NL input for the EU security strategy

European security is under severe pressure. Russian aggression not only threatens Ukraine, but also affects the security of all of Europe. The Kremlin views this war as part of a broader conflict with the West. In addition, the international security environment in which the EU has developed over the past 80 years is changing rapidly and structurally, affecting the existing European security architecture. Our rules-based order reflects our history and a shared commitment to peace, democracy, the rule of law, and human dignity. Security threats are intertwined, and there is a strong interaction between domains such as defence, technology, and economic security. Hybrid threats, cyber security challenges, and espionage affect our societies.

In view of growing security threats on the European continent, European countries urgently need to take on a significantly greater role and responsibility for their own security and defence. This starts with a *burden shift* in NATO, where European Allies will take on a greater role relative to the United States. It is underpinned by a strong European Union. The EU will have to act in a more powerful and transactional manner when needed. A strong Europe also requires strong partnerships with countries such as the UK, Canada and Norway.

While the EU security strategy cannot contain the single solution to the threats the European continent is facing, it is an important step towards a more powerful European Union. It should integrate existing strategies, ensuring a coherent approach that addresses the nexus between the external and internal security of the EU. The Netherlands proposes the following priorities:

1. Support to Ukraine
2. Strengthening CFSP/CSDP and the European contribution to NATO
3. Mitigating high-risk strategic dependencies in medicinal products, the energy transition and digital priority domains through more strategic economic foreign policy and economic security;
4. Strengthening the European defence industry and innovation, including third-country cooperation
5. Countering hybrid threats and strengthening resilience

Support to Ukraine

- The security and future of **Ukraine** are inextricably linked to European security, so continuing support for Ukraine should be a cornerstone of the EU security strategy. Security commitments to Ukraine should build on the EU's strengths and successful track record, such as mobilising financial resources and sharing this burden among all Member States, ramping up Ukraine's defence industry, and providing technical advice and training (EUAM, EUMAM).
- It is crucial to implement the **EU Ukraine support loan** quickly and assist Ukraine – every day counts. The urgent needs of Ukraine should lead, so the derogations for the purchase of military equipment in third countries need to be used.
- Regarding the **EPF**, the current blockade of EUR 6.6bn needs to be lifted, or Member States should consider reallocating funds that cannot be allocated to the EPF to direct military support to Ukraine.

Strengthening CFSP/CSDP and the European contribution to NATO

- The Netherlands calls for **increased use of Qualified Majority Voting** in CFSP decision-making, and where needed, for appropriate use of Article 122 of the TFEU. Enhanced cooperation for those countries that wish to advance policy should be considered, for instance through the enhanced cooperation instrument.
- NATO remains the cornerstone of our collective deterrence and defence. The EU is important for taking more European responsibility for security and defence through a legislative framework, financial impulses, and coordination to incentivise common security and defence cooperation. Enhancing the **European contribution to NATO** is crucial in this regard. The Netherlands calls for further development of cooperation in the field of defence capability development and industry (see also our Food-for-Action paper, co-signed by a total of 29 NATO Allies), for example, by improving

the exchange of information on capability targets and joint procurement between relevant NATO (IS, NSPA) and EU (CION, EEAS, EDA) bodies.

