessary to address its limitations and ensure long-term protection and integration for displaced populations?

The structure of the policy brief is as follows. First, a short introduction into the TPD will shed light into this protection instrument. Second, the brief addresses its limitations. Third, another policy option – the Long-Term Residents Directive – is being assessed. Fourth, several challenges in the EU's response are being addressed, e.g. financial shortcomings, the role of civil society and EU agencies, concerns about human rights, double standards in EU responses to crises and integration challenges. Finally, the policy brief proposes key recommendations, before ending with a conclusion. While this action was widely welcomed and praised, it is relevant to note the shortcomings of this instrument, mainly its temporary aspect. The TPD was initially implemented as a forceful reaction to the refugee issue that was brought about by the dissolution of former Yugoslavia and the wars that followed in the 1990s (Motte-Baumvol et al., 2022). The Directive only comes into effect when a large number of displaced people from third countries enter an EU Member State and are unable to return home, although the Council of the European Union (hereinafter: the Council) is the sole actor deciding what amounts to such a "mass influx" (Motte-Baumvol et al., 2022, p. 12). In this context, a third country national is a person that comes from a "country that is not a member of the European Union, as well as a country or territory whose citizens do not enjoy the European Union right to free movement [...]" (European Commission, 2024). The objectives of this instrument are twofold: firstly, it aims at setting minimum requirements for providing temporary protection and, secondly, ensuring balanced efforts among Member States (Kerber, 2022). Within the TPD, temporary protection, as outlined in Article 2(a), entails immediate protection to displaced people from third countries during mass influxes, ensuring the asylum system can handle the influx effectively, benefiting affected individuals and others seeking protection (European Parliament & Council of the European Union, 2001). The ongoing conflict between Ukraine and Russia led to more than 6 million (Frontex, 2022) displaced and vulnerable persons that, in their search for security and stability, sought refuge in the EU neighbouring countries, which bear the highest cost from this influx of migrants. Nevertheless, the activation of the TPD might be considered a success. Not only it established a precedent for migration-related issues and lessons to be taken

Temporary Protection:

Temporary protection is the immediate protection to displaced people from third countries during mass influxes, ensuring the asylum system can handle the influx effectively, benefiting affected individuals and others seeking protection.

for the future, but it showed that the EU can speak with one voice and it ensured that limited administrative resources were not overextended. However, despite its advantages, this is just the tipping point of the Ukrainian refugee crisis, and the EU officials should not pat themselves on the back and consider this job done. They should rather insist on a long-term and proactive mechanism for future refugee crises and for the integration of the current Ukrainian migrants. Because of the current limitations of the TPD, the EU should focus on forward looking policies by stressing the following aspects: (i) capacity-building; (ii) integration and social cohesion; and (iii) inclusive protection.

2. Critique of the Temporary Protection Directive

The TPD is Running Out of Time. In order to understand what other policy options for the protection of Ukrainian refugees there are, it is important to look at the TPD more in depth. The purpose of this Directive is, among other things, to prevent overburdening a country's asylum system and to streamline procedures (Trauner & Valodskaite, 2022). Additionally, as the name suggests, it is a temporary mechanism that will come to an end, eventually, under the following conditions laid out in Article 6(1) of the Directive: a) the maximum extension has lapsed; b) before the expiration deadline, the European Commission (hereinafter: the Commission) submits a proposal that the Council shall approve through qualified majority voting (European Parliament & Council of the European Union, 2001). The Council has already extended the TPD to the fullest extent allowed by law, thus this system is set to end on the 4th of March 2025, yet the most important aspect is that the TPD, under no circumstance can last more than three years. Therefore, the EU cannot and should not wait until the TPD expires, which is why I recommend considering a more future oriented policy option.

The second option is that the Union decides to end the TPD before the deadline, should the war end or the parties agree to ceasefire. However, there are other conditions that must be fulfilled.

Figure 1: Refugees from Ukraine at the main railway station in Rzeszow, Poland (EU Civil Protection and Humanitarian Aid, 2022)

For instance, for the return of the person that received such temporary protection, the country of origin must be considered a safe destination, according to international accords, such as the European Convention on Human Rights or the Refugee Convention (Ineli-Ciğer, 2023). Unfortunately, there are no reasons that suggest the necessary developments for the activation of the second clause as of now. Also, the political environment is not yet suitable to amend the TPD to extend it beyond its legal limit, which only makes it more important that the EU looks at the future integration of Ukrainians.

3. What Will the EU Do Now?

The European Union has already prepared some scenarios, although there should also be a strong political will to implement them. For instance, the three current scenarios entail amending, extending or even re-activating the TPD, creating a new protection or residence status under EU law or amending other EU legal migration laws (European Parliament, May 2024). Such a policy that could and should be amended is the Long-Term Residents Directive (LTRD). Shortly, this Directive allows persons to become long-term residents if they have been lawfully residing in an EU Member State for five continuous years. According to Articles 5 and 6 of the Directive, this can be achieved if the person in question has a reliable source of income, health insurance, has complied with the relevant integration procedure mandated by the MS and does not pose a public threat (European Parliament & Council of the European Union, 2003). Some of the biggest benefits of this Directive are the permanent residency permit and the equal treatment that allows them to access services, rights and privileges, ensuring a smoother integration process (Ineli-Ciğer, 2023).

3.1. The Illusion of Protection?

Despite its advantages, the current setting of the LTRD has the immense disadvantage of not protecting any Ukrainian refugees because, as of March 2025, not a single refugee will have spent the required time on EU territory. Even though the LTRD is not applicable now, it is still relevant to discuss its shortcomings, should it be amended soon or enforceable in a couple of years. This Directive requires people to live continuously in one EU country for five years to be eligible for long-term residency. However, according to data from the OECD and the EU Asylum Agency, only 66% of those surveyed applied for temporary protection in the country they preferred. This means that if someone is not in their preferred country yet and does not plan on staying there, the time spent there will not count towards the five-year requirement. As a result, some people have to spend extra time and resources before benefiting from the Directive. Additionally, many families travel back and forth between the EU and Ukraine. Although the Directive allows for short absences (Article 4(3)), the allowed time away is often too short, forcing Ukrainians to make difficult choices.

Moreover, women are particularly vulnerable as the Directive requests a consistent income which might be lacking because of their caregiving responsibilities, especially when there are no such facilities (Ineli-Ciğer, 2023). Hence, I welcome the steps taken by the European Commission that is currently amending this Directive, albeit small.

3.2. Money, Money, Money

The Council of the EU announced that EU funds will be provided for all Member States for their efforts from the decision to activate TPD (Council of the European Union, 2022), but the question is whether these funds were enough to begin with. To mention just one, the Asylum, Migration and Integration Fund (AMIF) has around 10 billion euros available for a span of seven years. The fund is supposed to be used for an effective control of migration flows, as well as for the establishment and development of immigration and asylum policies, which include integration too (Motte-Baumvol et al., 2022). Its shortcomings stem from the fact that 60% of the money has already been pre-assigned to

Member States (Rasche, 2022), which not only means that frontline Member States are most likely underfunded, but also that the rest of the fund, circa one third, is allocated to emergency aid (Motte-Baumvol et al., 2022), which is insufficient.

The current financial arrangement makes people wonder whether there are enough resources available. Frontline Member States may face significant pressures if allotted aid is insufficient to address spikes in the number of refugees arriving or a prolonged humanitarian crisis. Moreover, the International Monetary Fund (IMF) predicted that the costs of supporting refugees might total between 30 and 37 billion euros only in 2022 across the Union, which usually is 0.2% of the GDP. Yet, in frontline states these costs could amount to 1% of their GDP (Bird & Noumon, 2022) and, while short-term, they still pose a significant burden on such states (Rasche, 2022).

4.1. The EU Needs People...

Besides financial aid, the Member States that border Ukraine also needed manpower, which in the early moments of the war, came from the civil society. At EU level, after the activation of the TPD, the European Commission created a Solidarity Platform in which Frontex, Europol and the European Union Asylum Agency (EUAA) are involved (Carrera et al., 2022). The purpose of the platform is more for monitoring and information exchange to avoid and prevent double registrations, as well as potential violations of the TPD (PubAffairs Bruxelles, 2022). As one can expect, the border crossings were flooded by migrants and in states such as Poland, the waiting time could reach a few hours. The Commission announced that Frontex and Europol staff were already present in some of the Member States (Carrera et al., 2022) , but there seems an overall belief that efforts could have stepped up. There are reports of members from the civil society who may feel overworked or left on their own when state-run facilities that were supposed to house refugees were lacking (Rasche, 2022). These actors have already made it clear to these authorities that there is an urgent need for increased coordination and support (International Rescue Committee, 2022).

4.2. ...and the People Need the Help of the EU

Because the authorities and the civil society were at the forefront of the highest migration streams, they also witnessed the "dark face" of migration. Most of those that arrived are vulnerable and unaccompanied, without any means of help from friends and family (International Rescue Committee, 2022). Other vulnerable groups include unaccompanied and separated children, children travelling with unrelated adults, disabled individuals, minorities like Roma and LGBTQI+ people, and those unable to obtain temporary protection due to incomplete or incorrect information (Näre & Tkach, 2024).

Although some people sought to take advantage of their vulnerabilities, authorities quickly discovered abuses of such kind and other human rights breaches happening at the borders. For instance, there were reports from the Polish and Romanian borders of men luring (young) women by promising them rides, shelter and work (The Associated Press, 2022). Experts warn of traffickers that profit from families' weaknesses, people who run the risk of being pushed into prostitution, forced begging, and forced criminality due to trafficking (Näre & Tkach, 2024). Psychologists stress the emotional strain and trauma that the refugees had to endure (The Associated Press, 2022), which shows the clear and urgent need for coordinated support between civil society, national authorities and EU agencies.

