CHECK UPON DELIVERY

Dual Use and Military Mobility Seminar
23 February – Ghent

Good morning all,

My name is Philippe Duponteil. I am the Director of DG TAXUD - Directorate B - Customs tariffs and Digital Delivery of Customs and Taxation Policies. I would like to welcome you to the second day of this Dual Use and Military Mobility Seminar.

[round of thanks]

Yesterday, we had interesting presentations and exchanges on Credible Deterrence and Defence Readiness, Dual Use Infrastructure and Streamlining Border Crossing Procedures. The latter also containing presentations on Form 302. I would like to take this opportunity to expand a bit on that topic.

First of all because it is an example of cooperation between different stakeholders: national authorities (customs authorities and military), the European Commission, the European Defence Agency (EDA) and NATO. As was explained yesterday, the story began with the first EU Action Plan on military mobility, in which specific actions were identified to streamline and simplify customs formalities for cross-border military movements and at the same time looking to ensure synergies with NATO. In parallel to that process, the EU Form 302 was created to fill the gap and ensure the same approach for military movements outside the NATO umbrella. Also, this form can be used by non-NATO EU Member States. NATO Form 302 and the EU Form 302 are very much aligned in terms of process and content, which allows me to share with you some reflections.

From a legal perspective, digitalising EU Form 302 requires some amendments to the EU Union Customs Code. At this moment, there are no legal provisions that ensure a legal base for such a system. From a digital policy angle, especially by looking at horizontal rules such as the GDPR and the fact that there are multiple stakeholders operating this form, we would need to indicate who has access to the information, when, under which condition and if there are some special requirements considering that we are not talking about the usual customs goods, but about military goods. As you have heard from my DG TAXUD colleague yesterday, we are following the discussions between EDA and the contributing Members to ensure that the outcome of the discussion is aligned with the EU customs legislation, and to grasp the most important elements to prepare the amendments when the time comes.

Digitalising Form 302 would bring many advantages. It would facilitate cross-border movement of military goods, reduce administrative burden, bring uniformity and harmonisation. These are the traditional advantages, but having the data in a structured format could also allow extracting such information and populating other systems, just like many logistics hub function today. Such a digitalisation would also mean that the exchange and storage of information are automated. From a pure system perspective, a coherent solution would be to deploy a central system where all relevant stakeholders have access. Military personnel could authenticate via a platform, which could be similar to the one TAXUD has currently in place for economic operators. It goes without saying that such a platform and system would require extra security measures and would need to be cyber resilient.

In this regard, DG TAXUD has broad experience in delivering and running secure systems. We operate several EU trans-European systems (that are, distributed systems and networks), hybrid solutions, but also systems with links to non-customs domains. These platforms are critical infrastructures with increased visibility due to the current geo-political context.

As you know, the sanction packages in the context of the war in Ukraine are implemented and monitored through DG TAXUD customs systems.

Customs systems are a key element of the logistical chain, even more when considering military equipment. By ensuring the confidentiality and integrity of the data, the EU will create a more secure and prosperous digital environment, protecting trade, supply chains

and sensitive information, including military, financial, intellectual property and military secrets.

Customs are a key instrument in the EU's geopolitical action. Modern, secure and state-of-the art digital systems will guarantee our ability to respond swiftly to threats. Investing in robust and cyber-secure systems will protect our citizens well-being and will contribute to protecting the European values and principles.

Besides the actual development and design of these solutions, DG TAXUD brings also extensive experience in analysis and project methodology knowledge to accompany a transition from an "*as is*" to a "*to be*" situation. In this case, for military mobility 2.0 we would go from a paper-based approach, to something fully digital.

In the context of the above, we would reach out to our NATO-allies as it became clear in several discussions that there would be an absolute benefit in digitalising not only the EU Form 302 but also the NATO Form 302.

Moreover, this would be an excellent example of enforced EU-NATO cooperation. Discussions with NATO on the above are at a very preliminary stage and will for sure also have to touch upon the financing of the project that I am describing here.

If there is the wish to go in the direction I have described above, you will find an ally in our Commission Services.

Today we will hear panels about access to finance and cyber resilience of the transport infrastructure.

These are two fundamental aspects that have strong interlinks: executing projects require finance, and ensuring the cyber resilience of the transport infrastructure requires adequate project management, funding and execution. When thinking about the cyber resilience of the transport infrastructure, I am reminded about the complexities of one of the large funds we run in DG TAXUD, which is called "Customs Equipment". This fund aims at co-financing control equipment, scanners and infrastructures in general in the customs domain. It is an initiative that is working very well, and in that framework we also recently tackled the issue of cyber resilience of certain equipment, the use of 5G or networking equipment from certain unreliable producers. I

believe the experience we have developed in the past years on this programme could be of valuable to the EU-NATO task force on resilience of critical infrastructure, because we actually mapped some security challenges, thus I encourage the colleagues to get in touch one with another. At the same time, the Customs equipment programme is a good example on how to establish some funding mechanisms that tap directly into the EU budget.

With this final reflection, I leave you in the good hands of Dr Fiott for the panel on Access to Finance and Funds, and with Major General Michel Van Strythem of the Belgian Cybercommand for the panel on Cyber resilience.

I wish you a very nice day with fruitful exchanges.