- The Netherlands calls for rapid further implementation of the actions of the White Paper on European Defence. The Defence Readiness Omnibus and Priority Capability Area approach to fill critical gaps in European defence are best practices that should be built upon. We strongly advocate for further proposals **to address the legal obstacles to the operational readiness** of our armed forces and defence organisations.
- NATO article 5 remains the cornerstone for our collective defence. At the same time, it is important to **further operationalise Article 42.7 TEU** by increasing the EU's ability to coherently use all of its instruments to reinforce security within the Union and thereby NATO's deterrence in the light of a crisis. This may include the optimalisation of EU legislation in the lead up to a crisis scenario, as well as increased EU-NATO crisis management cooperation, including establishing a clear division of tasks, pre-agreed procedures, and emergency protocols (in the event of a scenario in which NATO Allies trigger Article 5 and vice versa with regard to Article 42.7 TEU and 222 TEU).
- **Intelligence cooperation** at the European level should be intensified. The Single Intelligence Analysis Capacity (SIAC) should be strengthened, as agreed in the EU Strategic Compass, including by connecting its intelligence products more efficiently and expediently to the EU's broader toolbox. A comprehensive **EU-wide threat assessment,** based on SIAC reporting, should be developed to support decision-making and ensure a shared understanding of the security risks faced by the Union.
- **Security and Defence Partnerships** (SDPs) should focus on strategic partners that are most important to European security and the EU's geopolitical interests. Existing SDPs with key partners such as the UK, Canada, and Norway should be deepened and further implemented.
- **CSDP missions and operations** should be realigned with the EU's strategic security objectives, to ensure executable mandates, to recommit the necessary capabilities to match our political ambitions in the field of security and defence, and to be bolder in adjusting our presence where needed. To enhance the effectiveness of EU external instruments, CSDP efforts should also be deployed in coherence with political engagement, development cooperation, and economic diplomacy.
- Complementarity with NATO remains a guiding principle for the continued development of EU command-and-control arrangements. Therefore, the current **Military Planning and Conduct Capability** should evolve and be strengthened in support of EU missions and operations that deliver clear added value and have the biggest impact on the security of the European continent, such as EUMAM Ukraine and EUFOR Althea.
- In order to make sanctions more effective, the Netherlands calls for the exploration and possible establishment of a **sanctions body** at the EU level.

Mitigating high-risk strategic dependencies in medicinal products, the energy transition and digital priority domains through more strategic economic foreign policy and economic security

- In an era of increasing weaponisation of economic dependencies and rising economic coercion, the Netherlands supports the EU's framework for an effective, coordinated, and coherent economic foreign policy. The EU should stand together and demonstrate solidarity, remain open to partner with third countries and businesses for our competitiveness and resilience, whilst being ready to protect and act when necessary.
- The EU should expedite efforts to identify, mitigate, and prevent **high-risk strategic dependencies and foreign influence in critical infrastructure**, including and specifically in medicinal products, the energy transition and digital priority domains. More specifically, the Netherlands advocates the need for coordinated EU action in the development and deployment of sovereign digital technologies for public administrations, in particular for cloud and AI.
- To mitigate our dependency on critical inputs, the EU needs to deliver on concluding and deepening FTAs and on diversification projects with like-minded partners via strategic partnerships.
- The EU should adopt an overall **"variable geometry" partnership approach**, i.e. pursuing ad-hoc coalitions with third countries for different (geo-economic) challenges and opportunities, based on common values and interests. Specifically, the Netherlands calls for both the deepening of existing **Digital Partnerships**, and the pursuit of new ones, also with countries in the Global South, to boost the EU's position in strategic digital infrastructure (such as sea cables) and value chains, including on semiconductors, defence-related applications, and digital services and technologies such as AI, quantum, cyber security, cloud, space, and sensors. The EU should pursue mutually

beneficial partnerships with third countries, including in the context of development cooperation and Global Gateway, to secure its broader interests, including in the security domain.

- The Commission and its Member States should adopt an integrated **European critical value chain strategy**, including coordinated financing for (commercialised) **Critical Raw Material (CRM) diversification projects** within the EU and with third countries under the aegis of the CRM Centre as part of the ResourceEU initiative. This is also necessary to tackle the market disruptions and the perceived failure of the market in the field of CRMs.
- The EU should strengthen its economic position in the most critical technologies via the Chips Act 2.0 and other forthcoming related technology and research initiatives. This requires coordinated targeted investments in critical technologies and innovation ecosystems, for example through the ECF, Horizon Europe, while maintaining a level playing field.
- The EU should better involve the high-tech industry via front-runner groups for developing **technology ecosystems** in these sectors. In addition, engagement with relevant companies and research institutions on vulnerabilities needs to be stepped up, for example through the Commission's recently proposed Trusted Advisory Group and through strengthening efforts for continuous public-private monitoring of vulnerabilities, and further follow-up of the 2024 Council recommendation on research security.