4.3. Everybody Is Welcome, Except Some More Than Others

In between the adoption of the TPD and the war on Ukraine, Europe has been hit by multiple migration waves, such as those following the "Arab Spring" and the conflicts in Libya, Syria, Afghanistan (Carrera et al., 2022). Yet, for

neither of these, was the Directive set in motion. Some claimed that the reason for the non-activation was the unpreparedness of the Union or the existence of better suited tools (Trauner & Valodskaite, 2022), while others argue that the 2015 wave was mainly composed of people with whom Europeans do not share many similarities (e.g.: non-Europeans, Muslims, mostly men), which hindered the help. This double standard could also be seen during the 2022 wave, as Ukrainians were welcomed with open arms, while third country nationals (TCNs) coming from countries such as India, Nigeria or Sudan not so much (Busari et al., 2022, March 4). For Ukrainians, the TPD applies, while for TCNs, it is up to the MS whether to extend its application, as this process is voluntary (Ineli-Ciğer, 2022). When the war started, Ukrainians could enter the EU because of the visa-free agreements with the Union, while there have been reports of TCNs being stuck at borders, not being allowed to enter. In light of such abuses, some have been very vocal about

> **"the discriminatory and xenophobic life-threatening treatment of non-white third country nationals and asylum seekers from African, Asian and Middle East countries"**
>
> (Carrera et al., 2022, p. 2).

Lastly, even if the war would end soon, the reconstruction of Ukraine would still be a long and costly project, thus one can expect Ukrainians and TCNs to stay in the EU longer than anticipated. Some might not even go back (Ho et al., 2022), which only reinforces the need for social cohesion and integration of migrants. Migration is not an easy process for either migrants or the host countries and this wave is particularly important to look at because of its composition of "elderly, children and women of working age" (Botelho, 2022).

Moreover, according to Eurostat (2024), out of all TPD beneficiaries, women make up 46.2%, while children 33.2%, the two categories that need the most support.

Firstly, the need to integrate is the most difficult for females because of their responsibilities, which are obstacles to obtaining necessary services, as well as to their chance for respectable and safe employment. Reports have shown that integration into a host country's labour market depends on whether there is a skill mismatch. Therefore, these are real concerns for the Ukrainian migrants, who typically already completed their higher education, might land low-paying positions that do not align with their background or abilities (Bird & Noumon, 2022). Other obstacles are language, lack of facilities/ services or accreditations, as well as bureaucratic differences (Botelho, 2022).

Secondly, as already mentioned, the border Member States will bear the most costs in the short term because of government spending on essential services, such as education, health care and housing, while in the long run, migrants will help with the economic growth (Pogarska et al., 2023).

Thus, it is important to understand that these short-term costs, but long-term benefits are closely connected.

5. Key Recommendations

All things considered, the EU took some positive steps towards migration, if there is political will. However, the relative success coming from the activation of the TPD and its possible continuation through the LTRD are not without flaws. One should not look only at the LTRD as it is, but in

European Countries (excluding Russia)	Absolute number of refugees	Percentage
Germany	1,178,610	31.50%
Poland	957,505	25.63%
Czech Republic	353,510	9.40%
United Kingdom	244,560	6.54%
Spain	202,690	5.42%
Italy	170,925	4.57%
Moldova	123,295	3.30%

Figure 2: Ukrainian Migrants in EU Member States as of 2024 (Source)

order for the refugees to truly benefit from these policies, there is a need for a comprehensive approach, that should include the elements listed below. Thus, considering the previous arguments, I argue for the following...

Firstly, the current design of the LTRD does not allow the beneficiaries to make use of it to the fullest extent. For that I suggest the following:

- Allowing beneficiaries to total the years they spent in a maximum of two Member States rather than having to spend five years in one Member State.
- Increasing the maximum allowed time of absence from 10 months to at least 12, which would allow Ukrainians to briefly go back, while still retaining their legal status.
- Less stringent financial requirements for women that could benefit from the LTRD, but that do not meet the criteria due to the obstacles faced.

Secondly, we have seen that the European Union is not fully equipped to financially sustain either the Member States or the refugees, as illustrated by the Commission scrambling for funds, which ultimately came from various places. For that, I recommend streamlining the available funds, so that they are easy and ready to be accessed.

- Allowing beneficiaries to total the years they spent in a maximum of two Member States rather than having to spend five years in one Member State.
- Other recommendations entail offering tailored approaches and (financial) support as the many frontline Member States have different needs, depending on their national resources and streams of migration.
- There is an urging need for the EU to pay more attention and make funds more accessible to local authorities and civil society organisations. These two actors can assess their and the refugees' needs the best since they do the most work on the ground.
- In order to increase preparedness and reception capabilities, I recommend dividing material resources between Ukraine and the border states, as there is a pressing need for

"dignified and sufficient reception conditions" (International Rescue Committee, 2022).

- One cannot talk about long-term residence without integration and for that, I suggest the Commission increase funding in the essential areas of living (e.g.: education, health care, housing etc.) in the frontline Member States.

Thirdly, as previously argued, there is a need for support at reception centres. Hence, I believe that the Solidarity Platform should be boosted from information to personnel exchange. Members of Frontex and Europol would be mandated to help the national authorities to conduct checks at the borders and ease the burden in the neighbouring Member States.

- Considering the large amount of women and children that are crossing the borders and their increased vulnerability, the aforementioned agencies would also examine the reception centres and prevent abuses and human rights violations from happening, with the help of the European Union Agency for Fundamental Rights, which would have a monitoring role.
- Additionally, Child Protective Services should also be present to aid the authorities in tracing families, reuniting them in offering support for (unaccompanied) minors.

Lastly, I urge the Commission and the Member States to not apply double standards, but to award fair and equal treatment to all refugees, regardless of their "citizenship, nationality, religion, or ethnicity"

(International Rescue Committee, 2022).

6. Conclusions

The TPD can be seen as a necessary change in the context of how the EU responds to the influx of Ukrainian refugees, providing millions with shelters and rights. It has to be said that the shortness of the TPD shows that there are limitations as to how such instruments can be useful in long-term crisis management. There is a recognition that moving forward there has to be a more sustained approach, such as legal instruments that can assist long-term refugees. The current or future policy options are worrying because of their limitations on the movement of people and financial or logistical constraints on the frontline Member States. Taking all these issues into consideration, the EU needs to take a further step and quickly revise its legal framework in order to form more effective and protective options when dealing with refugees.

This includes loosening residency requirements, raising the level of financial support and strengthening collaboration of civil society, local governments, and EU agencies.

Additionally, the EU must ensure that issues of discrimination will be addressed and that equitable status for all refugees, irrespective of their nationality will be provided. All in all, what this paper attempts is to transform and appropriate the experience of the Ukrainian crisis by projecting it onto other policy challenges having more to do with solidarity, planning and adjustments, in the face of neverending wars.

References

Bird, N., & Noumon, N. (2022, December 15). Europe Could Do Even More to Support Ukrainian Refugees. IMF Blog. https://www.imf.org/en/Blogs/Articles/2022/12/15/europe-could-do-even-more-to-support-ukrainian-refugees

Botelho, V. (2022, June 20). The impact of the influx of Ukrainian refugees on the euro area labour force. European Central Bank. https://www.ecb.europa.eu/press/economic-bulletin/focus/2022/html/ecb.ebbox202204_03~c9ddc08308.en.html

Busari, S., Princewill, N., Nasinde, S., Tawfeeq, M. (2022, March 4). Foreign students fleeing Ukraine say they face segregation, racism at border. CNN. https://edition.cnn.com/2022/02/28/europe/students-allege-racism-ukraine-cmd-intl/index.html

Carrera, S., Ineli-Ciğer, M., Vosyliute, L., & Brumat, L. (2022). The EU grants temporary protection for people fleeing war in Ukraine. CEPS Policy Insights, 9.

Council of the European Union. (2022, March 4). Implementing Decision 2022/382 establishing the existence of a mass influx of displaced persons from Ukraine within the meaning of Article 5 of Directive 2001/55/EC, and having the effect of introducing temporary protection. Official Journal of the European Union, L 71/1-6.

EU Civil Protection and Humanitarian Aid. (2022). EU Civil Protection in Poland. Flickr. https://www.flickr.com/photos/eu_echo/51942393272

European Council. (n.d.). Refugees from Ukraine in the EU. Retrieved May 21, 2024, from https://www.consilium.europa.eu/en/infographics/ukraine-refugees-eu/#0

European Parliament & Council of the European Union. (2001, July 20). Directive 2001/55/EC on minimum standards for giving temporary protection in the event of a mass influx of displaced persons and on measures promoting a balance of efforts between Member States in receiving such persons and bearing the consequences thereof. Official Journal of the European Union, L 212/12-23.

European Parliament & Council of the European Union. (2003, November 25). Directive 2003/109/EC on the status of third-country nationals who are long-term residents. Official Journal of the European Union, L 16/44-53.

Eurostat. (2024, February 8). Over 4.3 million people under temporary protection. Eurostat. https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20240208-1#:~:text=On%2031%20December%202023%2C%204.31,protection%20status%20in%20the%20EU.

Frontex. (2022, May 12). Update on Ukraine: more than 6 million refugees cross EU's borders [Press release]. https://www.frontex.europa.eu/media-centre/news/news-release/update-on-ukraine-more-than-6-million-refugees-cross-eu-s-borders-xgNX2Q

Ho, M. S. D., Deen, B., & Drost, N. (2022). Long-term protection in Europe needed for millions of Ukrainian refugees. Clingendael Institute.

Ineli-Ciğer, M. I. (2023, September). When Temporary Protection Ends: longer-term solutions for refugees from Ukraine. Swedish Institute for European Policy Studies. https://www.sieps.se/globalassets/publikationer/2023/2023_11epa.pdf

International Rescue Committee. (2022, March 8). As people continue to flee Ukraine, Europe must turn its promises of protection into a lasting reality. https://www.rescue.org/

Kerber, K. (2002). The temporary protection directive. European Journal of Migration and Law, 4(2), 193-214.

Motte-Baumvol, J., Mont'Alverne, T. C. F., & Braga Guimarães, G. (2022). Extending social protection for migrants under the European Union's temporary protection directive: lessons from the war in Ukraine. Available at SSRN 4096325. http://dx.doi.org/10.2139/ssrn.4096325

Näre, L. & Tkach, O. (2024, May, 21). The temporary protection of Ukrainian refugees: a model for the future or a case of discriminatory exceptionalism?. Mixed Migration Centre. https://mixedmigration.org/temporary-protection-ukrainian-refugees/

Pogarska, O., Tucha, O., Spivak, I., & Bondarenko, O. (2023, March 7). How Ukrainian migrants affect the economies of European countries. CEPR. https://cepr.org

PubAffairs Bruxelles. (2022, May 31). Solidarity with Ukraine: Commission launches an EU platform for registration of people enjoying temporary protection or adequate protection under national law. https://www.pubaffairsbruxelles.eu/eu-institution-news/solidarity-with-ukraine-commission-launches-an-eu-platform-for-registration-of-people-enjoying-temporary-protection-or-adequate-protection-under-national-law/

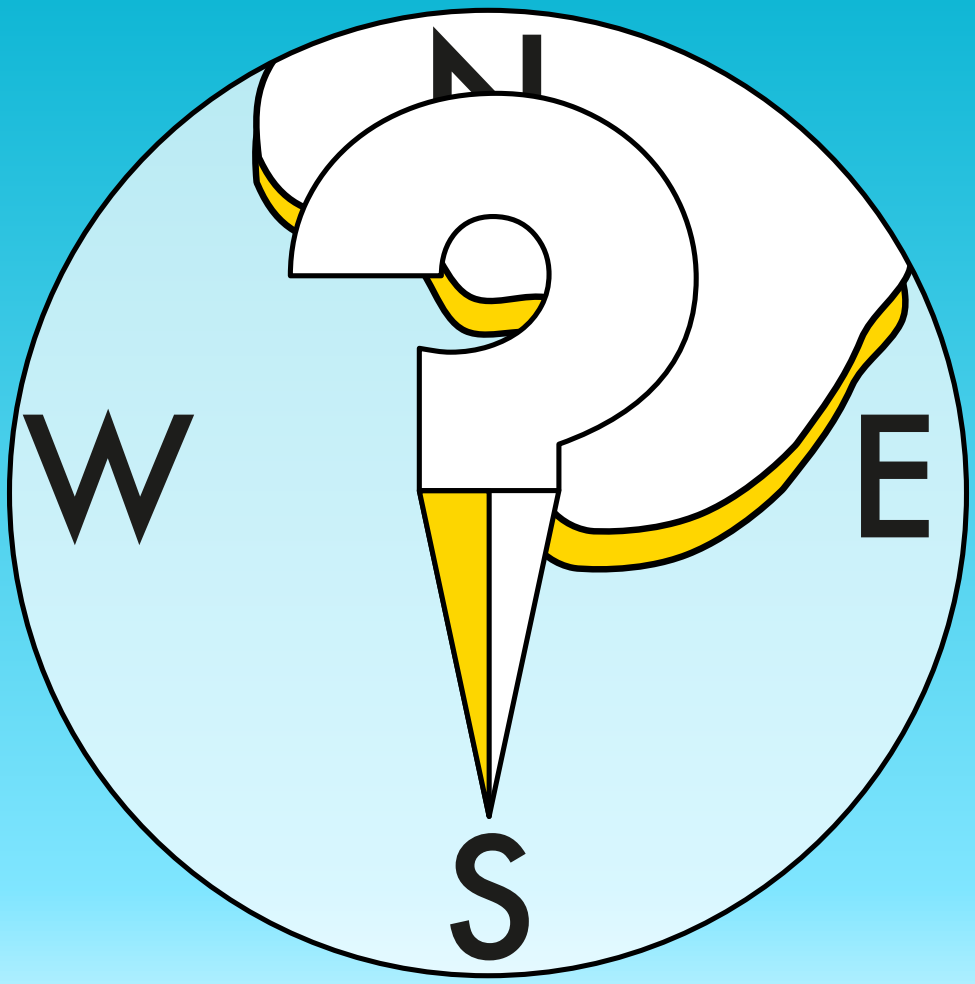
Rasche, L. (2022). Implementing temporary protection in the EU. Policy Brief. https://www.delorscentre.eu/fileadmin/2_Research/1_About_our_research/2_Research_centres/6_Jacques_Delors_Centre/

Publications/20220623_Rasche_Temporary_protection.pdf

The Associated Press. (2022, March 12). Concern Grows Over Traffickers Targeting Ukrainian Refugees. Voa News. https://www.voanews.com

Trauner, F., & Valodskaite, G. (2022). The EU's Temporary Protection Regime for Ukrainians: Understanding the Legal and Political Background and Its Implications. In CESifo forum (Vol. 23, No. 04, pp. 17-20). München: ifo Institut-Leibniz-Institut für Wirtschaftsforschung an der Universität München.

United Nations High Commissioner for Refugees. (2022, March 31). UN High Commissioner for Refugees calls for immediate end to Ukraine war, which has uprooted over 10 million people [Press release]. https://www.unhcr.org/news/news-releases/un-high-commissioner-refugees-calls-immediate-end-ukraine-war-which-has-uprooted



Arctic Exceptionalism

Navigating Challenges in a Changing Region

Jonathan Barry

Jonathan Barry is a former senior advisor to the Canadian Minister of National Defence. He is currently pursuing a Master in Public Affairs at Princeton University.

1. Introduction

The concept of Arctic exceptionalism is central to discussions about the the region's governance and international relations. Introduced by Mikhail Gorbachev in his pivotal 1987 Murmansk Speech, he envisioned the Arctic as a "zone of peace" insulated from the geopolitical tensions that defined the Cold War. This notion emphasised cooperation over conflict, promoting environmental protection, scientific research, and peaceful collaboration among Arctic nations [(Gorbachev, 1987)].

In recent years, however, Arctic exceptionalism has been challenged. The accelerating impacts of climate change have made the Arctic's resources more accessible, drawing increased attention from global powers. The geopolitical landscape shifted dramatically following Russia's 2022 invasion of Ukraine, disrupting the collaborative spirit among the eight Arctic states. Despite these tensions, the Arctic's unique geopolitical, environmental, and strategic importance continues to shape its future.

2. The Strategic Importance of the Arctic

The Arctic has become a focal point of global strategic interest due to its vast natural resources, emerging shipping routes, and significant geopolitical positioning. The region is estimated to contain approximately 13% of the world's undiscovered oil and 30% of its untapped natural gas reserves, making it critical for future energy exploration [(U.S. Geological Survey, 2008)]. As climate change accelerates the melting of Arctic sea ice, new maritime passages like the Northern Sea Route (NSR) and the Northwest Passage are becoming more navigable, potentially reducing shipping times between Asia, Europe, and North America [(Smith & Stephenson, 2013)].

Russia has heavily invested in its Arctic infrastructure and military capabilities, reopening Soviet-era military bases and developing the world's largest fleet of icebreakers, including nuclear-powered vessels. This expansion aims to secure control over the NSR and capitalise on resource extraction, raising concerns about the militarization of the region [(Østhagen, 2020)]. The United States and its allies have responded by increasing their military presence and enhancing their strategic posture in the Arctic [(U.S. Department of Defense, 2019)].

China, declaring itself a "near-Arctic state," seeks to establish a foothold in the region through its Polar Silk Road initiative, aiming to access resources and new trade routes [(State Council Information Office of the People's Republic of China, 2018)]. These developments have heightened global competition in the Arctic, with non-Arctic nations asserting interests that challenge traditional governance structures.

Despite these strategic competitions, the Arctic remains an area where limited cooperation is both possible and necessary. The harsh environment and the challenges posed by climate change require collaborative efforts for search and rescue operations, environmental protection, and addressing the needs of Indigenous communities. Maintaining open lines of communication, even if limited, is essential to manage risks and ensure safety in the region.

3. Environmental and Governance Challenges

The Arctic is experiencing climate change at a rate nearly three times faster than the global average, leading to unprecedented environmental shifts [(AMAP, 2021)]. Sea ice is diminishing, permafrost is thawing, and ecosystems are being disrupted, affecting not only the environment but also the livelihoods of Indigenous peoples.

Historically, the Arctic Council has played a critical role in fostering cooperation on these issues. Established in 1996, it serves as the primary forum for collaboration among Arctic states and Indigenous peoples, focusing on

environmental protection and sustainable development [(Arctic Council, 1996)].

The Council has been instrumental in producing comprehensive environmental assessments and facilitating agreements like the Arctic Search and Rescue Agreement.

However, geopolitical tensions have strained the Council's effectiveness. Following Russia's actions in Ukraine, cooperation has become more challenging, and some joint activities have been paused or limited [(Solomon, 2022)]. Despite these difficulties, it is important to maintain practical cooperation on issues that require collective action, such as environmental monitoring, Indigenous community support, and search and rescue operations.

4. Arctic Exceptionalism in Action

One of the enduring examples of Arctic exceptionalism is the continued collaboration on search and rescue operations. The harsh and unforgiving Arctic environment makes cooperation in this area vital for saving lives. The 2011 Arctic Search and Rescue Agreement enhanced coordination among member states, demonstrating that practical cooperation is possible even amid broader tensions [(Arctic Council, 2011)].

Similarly, joint efforts on environmental protection and scientific research have persisted on a limited basis. For example, data sharing on climate change impacts and migratory patterns of Arctic wildlife continues through various channels, benefiting all parties involved [(Arctic Council, 2017)].

Backchannel diplomacy has also found a place in the Arctic context. Informal dialogues and technical meetings offer opportunities for communication that might not be possible in more formal settings, helping to manage misunderstandings and reduce the risk of escalation [(Exner-Pirot, 2022)].

5. Policy Recommendations

While it is necessary for Western nations to increase investment in the Arctic, particularly concerning security and infrastructure, it is imperative to recognize the value of limited cooperation in specific areas. Enhanced military capabilities can deter aggression and protect national interests, but they should be complemented by maintaining channels for practical collaboration.

Recommendations include:

- **Maintain Communication Channels:** Even amid high tensions, keeping open lines of communication for search and rescue operations, environmental emergencies, and Indigenous affairs is crucial.
- **Engage in Backchannel Diplomacy:** Utilise informal settings and technical meetings to address mutual concerns, reduce misunderstandings, and manage risks.
- **Focus on Practical Cooperation:** Prioritise collaboration on environmental monitoring, scientific research, and support for Indigenous communities, where shared interests can supersede political differences.
- **Strengthen Multilateral Agreements:** Uphold and reinforce existing agreements that facilitate limited cooperation, ensuring they remain effective and are not undermined by geopolitical disputes.

By balancing security investments with these targeted cooperative efforts, Western nations can manage the challenges in the Arctic effectively.

This approach acknowledges the realities of geopolitical tensions while leveraging opportunities for practical collaboration that benefit all parties involved.