Strengthening the European defence industry and innovation, including third country cooperation

- **European defence finance** through EDIP, EDF, SAFE, and the new Multi-annual Financial Framework must support accelerating the fulfilment of identified capability shortfalls and NATO capability targets. Respect for the rule of law and effective application of the Charter of Fundamental Rights are preconditions for Union spending.
- **Further simplification and a coherent approach** to all European defence initiatives is necessary to strengthen the European Technological Defence and Industrial Base (EDTIB). Special emphasis should be placed on innovation and dual-use technologies, for many of which Europe currently has a strong position on the civilian domain, which could benefit military applications.
- The **production capacity of European industry** should scale up faster to meet current demand. Incentivizing joint development, joint industrialisation, and joint procurement should contribute to a more long-term perspective for industry to make the necessary investments in the supply chain to scale up production. The Omnibus should support the abovementioned objectives, and Member States should drive partnerships for defence industrial collaboration and a value chain approach by nurturing education, knowledge institutions, industry, and governmental programs.
- More investment in, and procurement from our own **European defence industry** is needed to improve readiness, resilience, and supply security. High risk strategic dependencies should be mitigated, and strategic partnerships within NATO should safeguard interoperability, avoid duplication, and enable cooperation with capable and key allies. Cooperation with third countries remains crucial while ramping up the European defence industry. This particularly regards the UK, Canada, Norway, and the US, also with regard to Ukraine's short-term needs, which the EU cannot meet alone.
- European policy should stimulate **open and competitive supply chains** with cross-border cooperation to ensure that the entire European defence industry can benefit from increased European demand and contribute to a resilient and competitive EDTIB.
- In cooperation with NATO, the EU must increase **AI capabilities** in the military domain and deploy them for, amongst other things, situational awareness, autonomous systems, intelligence, cyber defence, and logistical optimisation; research innovations such as AI should be systematically integrated into defence programmes. The EU should ensure interoperability of AI systems within European armed forces to make deployment effective and strengthen cooperation between civilian and military AI innovation channels in order to increase production.

Countering hybrid threats and strengthening resilience

- Tools and measures to counter hybrid threats should be integrated in a **campaign approach**, thereby facilitating asymmetrical responses that target the strategic objectives of our adversaries.

- **Response capacity** should be strengthened through enhancing cyber capabilities, improving readiness and deployment of joint hybrid and cyber response teams, as well as establishing a clear EU escalation framework for responding to large-scale cyberattacks.
- The EU should further strengthen its approach to **crisis management** by reinforcing the European *Union Civil Protection Mechanism* (UCPM) and the *Emergency Response Coordination Centre* (ERCC), based on an all-hazard and whole-of-government approach.
- **EU information-sharing structures** should be secure and improved to ensure timely exchange across Member States, EU institutions, and with NATO, in order to overcome intelligence and coordination gaps. The EU should set minimum requirements for **crisis communication** during cyber incidents and establish an EU Cyber Shield with EU-wide threat monitoring across sectors.
- To optimise societal and institutional preparation for crisis situations, **EU crisis management exercises** should be aligned with – and where possible connected to – NATO crisis management exercises.
- Regarding **resilience**, the EU should develop baseline requirements, complementary to those of NATO, as well as a stockpiling network taking military mobility into consideration.
- A **resilient, 'collectively self-reliant' society** must be created through the involvement of and cooperation between government, citizens, local communities, and civil society, the private sector, social partners, as well as the scientific and academic communities, advancing a whole-of-society engagement.
- The EU should facilitate the exchange of best practices on economic preparedness between EU Member States.
- To increase **democratic resilience,** the Netherlands calls for an **analysis of the external and internal threats** to our democracies, as well as coordination and information sharing on FIMI. This should be conducted within the Centre of Democratic Resilience to determine concrete next steps.
- Furthermore, the EU should invest in independent media and the promotion of information integrity online. In addition, the Netherlands calls for attention to strengthening—legally and financially—**civil society organisations** as indispensable players in a vibrant democracy.
- The EU should ensure consistency in external action when it comes to promoting the **responsible European AI model** along the lines of the EU AI Act and the Council of Europe Framework Convention.
- The EU should address the increasing size and speed of the dissemination of **disinformation**, economic sabotage, and digital interference. AI policy must therefore be linked to the protection of elections, protection of critical infrastructure, and the implementation of the NIS2 Directive.
- The EU should continue to work on the security of the **Schengen area**, through effective border management, countering the instrumentalisation of migration, fostering returns of individuals posing a threat to public order and national security and close law enforcement and judicial cooperation.