6. Conclusion

The Arctic stands at a critical juncture, facing immense challenges from climate change and increasing geopolitical competition.

While recent events have strained the concept of Arctic exceptionalism, the region still offers avenues for limited cooperation that are essential

for safety, environmental stewardship, and supporting Indigenous communities.

Recognizing the Arctic's unique role as a space where backchannel diplomacy and practical collaboration can occur is vital. By adopting a measured approach that balances security concerns with targeted cooperation, nations can navigate these challenges and contribute to a more stable and sustainable Arctic future.

References

AMAP. (2021). Arctic Climate Change Update 2021: Key Trends and Impacts. Arctic Monitoring and Assessment Programme (AMAP).

Arctic Council. (1996). Declaration on the Establishment of the Arctic Council.

Arctic Council. (2011). Agreement on Cooperation on Aeronautical and Maritime Search and Rescue in the Arctic.

Arctic Council. (2017). Agreement on Enhancing International Arctic Scientific Cooperation.

Exner-Pirot, H. (2022). "Navigating the New Arctic Politics." The Polar Journal, 12(1), 5-21.

Gorbachev, M. (1987). The Speech in Murmansk at the Ceremonial Meeting on the Occasion of the Presentation of the Order of Lenin and the Gold Star to the City of Murmansk.

Østhagen, A. (2020). "Coast Guard Cooperation and Maritime Boundary Agreements: Arctic Lessons for the South China Sea?" Ocean Development & International Law, 51(2), 107-124.

Smith, L. C., & Stephenson, S. R. (2013). "New Trans-Arctic Shipping Routes Navigable by Midcentury." Proceedings of the National Academy of Sciences, 110(13), E1191–E1195.

Solomon, E. (2022). "Arctic Council Faces Uncertainty Amid Geopolitical Tensions." Arctic Today.

State Council Information Office of the People's Republic of China. (2018). China's Arctic Policy.

U.S. Department of Defense. (2019). Report to Congress: Department of Defense Arctic Strategy.

U.S. Geological Survey. (2008). Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle.

"The author acknowledges the assistance of OpenAI's ChatGPT in the editing of this article."

The Muslim Brotherhood as Hybrid Actor

Ralph Thiele

Colonel (ret.) Ralph Thiele is an experienced defence expert and thought leader. He is a strategy consultant, researcher, expert witness and publicist.

This article is the summary of a speech given by the the author on 24th October in Abu Dhabi at Trends Fourth Forum on Political Islam - The Muslim Brotherhood and Violence

1. The West under fire

The world has become a rougher place. The US and its democratic allies are under "heavy fire from a loose but increasingly tight front" consisting of China, Russia, Turkey, Iran and radical political Islam, as leading French philosopher Bernard-Henri Lévy observed in a recent interview with Politico. At the heart of the conflict are power, prosperity and a new world order.A hybrid front has emerged that operates in grey areas and is difficult to identify. Actors in political Islam, such as the Muslim Brotherhood, have positioned themselves to take advantage of the upheaval in the world order. They want to play a central role in shaping political, legal, social and cultural systems worldwide with an all-encompassing, totalitarian interpretation of Islam. The Brotherhood's mission is to islamise society through the promotion of religious law, values and morals. It has long combined preaching and political activism with social welfare to advance this goal. But it has a history of violence. Several countries, including Saudi Arabia, the United Arab Emirates and Egypt, have designated the Muslim Brotherhood a terrorist organisation because of its perceived destabilising influence and links to Islamist extremism. In other countries, however, the Brotherhood continues to operate legally and engage in political activism. Following Egyptian President Sisi's visit in April 2019, the White House instructed national security officials to pursue a terrorist designation for the Muslim Brotherhood. However, countries such as Qatar and Turkey have cultivated ties with the Brotherhood and its offshoots, and many exiled members of the Egyptian group have settled in these countries.

2. The new gold standard

Today, the Brotherhood and its affiliates see a hybrid approach, which can start in the grey areas of the democratic constitutional state, as a biotope of Islamist possibilities. The aim is to change the democratic political order so that it is reorganised according to Islamist, undemocratic and anti-liberal principles. Still relatively small groups of full-fledged Brotherhood members in European countries have created an extensive network of NGOs, mosques, schools, lobby groups and other types of institutions that exert a disproportionate influence both within Muslim communities and on European politics and civil society.

In light of recent developments in threats to national and international security, prosperity and defence, hybrid campaigns have become the new gold standard.

Hybrid threats aim to disrupt governments, societies and international alliances. Hybrid actors such as the Brotherhood operate in 'grey areas'.

They use a wide range of social, political, economic, informational, technological and paramilitary tools to achieve maximum effect. The use of non-kinetic means in combination with violence is a key feature of hybrid conflicts. And modern, new and disruptive technologies, such as AI, cyber, robotics, space and many more, provide the Brotherhood with extended

reach and high impact, not least on social media, where they attract a growing community of followers and supporters.

3. Monitored by European security services

Until now, the Brotherhood has generally been able to operate freely in the West within a democratic framework because it is not considered a terrorist organisation. While the Brotherhood's branches in the Middle East have historically kept many aspects of their activities secret, they haven't denied their own existence in the way that is common in the West. Here, most Brotherhood-linked activists and organisations not only shroud their inner workings in secrecy, but even refuse to admit any connection to the Brotherhood. In contrast, the still relatively small groups of full-fledged Brotherhood members in each European country in which they are active have created an extensive network of NGOs, mosques, schools, lobbying groups and other types of entities that exert a disproportionate influence both within Muslim communities and on European politics and civil society. Brotherhood activists and sympathisers also tend to attack those who highlight the existence of Brotherhood-linked networks in Europe and their problematic nature with accusations of shoddy research, conspiratorial views and bigotry. The Brotherhood is not listed as a terrorist organisation by the European Union or by any European country. At the same time, however, the security services of virtually every European country have long monitored the movement. With varying degrees of intensity, European security services have kept the Brotherhood under surveillance. Virtually all of them have taken a very negative view of the Muslim Brotherhood on the continent. They have publicly expressed their views on the Muslim Brotherhood in Europe over the past twenty years, stating that

- An extensive and sophisticated Brotherhood-linked network operates covertly in Europe at both national and pan-European levels
- European-based Brotherhood-linked activists have created front organisations that allow them to operate within society and advance their agenda without being readily identifiable as part of the Brotherhood
- Brotherhood networks in Europe are not involved in terrorism, but have views and objectives that are problematic, subversive, undemocratic and incompatible with basic human rights and Western society

4. The Handbook

Together with Thomas Jäger, I led a major research project and earlier this year published the Handbook of Political Islam in Europe: Activities, Means, and Strategies from Salafists to the Muslim Brotherhood and Beyond (Springer Handbooks of Political Science and International Relations) 2024.

Political Islam:

Political Islam refers to movements and ideologies that seek to implement Islamic principles and values within political frameworks, aiming to influence government, law, and social policy based on interpretations of Islamic teachings.

We have approached the field of political Islam from a European security perspective and found that

- The Muslim Brotherhood as the key actor of political Islam
- With remarkable involvement of Salafists and national political actors such as Iran and Turkey
- The Brotherhood is ubiquitous
- But unevenly distributed

The Handbook contains a series of case studies and country reviews written by distinguished experts in the field. It offers a comparative perspective and a comprehensive overview of the ideology and spread of Political Islam and its

actors in more than 20 European countries. The contributors identify the main actors of political Islam and the activities, means and strategies they pursue and employ across the continent. They also discuss whether and how Political Islam could undermine the Western liberal democratic order and its associated values in hybrid ways, with and without violence.

Muslim Brotherhood activities are reported in virtually all the countries and regions studied. A key finding for Spain is that the Islamist scene there is dominated, if not "monopolised", by the various variants of the Muslim Brotherhood. The contribution on the Netherlands notes that the Brotherhood has managed to gain more influence through practical cooperation with other organisations than its size in the Netherlands would suggest.

Among the countries where political Islam is more extensively observed are European countries with large populations, such as Germany, the United Kingdom and Spain, as well as Austria, Switzerland and Sweden. Conspicuously absent or barely present is Political Islam in countries such as Portugal and Greece. The article on Portugal notes that no state or transnational actors are known to be "promoting political Islamism" on Portuguese territory. And traces of political Islam in Greece are described as being in an 'embryonic stage of development'. The country chapter on Romania states that 'the risks of influence of Islamist practices on the current democratic establishment in Romania are currently low'.

Similarly, the article on the Western Balkans notes that the region's Islamic communities 'remain moderate, with their official narrative only rarely fragile enough to succumb to radical influences'.In terms of goals and means, Bassam Tibi identifies the creation of an Islamic state as the overarching, ultimate goal of political Islam. This overarching goal is taken up in principle in several contributions, e.g. from Austria, Belgium, Sweden and the United Kingdom. The article on Austria makes the general observation that the goals of Islamist actors in that country - but also in other European countries - have changed over time: For the first generation of Islamist activists, Western European countries thus served as a base from which they could support the parent organisations in their countries of origin and change conditions there in order to return to their home countries as soon as possible. Now, however, political Islam organisations seem to be concentrating more on influencing local politics.

One goal, according to this article, is to build Islamic parallel societies and, in the long term, to spread their visions in Western societies. Another goal, repeatedly mentioned, is to gain (sole) interpretive sovereignty over the understanding of Islam vis-à-vis the Muslim community in the respective state.

5. Policy Recommendations

Political Islam challenges enlightened democratic states in many ways. In the coming years, the number of subtle, hybrid actors is likely to increase at the expense of those who are easier to categorise. New and disruptive technologies have become force multipliers for their actors to translate their objectives into action, including violent action. This is a challenge for the entire state and society, and must be met with nationwide and society-wide measures. Understanding this socio-cultural dimension and resisting its forces requires political education, defensible democracy and thus the self-organisation of democratic life. It is also an important task of the security services to keep track of the various vectors of attack on state stability and social cohesion. Recommendations for the future containment of Islamist threats in Europe include

- Long-term policies that allow for economic and social balance in societies, intercultural dialogue and the use of appropriate language, transparent and result-oriented cooperation with relevant actors
- Integration of immigrants to counter any potential susceptibility to radical ideas
- The "minimum" recommendation is to promote awareness of the Muslim Brotherhood's

activities, and to do so in a comprehensive format and with massive technological support such as AI, trend analysis, etc. Three vectors are important

Three vectors are important:

- Many threats come from outside. Helping to stabilise unstable regions is a useful preventive measure. Denying perceived threats access to the country is another important protective measure. This applies in particular to the actors of political Islam who want to take root among us by marching through the institutions.
- Many threats come from within. These can be prevented by better, more conscious integration, by more consistent action against identified activists and mentors, but also by less naivety in dealing with political Islamism that seeks to create a different, non-democratic society.

Cyberspace easily transcends external borders and domestic political rules. We need to get better at regulating this new domain and much better at identifying and countering dangers, threats and attacks. Technology can help enormously, for example in improving our security and preventing sabotage and terrorist attacks.

To sum up:

Our fellow Muslims are not the problem.

The Muslim Brotherhood and Islamists are the problem. And we need to do a better job of dealing with hybrid threats. Going forward, it will be important to improve cooperation between the police, judiciary, media, civil authorities, intelligence services and the armed forces so that anti-state and anti-democratic efforts by the Muslim Brotherhood can be promptly identified and prevented.

epis ThinkTank

International Politics Shaped By **You**

EPIS Thinktank

Who We Are

EPIS is a young think tank on foreign affairs and security policy. We publish scientific articles, send members to international conferences, and maintain a network of: students & young professionals.

The deal:

- You professionalize yourself in your field
- We help you start your career

What We Do

EPIS Magazine

- In-Depth Analyses of Political Issues of Your Choice
- 80 Pages
- 3x/Year

EPIS Working Groups

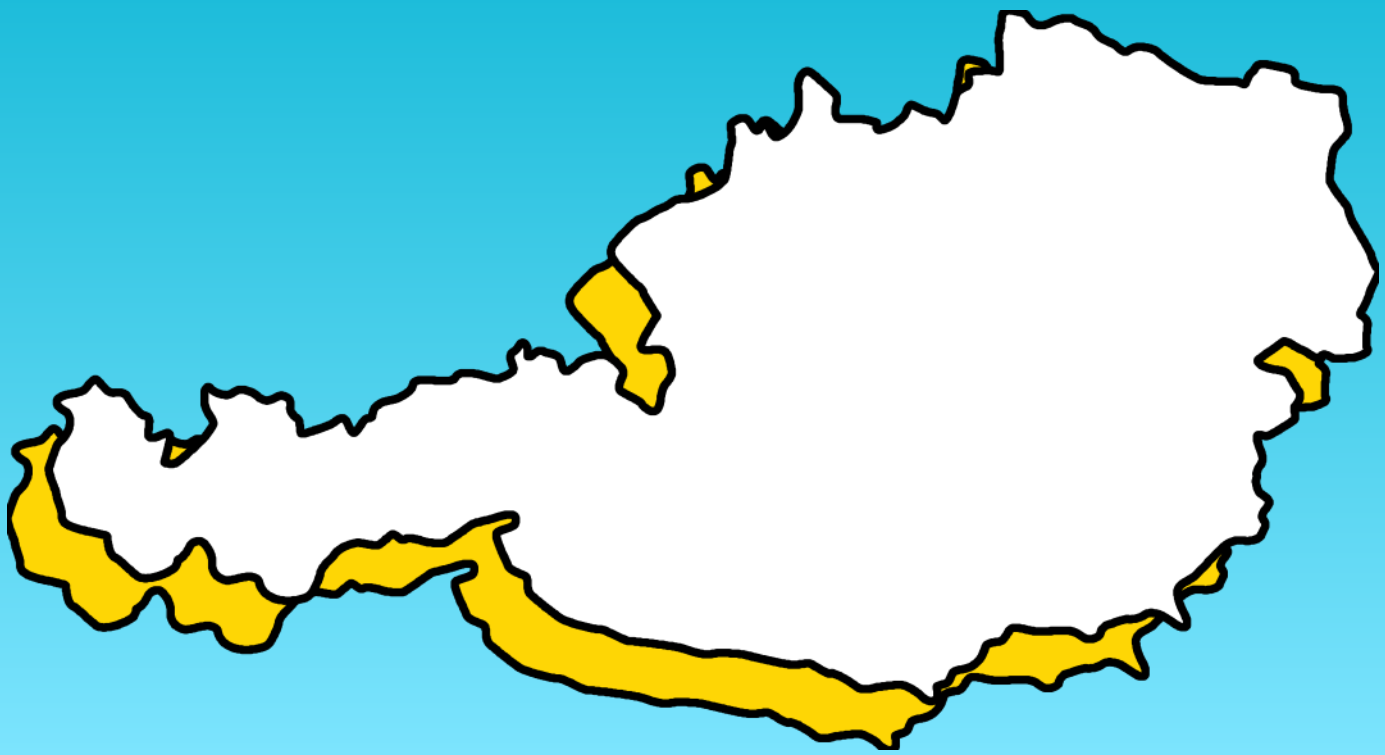
- Monthly Briefings on Political Developments in Eight World Regions

EPIS Talks

- Deep Dive into the Articles of our Magazine with the Authors

EPIS Blog

- Short Analyses of Political Issues of Your Choice
- Weekly Release



Defence and Security of Austria and Beyond

Interview with Former Minister of Defence Fasslabend

Dr. Werner Fasslabend

Werner Fasslabend, born in 1944, is an Austrian politician and academic. He served as Austria's Defence Minister (1990–2000), advancing defence reforms and EU/NATO partnerships, and was Third President of Parliament (2000–2002). Currently, he presides over the Austrian Institute for European and Security Policy (AIES) and holds roles in various European institutions. He lives with his wife and two children.

Himmel: Mr Fasslabend, thank you for inviting us to your institute located here at the Springer Castle and also close Schloss Schönbrunn here in the lovely city of Vienna. You have been the defence minister quite a long time. But before that, you studied law. How did that come? Why did you study law at the beginning?

Fasslabend: I mean, this was just a question of starting my business career. I was not sure, but everybody told me that law would be the best and of course I was highly interested already in politics and in official affairs and in so far it was not a strange decision for me and not a difficult decision. Afterwards I joined private industry. I worked 20 years for Henkel company.

As a product manager and the sales director. And I did this until I became Minister of Defence. Even when I was already Member of Parliament.

Himmel: You still as a Member of Parliament worked at Henkel?

Fasslabend: Yes.

Himmel: Have you considered, as you mentioned, that you were already interested in politics, whether opportunities or possibilities, during your studies, to get involved in politics? Was it able to combine law with politics?

Fasslabend: I did it from the beginning. I mean, I started with political activities already when I was a teenager, so I went in order to join political meetings, or official sessions in my hometown. When I was a student they asked me whether I wanted to take part at the campaign and afterwards I became a member of a party. I came into different functions, in the region, in the Bundesland and then on national level.

Himmel: Around what time was that? When you've joined there, you've been politically active.

Fasslabend: I became active when I was around about 20. I guess this was during my studies. The first national campaign I participated was in 1959.

Himmel: How were these times?

Fasslabend: You could not compare it, of course, because the general situation in Europe was completely different. I was living extremely close to the so-called Iron Curtain.

My house was positioned only 150 metres away from the Iron Curtain. So far this was with the border versus Czechoslovakia, and insofar I experienced this ideological discussion and the relationship between East and West from the beginning of my life.

Himmel: Could you describe how the Iron Curtain looked like?

Fasslabend: It was the river Morava.

The middle of the river used to be the border between Austria and Czechoslovakia, and the other side you had already the real Iron Curtain with fences. Usually one could listen during nighttimes the crying of people who wanted to flee to cross the Iron Curtain, shootings from the soldiers, barking dogs.

Himmel: How did that affect your political views, your political engagement?

Fasslabend: Probably it did quite a bit.

I mean on the one hand, of course it enforced, the tendency to occupy myself with all the political questions between East and West, the basics of politics, of political systems, the importance of freedom, of an economic system.

It also contributed to my specific interest of defence. I could see these military systems at the other side. When there was the Spring of Prague, I still have in my ears the noise of the chains of the tanks of the Russian tanks that came from Bratislava, went to the north to Prague.

Himmel: You've been then in your political career, I would say at the height of your political career, the Defence Minister of Austria. We've come across two topics which we're most busy with, first one being the modernization of the Austrian armed forces and the other one is trying to enhance the role of Austria in peacekeeping

questions. Beginning now, with the first of this one, the modernization: What were the major challenges or opportunities which came with that?

Austrian paradox, you could say, in our history that at the same time when Austria became neutral as a price to get the States Treaty and to get rid of the occupying powers, at the same time

Fasslabend: A big challenge, it could not have been bigger than it was in reality. You know why? Because, of course, the end of the Cold War brought the challenge to change the system completely. On the other hand, also the solution of the Warsaw Pact changed Austria's situation in between the two blocks. Of course, it also brought a new freedom to organise our defence, because we had many restrictions out of our state treaty. Austria did not have the right to buy missiles - we did not have missiles until 1989. The we were forbidden to protect ourselves as it was necessary as a neutral country. Because you cannot defend your country, especially the airspace, when you are not able to have missiles. Not ground to air, not air to air. So far you can imagine how difficult it was.

Himmel: So, the Austrian armed forces had to rely on conventional weapons.

Fasslabend: Artillery, yes, very traditional systems.

And this was one of my first programmes to buy missiles systems.

The State Treaty of Austria, signed on May 15, 1955, re-established Austria as a sovereign and neutral state after World War II. It ended the Allied occupation, prohibited unification with Germany, and ensured Austria's permanent neutrality. The treaty laid the foundation for Austria's independence and its non-alignment during the Cold War.

Himmel: That's very interesting. How does one build up a missile system? I guess it's a bit hard to start off at all to implement such a system into a running army.

Fasslabend: It's not so difficult, no. I mean people, of course, they had learned a lot. At least a few specialists within the army that had made the courses in the United States or in other countries. So far, they had not only theoretical experience, but even a practical experience to handle such systems. What we did, we bought the system. Especially at the beginning, European systems. Mistral from France, from Sweden and then also Sidewinder missiles from the States.

Himmel: As you now mentioned, where you get the missiles from, I can see that these were all Western or European or NATO-related countries. Was there, in regard to the neutrality, also an idea to reach out to Eastern, former Eastern bloc countries to maybe collaborate with them in the question of missiles?

Fasslabend: I think there was a very short phase where it was considered to do so in order to convince the Russians during the Cold War period to allow Austria to buy missiles, but they were not very positive to this idea. And then Austria, of course, went to the Western countries in order to buy them because everybody knew that there would not be a possible aggression from the western side. But if then from the eastern side.

Himmel: How did it come up that you could convince the powers to allow Austria to acquire missiles?

Fasslabend: We did not, but without that, the moment had come that the States Treaty was not the basis any longer for our material decisions and for our military politics. It was at the end of the Cold War.

Himmel: New times, new strategy.

Fasslabend: Right.

Himmel: But you've kept the strategy of neutrality, which is also a very basic principle of Austrian policy or of Austrian foreign policy. How did that affect when you draft a new policy, when you draft a new strategy. You have a new millennial, where's Austria going to?

Fasslabend: The Austrian situation what concerns neutrality is a little bit different to most of the other countries, because in Austria neutrality is part of our constitution. This is also the difference to Sweden or Finland. Back then people did not differ, but they thought, neutrality means we are free and after a while they also meant, this would protect us. Because the others more or less recognised our neutrality, and therefore this also would bring some security. At the End of the Cold War, at least the specialists had realised that this situation had changed or was changing completely. We had to change politics more or less completely, and this was not only by our own military steps we did, but also the fact that we joined NATO Partnership of Peace and even joined NATO missions in former Yugoslavia. I personally also organised the first NATO workshop outside of NATO territory and was also for the first time, the discussion whether Austria should join NATO.

Himmel: I want to take a last question on the history of the neutrality because we've now interviewed a lot of small nations. I wouldn't consider Austria a small nation, but Austria has a

very special position as it was once a huge empire, combining a lot of people, a lot of different states, a lot of different cultures around taking a huge part of Europe and the Balkans and has been shrunk to its current size. Does that in any case affect the foreign policy?

Fasslabend: It does not affect Austrian politics in the way it should. Due to the fact that more or less Austria not only overtook a new role or was maybe pushed into a new role and situation, but it as by historic reasons, overtaken this new role to an extent that was not necessary, and I guess we probably could be much more efficient than we are at the moment.

Himmel: Now you've mentioned that Austria is in a NATO partnership, not a full member of NATO. Is that a first step?

Fasslabend: I would say it was an automatic reaction to the new situation after the end of the Cold War. Austria joined the same time when we joined EU in 1995. We also joined NATO Partnership for Peace that was newly founded. After the end of the Cold War, nobody had a plan, nobody was prepared for such a situation.

Himmel: Were the politics taken by surprise?

Fasslabend: Of course, I had as a long serving defence Minister quite a good standing within the Group of Foreign and Defence Ministers and so far, very often or just in smaller circles, discussed what one could. The American, British, German Defence Minister, and we sat together, and we asked ourselves what could we do in order to stabilise Eastern Europe. What would be necessary? To be done politically, but also militarily and insofar we found a few ways and I think the Partnership for Peace concepts was one of them. There was no question about stability then, but rather, what could we do in order to stabilise countries like Poland, like Czechoslovakia, like Hungary, Romania.

Himmel: How?

Fasslabend: I mean you have to be aware that of course also the military in those countries where of old communists and insofar those countries needed new assistance, and they needed new ways also to be linked to the rest of Europe, because otherwise, we would have had more or less a continuum of politics even after the breakdown of the Soviet system. This really was a fascinating period where you could contribute quite a bit and due to Austria's situation and the experience in Central Eastern Europe, we also had the opportunities in official sessions to shape those systems quite a bit.

Himmel: That is what I would then also call your second agenda: the enhanced role of Austria's peacekeeping. What were the ideas? What are the ideas you've changed out?

Fasslabend: I think the main question certainly was the political stability of our neighbourhoods of Central Eastern European. And in this context, it was politics, it was economy, it was security. And cultural questions, of course. What we're trying to do is not only political but also the security sector. For example, we brought all of our neighbouring countries into international missions, for example Slovakia, Hungary, Slovenia and so on. All of them had their first international missions together with an Austrian contingent. We tried to integrate them more or less into our politics or general security politics and more or less transfer our ideas and our systems also into those countries. We also founded then specific partnership between the Central European countries, it was called Central European Cooperation where we sit together and try to prepare ourselves in order to shape in for the future common battalions or common brigades for international missions.

Himmel: I think that brings us neatly to the last part which I wanted to delve in which is the future strategy, the future policies as you've now mentioned, Central European Cooperation as possibility or platform to cooperate, for example, in common brigades. Is that something which could be also a possibility for Europe, or for the EU especially?

Fasslabend: It was my privilege to initiate and

organise the first European Defence Minister meeting in 1998, at the moment when quite a lot of European nations were still resistant towards such an idea.

The 1998 European Defence Ministers' meeting was pivotal in advancing European security cooperation, spurred by the Balkan conflicts. It highlighted the need for an independent European defense capability, leading to the establishment of the European Security and Defence Policy (ESDP). This meeting set the stage for deeper military collaboration within the EU framework.

This also was more or less the beginning of common initiatives. As a consequence, I was sure that it was absolutely necessary to do so, but this is something that we just have to do in order to keep our European position respected. NATO is a need for Europe. Europe does need the cooperation with the Americans in order to withstand dangers coming from the east. But, of course, that this organisation never will be able to do the necessary job. In security policy, you have to differ between defence and security policy. European security, which means to do something for the stability of Europe's neighbourhood, will be a regional European task that nobody else can and will overtake. Europe is at the moment in the situation, that NATO is working and it also will be working in the future, whether Trump will be the next president or not. But the Americans never will care about security in Africa or in the Middle East, in the Caucasian region or at the Balkans. Whether this is the eastern Mediterranean, the Balkans, the Caucasian region, whether this is Iraq, Syria, Lebanon in Africa and Libya especially, but also other countries. And if you ask yourself, where is European Union, where is any European state? You will have to say nowhere. Nowhere in none of these countries, Europe does not even play a little role. You can go and the Caucasian region and the whole of the Middle East, the whole of Northern Africa, and after more or less the failure of French African policy you can see nothing is left. Therefore we will have to develop European security policy that enables to contribute to the stability in our immediate neighbourhood.

Himmel: I understand you correctly that you say the European Union requires NATO and requires to play a more dominant role within NATO as for their own security interests when it comes to close neighbourhoods.

Fasslabend: We will have to differ in the future. If there is a defence question like, let me say Ukraine, it is clear that the European countries only together with the Americans will be able to shape a military power that really is enough to counter any danger coming from Russia or from the east. But, the Americans, for sure, will not engage in northern Africa. As you can see, they have left the Middle East. They will not come back. They will not engage in the conquest of the region. They will not engage in the eastern Mediterranean. And insofar this is an absolutely clear task for the European nations, and they only can do it together.

Himmel: To understand the terms defence and security, because you differ between them: What are these terms?

Fasslabend: Defence would mean for me just to withstand a military aggression coming from the east. Security means to shape stability politically, militarily, economically. This means we need it from the Atlantic Ocean to the Indian Ocean.

Himmel: That's a huge part of the world.

Fasslabend: It's our neighbourhood. I mean, if a country like Turkey is to influence the politics, its complete neighbourhood, then the European Union should be able to do so at least in part of it. But not to be able to do so in any country, is something that I will not accept any longer.

Himmel: Should then the common European security policy not only focus on military, but also on political and economic questions?

Fasslabend: I think this is a natural division of labour for the future. Later, we'll be there for defence and the European nations within NATO have to engage themselves in Northern Africa and in the Middle East, the Caucasian region.

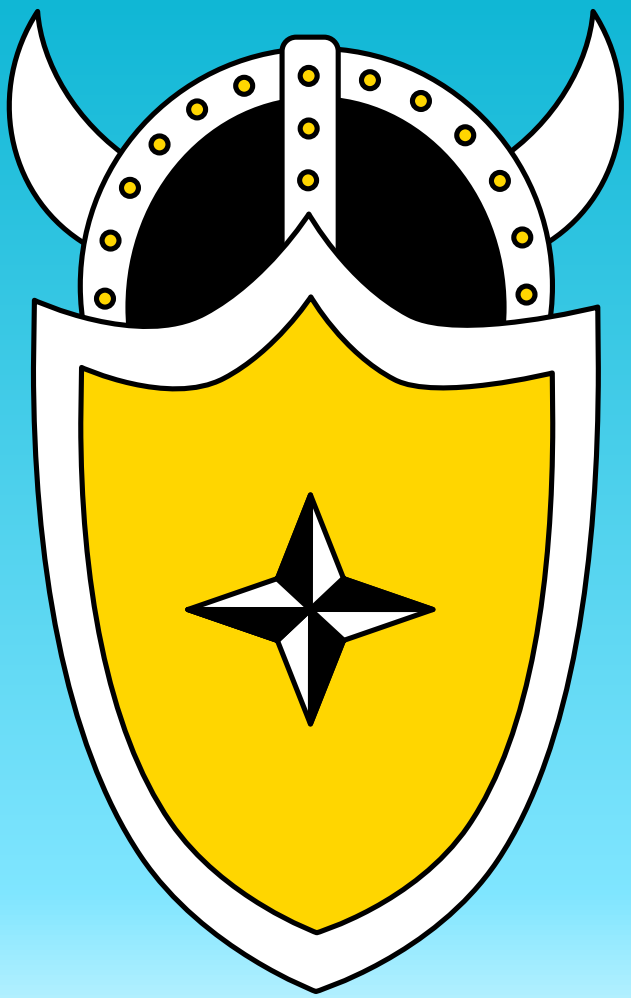
Himmel: Coming to my last question then. What is Austria's role in in in the upcoming development of maybe such a common defence and security policies of the EU or Europe?

Fasslabend: I'm looking at the one side to natural tasks we do have in order to shape a stable environment for our own country, which means engagement in Southeast Europe, the

Balkans. To engage ourselves also in Eastern Europe, because this is our immediate neighbourhood and there's a maybe a third region because we are influenced most by the development over there also will be the Middle East. So, Austria certainly will have to play a decisive role for the stability of the Balkans. I have to say that Austria was never hesitated to go into international missions. Due to our geostrategic situation and due to the fact also that we do have capabilities in order to make major contributions for the stabilisation of those regions, we will have to do it.

Himmel: Thank you very much, Mr Fasslabend, for your insights. And thank you very much for your time.

Fasslabend: Thank you. It was a pleasure.



Sweden's Historic Shift

NATO Membership and Its Mutual Impact on National Defence and Alliance Contributions

David Stadin

David Stadin is currently studying political science at Halmstad University and has a background in the armed forces. In addition to his academic pursuits, David boasts extensive involvement with Swedish civil defence organizations, occupying various board positions therein. Areas of keen interest encompass Swedish and international security policy, alongside defense politics.

1. Introduction

On 22 May 2022, Sweden made a historic shift in its security policy by applying for NATO membership. This decision ended 200 years of freedom from military alliances. On March 7, 2024, Sweden was officially admitted as the 32nd member of the defence alliance NATO. This event has great symbolic and practical significance for the country's military and security policy future (BBC, 2024). Sweden's entry into NATO not only represents a shift in the long-standing policy of neutrality and freedom of alliance that has characterised the nation's foreign and security policy stance, but it also entails far-reaching consequences for Försvarsmakten (The Swedish Armed Forces) organisation, strategy, and operational capability.

Försvarsmakten:

The Swedish Armed Forces (Försvarsmakten) consists of the Army, Navy, Air Force and The Home Guard

Sweden's membership in NATO means that the Swedish Armed Forces are now facing new and complex challenges such as adapting to the collective defence commitments that the alliance requires and integrating their military structures and operational capabilities with other NATO countries. But how has the Swedish Armed Forces changed since joining NATO?

2. Swedish Armed Forces in the NATO Era: Their structure and goals

To understand how the Swedish Armed Forces have changed since joining NATO, we first need to review their goals and structure. The ultimate task of the Swedish Armed Forces is to preserve the country's freedom and protect the right to choose how to live. To build a stronger defence, the Swedish Armed Forces train and have exercises often, both within the armed forces and with other authorities and countries. Exercises and operations occur around the clock, all year round – on the ground, in the air, at sea, and online. To be able to face every threat and cope with every challenge. The task of the Armed Forces also includes strengthening and protecting critical societal functions such as the Swedish parliament and being better equipped to cope with crises and natural disasters. The armed forces receive their mandate from the government, which also decides how much money will be allocated to the defence. Across the country, the Swedish Armed Forces has 46 regiments and units and 26.000 active personnel such as officers, soldiers and civilian employees. It also has 34.000 active in the reserve such as the Swedish homeguard, part time soldiers and reserve officers. The mission of the Swedish Armed Forces is largely to defend Sweden with military means and promote the safety of society by:

- Being available and prepared to be able to take heightened alert quickly
- Protecting Sweden's freedom of action in the face of political, military, or other pressure
- Defending Sweden against incidents and an armed attack
- Increasing the security by participating in operations here in Sweden, in the local area, and abroad
- Following international law, defend the national rights and interests in areas also outside Sweden

(Swedish Armed Forces, 2024)

The organisation and structure of the Swedish Armed Forces fall under the authority of the Swedish Parliament (Riksdag) and the government. Led by Supreme Commander General Michael Claesson, the Armed Forces are directed and overseen through the Armed Forces Headquarters. With approximately 50,000 active personnel, the Swedish Armed Forces comprise units from the Army, Navy, Air

Force, and the Home Guard. These branches share essential collective resources, including training, logistics, command and control, and intelligence. Regiments, units, and training institutions form the core structure, which is adjusted during times of heightened alert or mobilisation to reassign personnel, equipment, and infrastructure as needed. In peacetime, more than 70 locations across Sweden host the Armed Forces. (Swedish Armed Forces, 2023)

3. Sweden's Strategic Shift: Integrating with NATO and Strengthening the Swedish Armed Forces

Since March 11, the NATO flag has flown alongside the Swedish flag at Armed Forces installations across the country.

Sweden's membership in NATO marks a significant shift in the country's military-strategic landscape, directly impacting the Swedish Armed Forces' established defence plans.

All planning will align with NATO's three core tasks of deterrence and defence; crisis prevention and management; and cooperative security (NATO, 2023). Initially, the Swedish Armed Forces will base their participation in NATO's defence planning on existing national defence strategies. However, over time, these plans will be revised and adapted to align with NATO's frameworks. As a NATO member, Sweden's geography becomes crucial and introduces three key strategic points to the Alliance: 1) The Öresund Strait, a vital passage linking the North Sea to the Baltic Sea, which will now be fully controlled by NATO members; 2) Gotland, the largest island in the Baltic Sea, often referred to as an "unsinkable aircraft carrier" due to its central positioning in the region; and 3) The coastline along the Åland Sea and Gulf of Bothnia, which will facilitate the defence of Åland, a demilitarised zone between Sweden and Finland at the entrance of the Gulf of Bothnia.

These elements will influence NATO's future defence planning, especially concerning the defence of Finland and the Baltic states, as well as providing new strategic opportunities for the defence of Norway. Maintaining control over the Baltic Sea and ensuring the defence of Gotland, while also accommodating large troop movements planned by NATO will be of importance. Therefore Sweden must ensure its ability to serve as a host nation for NATO operations, involving ground, naval, and air forces. Swedish armed forces may become part of NATO's strategic deterrence capabilities. The ability to plan and lead host nation support, including logistics coordination with NATO, will become increasingly important. Given Sweden's geographic location, the need to improve operational command capabilities is paramount, particularly in the Baltic Sea region, northern Scandinavia, and in leading host nation support. The Swedish Armed Forces aim to establish a unified operational area with other Nordic countries and be part of the same operational command. Currently, Sweden is aligned with NATO's Joint Force Command in Brunssum, the Netherlands, but there may eventually be a shift to NATO's command in Norfolk (Swedish Armed Forces, 2024).

The Swedish cooperation with NATO is however nothing new. Sweden first contributed to a NATO-led operation in 1995 when it sent a battalion to the NATO-led peacekeeping force in Bosnia and Herzegovina. Since then Sweden has supported the NATO-led forces in Kosovo, Afghanistan, Libya, and Iraq as well as

participating in the enhanced NATO Response Force (NRF) in a supplementary role and subject to national decisions (NATO, 2024). As of recent the Swedish Government has decided to task the Armed Forces with planning and preparing the first Swedish participation in NATO's Enhanced Forward Presence. The Enhanced Forward Presence is a NATO-allied deployed defence and deterrence military force in Northern, Central, and Eastern Europe. This historic contribution will consist of a force equalling the size of a reduced battalion of 600 soldiers and will be sent to Latvia. It will be part of a brigade led by Canada beginning in early 2025 (Government Offices of Sweden, 2024) As Sweden has joined NATO, the country has also officially signed a Defence Cooperation Agreement (DCA) with the United States. This agreement establishes the framework for US forces to continuously operate in Sweden and gives them bigger authority compared to other NATO countries. Key aspects will be covered such as the legal status of US troops, access to deployment zones, and the pre-positioning of military equipment within Swedish territory. The agreement marks a significant step in strengthening military cooperation between Sweden and the US. It bolsters regional security, not only for Sweden but also for neighbouring countries, by reinforcing the US's commitment and physical presence in the region. The US has previously established similar DCAs with several European nations, including Norway, Denmark, and Finland (Government Offices of Sweden, 2023), (U.S. Department of State, 2023).

4. Sweden's contribution to NATO: Enhancing Security and Strengthening Europe's Defence Industry

All the countries surrounding the Baltic Sea, except Russia, are now members of the Alliance, reshaping the security dynamics of this part of Europe. The inclusion of Sweden and Finland will expand NATO's operational reach and strengthen the connections between the High North, the North Atlantic, and the Baltic regions. Sweden's strategic location and military assets can significantly enhance the Alliance's ability to conduct operations in Northern Europe. Additionally, Sweden's defence industry will be a major asset for NATO, as it is one of the largest in Europe. The nation's top defence companies produce some of the world's most advanced military technology, including Saab's Jas 39 Gripen fighter jet and BAE Systems AB's Combat Vehicle 90. With ongoing high demand for military equipment, particularly as countries continue supplying arms to Ukraine in response to the Russian aggression, Sweden's defence production capacity will remain crucial in the coming years. Sweden is also home to leading high-tech firms like Ericsson, the world's second-largest network provider; Hexagon, a key software company; and Northvolt, one of Europe's largest lithium battery manufacturers. The country holds significant reserves of critical minerals, such as iron ore and rare earth metals, which are essential for both the defence industry and the green transition (Wilson Center, 2024). Following a recent discovery in Kiruna in northern Sweden, the country now boasts the largest known deposit of rare-earth metals in Europe. This offers NATO a vital opportunity to reduce its reliance on critical minerals from China and other authoritarian regimes (Reuters, 2023).

5. Conclusions

Sweden's entry into NATO represents a historic shift in their security policy, moving from centuries of neutrality to active participation in collective defence. This transition not only affected Sweden's strategic position but also transformed the Swedish Armed Forces in profound ways. Integrating into NATO's defence structures, Sweden now plays a crucial role in regional security, particularly in the Baltic and High North regions, with strategic assets like Gotland and the Öresund Strait becoming vital for NATO operations. The Swedish Armed Forces face new responsibilities, from aligning with NATO's defence planning to enhancing operational command in the Baltic Sea. Sweden's defence industry also stands as a valuable asset, providing cutting-edge

technology and critical materials that support NATO's military and technological capabilities. As the country solidifies its role in the alliance, their contributions to regional security, deterrence, and crisis management will continue to grow, ensuring that Sweden and its armed forces not only benefit from the alliance but actively strengthen it.

References

BBC. (2024). Sweden formally joins Nato military alliance. https://www.bbc.com/news/world-europe-68506223

Government offices of Sweden. (2023). Defence Cooperation Agreement with the US signed. https://www.government.se/press-releases/2023/12/defence-cooperation-agreement-with-the-us-signed/

Government offices of Sweden. (2024). Swedish Armed Forces to contribute forces in Latvia. https://www.government.se/press-releases/2024/04/swedish-armed-forces-to-contribute-forces-in-latvia/

NATO. (2023). NATO 2022 Strategic Concept. https://www.NATO.int/cps/en/NATOhq/topics_210907.htm

NATO. (2024). Relations with Sweden. https://www.NATO.int/cps/en/NATOhq/topics_52535.htm?selectedLocale=en

Reuters. (2023). Sweden's LKAB finds Europe's biggest deposit of rare earth metals. January 13, 2023. https://www.reuters.com/markets/commodities/swedens-lkab-finds-europes-biggest-deposit-rare-earth-metals-2023-01-12/

Swedish Armed Forces. (2023). Organisational Structure and Responsibilities. https://www.forsvarsmakten.se/en/about/organisation/organisational-structure-and-responsibilities/

Swedish Armed Forces. (2024). Därför finns försvarsmakten. https://www.forsvarsmakten.se/sv/om-forsvarsmakten/darfor-finns-forsvarsmakten/

Swedish Armed Forces. (2024). Så förändras försvarsplaneringen av NATOmedlemskapet. https://www.forsvarsmakten.se/sv/aktuellt/2024/03/sa-forandras-forsvarsplaneringen-av-NATOmedlemskapet/

U.S Department of State. (2023). U.S. Signs Defence Cooperation Agreement with Sweden. https://www.state.gov/u-s-signs-defense-cooperation-agreement-with-sweden/

Wilson center. (2024). Sweden's Contributions to NATO: Bolstering the Alliance's Defence Industry and Air Capabilities. By Jason C. Moyer & Henri Winberg. https://www.wilsoncenter.org/article/swedens-contributions-NATO-bolstering-alliances-defense-industry-and-air-capabilities

epis ThinkTank

International Politics Shaped By **You**

EPIS Thinktank

Why Join Us?

- Make Your Voice Heard Through Our Various Formats and Participate in International Politics
- Publish Articles from Early on in Your Academic Career
- Receive Valuable Guidance throughout the whole Writing Process
- Become a Part of Our Network of Likeminded Students and Young Professionals in International Affairs

Interested? *Reach Out!*

Contact us on Instagram or LinkedIn or learn more about our work on our website!

@episthinktank

/epis-thinktank

epis-thinktank.de

EPIS BASICS:

LOOKING AT THE CONCEPT OF NEUTRALITY

In EPIS Basics, our authors explain basic knowledge of international foreign affairs and security policies. This encompasses basic theories, organisations and events This series is presented in depth here in the magazine. You can also find other smaller contributions on our Instagram page

Maximilian Arnold

Maximilian Arnold is currently in his third year of the BA in International Affairs at the University of St. Gallen (HSG). His main area of interest is security policy, with a particular focus on Swiss neutrality and its relevance in the evolving European security landscape.

Switzerland is famous for its banking, its watchmaking, its chocolate - and its neutrality. Unlike Sweden and Finland, which recently abandoned neutrality to join NATO in response to the war in Ukraine, Switzerland continues to maintain neutrality as a central pillar of its foreign policy, as it has for centuries. While the concept of neutrality may seem straightforward at first glance, its nuances are more complex. This article unpacks five important differentiations within the concept of neutrality.

Neutrality Law vs. Neutrality Policy

One of the most crucial distinctions when talking about neutrality, is that between neutrality law and neutrality policy. The law of neutrality is recognised under international law and, has been codified in the Hague Conventions since 1907 and is applied in the event of an international armed conflict. Neutrality policy encompasses all measures that a neutral state in war, or a permanently neutral state in peace, takes at its own discretion beyond its obligations under neutrality law. These measures are intended to ensure the effectiveness and credibility of a state's neutrality.

Occasional vs. Permanent Neutrality

Neutrality can be either occasional or permanent. Occasional neutrality occurs when a state decides to remain neutral in a particular conflict without a long-term commitment to avoid all future wars. In contrast, permanent neutrality is when a state commits itself to a neutral stance indefinitely. This concept emerged in the early 19th century with the Congress of Vienna (1815), where Switzerland's permanent neutrality was enshrined in treaty documents.

Integral vs. Differential Neutrality

Another important distinction within neutrality is between integral and differential neutrality. Integral neutrality refers to a state that attempts to remain impartial toward all conflict parties in all dimensions, including economic, military, and ideological impartiality. Differential neutrality, on the other hand, allows for certain forms of engagement, such as economic sanctions, while avoiding direct military involvement.

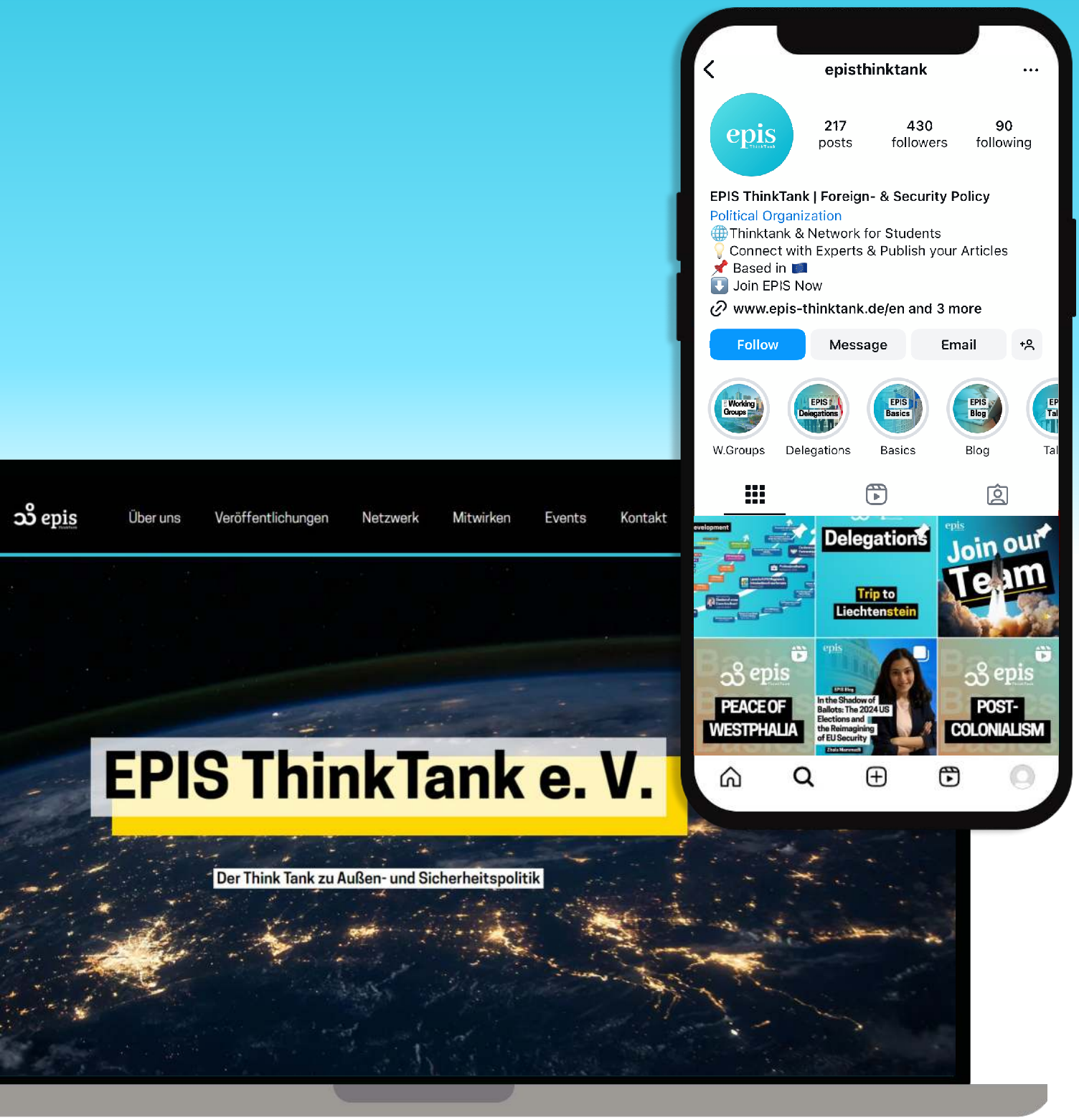
Armed vs. Unarmed Neutrality

Another common distinction is between armed and unarmed neutrality. Armed neutrality refers to a state that maintains military forces while pledging not to take sides in conflicts unless attacked. In addition to Switzerland, Sweden and Finland practised a policy of armed neutrality before joining NATO. Conversely, unarmed neutral states, such as Costa Rica, the Vatican, or Lichtenstein, do not maintain military forces capable of defending against violations of their neutrality.

Maritime vs. Territorial Neutrality

Neutrality in international law also distinguishes between maritime and territorial aspects. Maritime neutrality has long been important, as control of sea routes has been crucial to trade and military operations throughout history. In times of war, neutral states often insisted on the right to trade freely, even with belligerent states. Territorial neutrality, on the other hand, refers to a neutral state's obligations regarding its land and airspace.

Although there is a great deal more to the concept of neutrality, these five distinctions serve to illustrate the multifaceted nature of neutrality. They also provide a clearer understanding of how neutrality functions in international affairs and serve as a basis for further discussion of its evolving meaning and practical applications in different states.


epis
Über uns
Veröffentlichungen
Netzwerk
Mitwirken
Events
Kontakt
EPIS ThinkTank e. V.
Der Think Tank zu Außen- und Sicherheitspolitik
episthinktank
217 posts
430 followers
90 following
EPIS ThinkTank | Foreign- & Security Policy
Political Organization
Thinktank & Network for Students
Connect with Experts & Publish your Articles
Based in
Join EPIS Now
www.epis-thinktank.de/en and 3 more
Follow
Message
Email
W.Groups
Delegations
Basics
Blog
Delegations
Trip to Liechtenstein
Join our Team
PEACE OF WESTPHALIA
POST-COLONIALISM

Imprint

Editor-in-chief: Theodor Himmel

Publisher: EPIS ThinkTank e.V.

Contact: kontakt@epis-thinktank.de

ISSN: 2942-6030

Are you interested in our work?

EPIS ThinkTank e.V. welcomes your support. As a member, author or supporter, you can get involved. We have been participating in the political debate for sever- al years. As an association, we are young academics committed to fact-based and neutral debate. Our members come from all over Germany and the world.

Find out more on: www.epis-thinktank.de

or visit us on: