Contribution of The Netherlands to the public consultation of the European Commission on the renewal of the Internal Security Strategy for 2015-2020 – 3 October 2014

The Netherlands contribution to this consultation builds on the papers and input that have already been shared by the Netherlands with all Member States and the European Commission as part of the Council's preparatory process of the post-Stockholm Programme.

1. Which specific challenges need to be tackled by EU action in the coming five years regarding international crime, radicalisation and terrorism, cybercrime and cyber-attacks, natural and man-made disasters? What role should the border security have in addressing those challenges?

2. Taking into account the developments in the next five years, which are the actions to be launched at the EU level?

The conclusion adopted by the European Council on the 27th of June 2014 on the area for Freedom, Security and Justice[1], should be used as a point of reference for the revision of the Internal Security Strategy(ISS), in order to make sure that the revised ISS is in line with the focus on consolidation, implementation and cost effectiveness. The revised ISS should first of all aim to further enhance multidisciplinary approach and operational cooperation within the existing structures and frameworks and make full use of the existing (legal) instruments. The Netherlands calls for an effective and efficient implementation of the renewed Internal Security Strategy and calls for a regular review on its effectiveness and compliance with current threatsThe Netherlands supports the view that the five strategic priorities of the current Internal Security Strategy remain valid: (1) the disruption of international criminal networks, (2) the prevention of terrorism and addressing radicalisation and recruitment, (3) raising levels of security for citizens and businesses in cyberspace, (4) strengthening security through border management and (5) increasing Europe's resilience to crises and disasters.

The Netherlands has the following key points to further improve the approach of the five strategic priorities.

1. *Enhancing security in cyberspace*

Sustained efforts are needed to strengthen cyber security and fight cybercrime, whilst ensuring an open and free internet based on the multi-stakeholder model. The Netherlands strongly supports a comprehensive approach to tackling these issues. The implementation and continued development of the EU Cyber Security Strategy will strengthen this comprehensive approach. [2] In this regard, The Netherlands attaches great value to enhancing public-private participation and strengthening cooperation at the level of computer emergency response teams (CERT).

Given the speed of developments in cyberspace, in the coming years an updated EU-Cybersecurity Strategy should be considered in order to stay on top of these developments, and to reach a next level in cybermaturity. Attention has also to be drawn to the broader problem of the use of the internet for criminal purposes. The use of the internet as an instrument for facilitating criminal activities is universally present. Europol and the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) indicated in January 2013 that the internet is facilitating many criminal

[1] Pbl EU 2014 / C 240/ 05, 24 July 2014
[2] COM (2013) 1 final.

activities, such as illicit drug trafficking and human trafficking.[3] The increasing use of the internet for criminal purposes therefore necessitates a structural, cross-border approach.

Therefore, the Netherlands supports the further development of the work of the European Cybercrime Centre (EC3). EC3 helps to strengthen operational cooperation in the fight against cybercrime and is vital in enabling Member States to quickly and effectively exchange information between law enforcement authorities to fight cybercrime. Furthermore, international cooperation regarding prevention, investigation and prosecution of cybercrime needs to be enhanced. It is important that all member states implement the cybercrime directive[4] and ratify the Convention on Cybercrime of the Council of Europe (the Budapest Convention).[5]

2. *Preventing terrorism and addressing radicalisation*

Over the past few years, numerous instruments have been adopted, especially within the framework of the EU, to prevent terrorism and to address radicalisation and recruitment, largely in the framework of European Counter-Terrorism Strategy.[6] The Netherlands considers it important to build on these initiatives.

Known terrorists from (EU Member) States have travelled to and returned from a large number of conflict zones. States are faced with a number of gaps in what they know about terrorist travel. The ability to detect and monitor travel by known and unknown foreign terrorist fighters is an important key in protecting against the threat emanating from these terrorists. High level of expertise, the correct use of detection systems and the collection and exchange of travel information in the fight against terrorism is crucial. Without it, there can be no detecting or countering of terrorist travel.

Effective and proportional detection of terrorists requires a combination of elements. Travel information should be combined with information on terrorists, routes and risk indicators. Only when names, alarming patterns are found in travel information, or other (terrorist) information is transmitted to competent authorities (e.g. law enforcement, intelligence agencies, border police) they can decide what to do to best protect their citizens. A matching system without a timely and correct check creates a false sense of security. The subsequent exchange of information on known and unknown foreign terrorist fighters between the relevant authorities in a timely and accurate manner is fundamental.

This requires proactive sharing of information on known and unknown foreign terrorist fighters and terrorist travel. Cooperation and a comprehensive approach are essential. A level playing field between States is imperative. Any and all initiatives in this field should be aligned in order to strengthen current EU, national and international (joint) efforts. Cooperation must include sharing of identities of individuals with the other EU Member States through intelligence and/or law enforcement channels and in accordance with national law. In addition to the exchange of information the use of SIS and the Europol Focal Point must be strengthened. Starting with feeding

[3] Europol and EMCDDA, *EU Drug Markets report | a strategic analysis (2013)*, pp. 118-119.
[4] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA (OJ 2013, L 218).
[5] The Convention on Cybercrime (Dutch Treaty Series 2002, 18).
[6] COM (2010) 386 final.

more cases into the SIS and broadening its scope of deployment because relying solely on a “hit/no hit” approach is insufficient.

In this context, The Netherlands reiterates the necessity of European legislation on the use of passenger data for the purpose of counter terrorism and serious crime, provided that an adequate level of data protection safeguards is part of the instrument. Therefore the Netherlands wholly supports the call from the European Council on the Council and the European Parliament to finalize work on the EU Passenger Name Record proposal. In addition, the Netherlands is committed to strengthen EU cooperation in combatting radicalisation of potential terrorists.

3. Disrupting international criminal networks

Concerning the prevention of and fight against organized crime, administrative bodies operating outside the scope of criminal law are often responsible for overseeing compliance and regulation issues in relation to particular business sectors used by criminals in EU Member States. It is therefore important that robust processes are in place to enable administrative bodies to use their powers to prevent transnational operating organized crime groups from infiltrating in the legal infrastructure in member states, such as public procurement procedures, licensing systems and subsidies. Within this context the cross-border exchange of legal and other information for administrative purposes in cross border cases needs to be improved.

Based on the ISS 2010-2014 the Commission has given practical support to Member States by establishing a network of national contact points on the administrative approach to develop best practices, by sponsoring pilot projects on practical issues and by financing an ISEC study on the administrative approach. The Netherlands attaches great value to enhance and formalize the current (informal) EU structure for administrative cooperation within the context of preventing and combating organized crime, taking into account the EU policy cycle priorities 2014-2017 as well as the recommendations in the EU anti corruption report, including the role of local and regional administrations in anti-corruptions policies. This includes embedding the role of local authorities in the network as well as improving the organizational framework for exchanging information for administrative authorities for crime prevention purposes (based on existing EU instruments). The results and recommendations of the running ISEC project on the administrative approach should be used to develop proposals in this field.

Furthermore, in the fight against organized crime The Netherlands attaches great value to dismantling criminal organizations and confiscation and recovery of criminal assets and, to this end, cooperation in investigations within the EU. Financial investigations is a crucial instrument in the process towards confiscation and recovery of criminal profits and it can be an effective tool in mapping criminal organizations. There is a need for pragmatic solutions to increase the use of this instrument and to enhance effective cooperation in this field, making use of the supporting role of Europol and Eurojust, where needed. To ensure an effective approach, The Netherlands is in favor of the development of an additional legal framework for the mutual recognition of freezing and confiscation orders in addition to the Directive on Freezing and Confiscation that was recently adopted

The effectiveness of the fight against organized crime can also be enhanced by the creation of the European Forensic Area 2020. It is important that certain essential processes are reliable and

comparable in all Member States, this also holds for the collection, processing, and use of forensic data. Applying common forensic quality management standards for forensic activities contribute to serving justice and to the efficiency of the judicial chain. After all, by achieving an EU-wide quality level, member states and police and judicial authorities and services can rely on the equivalence of each others' forensic process and data. This will increase mutual trust and promotes the exchange of the information generated and the cross-border use of the forensic evidence in criminal proceedings. It is therefore important to implement the Council Conclusions of 13-14 December 2011 for the creation of a European Forensic Science Area in 2020.[7]

The Netherlands calls for the implementation of the Directive on trafficking in human beings (THB) and the EU Strategy towards the Eradication of Trafficking in Human Beings 2012–2016,[8] and supports the establishment of a post-2016 strategy. Like the current strategy, the new strategy should be concise, concrete and multidisciplinary and confined to addressing shared problems or gaps relating to the 'four Ps': 'Prevention, Protection, Prosecution and Partnership' based on the experiences with the implementation of the first strategy. Attention should be devoted to all forms of trafficking, including THB for sexual exploitation, labour exploitation, organ removal, forced begging and criminality and newly emerging forms of THB. The strategy should be drawn up by the Commission and Members States together, to ensure the widest possible commitment of all concerned.

The fight against human smuggling needs to be enhanced. For this reason, the Netherlands supports the initiative of the Commission to develop an EU Plan against human smuggling. This plan should be based on an integrated and multidisciplinary approach, needs to address the different aspects of human smuggling, create barriers for smugglers and should include the different actors responsible for the prevention of and the fight against human smuggling.

4. Strengthening security through border management

The Netherlands believes that border management is of great importance to internal security of the EU. In principle, the Netherlands is of the opinion that existing and new systems and platforms should be aligned as much as possible, provided this improves efficiency and prevents the overlapping of national systems. It is important to safeguard data protection in this context. The Netherlands is of the opinion that the Smart borders package will contribute to strengthen the internal security of the MS. The Netherlands acknowledges the importance of good cooperation between the authorities responsible for guarding the borders of the EU and the Schengen area. Improving inter agency cooperation is especially crucial to fight illegal migration at the borders, including human smuggling and secondary movements within the EU and detecting known and unknown foreign terrorist fighters. The Netherlands supports the feasibility study of the establishment of the European System of Border Guards.

5. Increasing Europe's resilience to crises and disasters

Concerning increasing Europe's resilience to crises and disasters, The Netherlands is of the opinion that the focus should be on implementing and making full use of the new legislative framework, the

[7] Council Conclusions on the vision for European Forensic Science 2020 including the creation of a European Forensic Science Area and the development of forensic science infrastructure in Europe, doc. no. 17537/11.
[8] COM (2012) 286 final.

civil protection mechanism.[9] Joint training and exercises will help to provide more practical experience with the mechanism and ensure its effective use.

3.Which specific research, technology and innovation initiatives are needed to strengthen the EU´s capabilities to address security challenges?

The Netherlands acknowledges the importance of research in the field of security. Security is clearly addressed as one of the societal challenges in the Horizon 2020 program under the heading of 'secure societies'. The Netherlands attaches great value to Horizon 2020 and intends to play an active role in it. It is important that the projects approved are of high scientific quality and are selected in a competitive application procedure. Challenges may be found in the field of cybersecurity, in the field of disaster resilience and crisis management, in the sharing of information between different parties, in the collection and selection of information and in the development of new tools/technologies that help partners to execute their security tasks in a more effective and efficient way. It is important to note that innovation should not only have a technological focus. Challenges such as using the wisdom of the crowd and optimizing human performance are equally important in the field of security. The Netherlands considers it important that the research is conducted with sufficient regard for human rights and privacy.

Specific challenges in technology are recognized in the defensive and offensive use of technology in general, and specifically in the domain of cybercrime. The possible disruptive effect on society calls for more awareness, action and collaboration. Technology is an integral part of all security domains, and should be treated as such. The underpinning assumptions are first that technology is an enabler for security risks and benefits. Due a high volume of initiatives, the large number of stakeholders, and the contribution that new technologies can have on society call for a flexible approach and joint initiatives. Second, technology based crimes and its effects call for (operational) cooperation between the Member States. This cooperation needs to provide the Member States with a new level of understanding, enable them to forecast new trends and recognize current trends in order to make adequate response possible. And third, alliances between all domains are necessary. Technology in all its variety is present in all domains, and not only in the domain of security. The technology research for security therefore needs to be connected with the other technology research areas. Collaborative actions are foreseen in the Triple Helix cooperation, between universities, industry and government, where technology expertise is needed to combat and prevent crime.

4.What is needed to safeguard rights of European citizens when developing future EU security actions*?*

The Netherlands fully endorses the powerful protection of fundamental rights as proposed by the Commission, *inter alia* by the effective application of the EU's Charter of Fundamental Rights.

The Commission is right to observe that the promotion of fundamental rights requires efforts to be made by all institutions and member states. The European Parliament has also shown itself to be a strong protector of fundamental rights, both in the member states and in EU legislation. The

[9] Decision no. 1313/2013/EU of the European Parliament and of the Council of 17 December 2013 on a Union Civil Protection Mechanism (OJ 2013, L 347).

Netherlands believes that member states too have their part to play here, given their responsibility for implementing EU law, and that the JHA Council likewise shares responsibility in this regard.

The Netherlands agrees with the Commission that the EU Agency for Fundamental Rights (FRA) makes a valuable contribution to the development of EU policy and that it is important to cooperate closely with the Agency. The Netherlands would also recall the important work done in this area by the Council of Europe and the close collaboration between the latter and the FRA. The Netherlands acknowledges the importance of effective legal remedies for enforcing rights deriving from EU law, as enshrined in article 19, paragraph 1 of the Treaty on European Union (TEU) and article 47 of the EU's Charter of Fundamental Rights. In addition, reference may naturally be made to the case law of the European Court of Human Rights (ECtHR) under article 13 of the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR).

The Netherlands recommends making this case law more widely known in order to ensure its uniform application by national courts. This emphatically does not call for new legislation, but for an overview, for instance in the form of a Handbook drafted jointly by FRA and the ECtHR and/or a communication, of the primary minimum requirements that already apply to national procedural law. Consideration could also be given to establishing cooperation arrangements between the FRA and the European Court of Human Rights. There has been similar cooperation several times over the past few years under the umbrella of the wider collaboration between the FRA and the Council of Europe.

Several regulations and directives have been enacted in this area in recent years. What is needed now is a period of consolidation, in which experience may be gained with these instruments. In evaluating European mechanisms, it is advisable not to set about introducing more far-reaching legislation or harmonisation immediately; benefits may also be gained by informing the public. One way of improving the enforcement of EU law is by encouraging member states to make more effective use of existing national enforcement mechanisms. In addition, it is crucial to prevent the fragmentation of procedural rights. To this end such rights should be viewed in relation to each other, so that matters such as limitation periods, costs or the right to information during legal proceedings do not depend on the particular subject matter of the dispute. In this context the Netherlands also emphasizes the importance of the rapid implementation of Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012, establishing minimum standards on the rights, support and protection of victims of crime.

Next to the abovementioned actions the Netherlands welcomes a quick approval by the Council and the EP of the new EU Regulation and Directive on data protection. With these rules, which content a very strong protection of the privacy of our citizens, the EU gives form to a very important and contemporary part of the Charter of Fundamental Rights.

In this context, it is important for MS to evaluate their legislation on data retention, given the arrest of the EU Court of Justice on this issue in order to strike the right balance between on the one hand to guaranteeing the interests of our common security and on the other hand ensuring the individual fundamental rights of our citizens.

And in the relation with third countries the Netherlands emphasize the importance of a strong EU-US umbrella agreement on data protection in the field of police and judicial information , which is

still object of negotiations. The Netherlands urges the completion of the umbrella agreement in autumn 2014. Important issues for the Netherlands are equal treatment for EU and US citizens and the right of access to the legal system of the US for EU citizens, who are not residents of the US, with the purpose to get full redress. A Congressional Agreement will be necessary to achieve these goals.

5. How can the EU´s foreign policy improve the security within the EU and/or your country?

As external and internal security are increasingly interlinked, better coherence between internal and external actions of the EU is needed. Strengthened coordination between various actors, EU Member States, EU institutions and agencies, would provide a more effective approach of the common challenges and result in better resource- and cost-effectiveness. Furthermore, strengthening cooperation between the fields of internal security (JHA) and external security (CFSP including CSDP and the European Neighbourhood policy) promotes an integrated approach towards stability both within and outside the EU's borders. The Netherlands wishes to focus on two key points.

First, as emphasized by the European Council (30 Augustus 2014), determined action is required to stem the flow of foreign fighters, calling for accelerated implementation of the package of EU measures in support of Member States efforts, aimed atpreventing radicalisation and extremism, sharing information more effectively - including with relevant third countries, dissuading, detecting and disrupting suspicious travel and investigate and prosecuting foreign fighters. The 'foreign fighters' phenomenon illustrates how closely the internal and external aspects of EU counter-terrorism are linked. The EU Coordinator for Counter-Terrorism has a crucial role in this matter.

It is essential that the existing cooperation on this phenomenon with multilateral organizations and international fora, such as the United Nations (UN) and the Gobal Counter Terrorism Forum (GCTF) continues. In this respect, focus should be placed on cooperation with the countries in the affected region, for instance on exchanging information to curb the jihadist travel. But the same is true for development cooperation aimed at enhancing economic growth and stability, especially the rule of law. Moreover, exchange of best practices in relation to strategic communication to stem the growth of jihadism and to strengthen the resilience of moderates are necessary as well.

Next to such robust coordination at EU level, close operational cooperation should be developed with third countries to develop a coherent approach towards combating terrorism/foreign fighters. Based on agreement on common strategic objectives and priorities for practical cooperation for practical cooperation in the region, focal action includes strengthening border and aviation security and counter-terrorism capacity.

Second, in a world where digital opportunities and threats have no boundaries, good cybersecurity also requires strong coherence between internal and external policies. Since cyber security threats do not stop at borders enhanced international cooperation in strengthening cyber security is also essential to reach the next level in cyber maturity.

Third, as recently illustrated in the Mediterranean, the cooperation with countries of origin and transit of migration must be intensified to foster legal mobility and tackle illegal immigration. To achieve this, we should focus on the combating of organized immigration crime, the trafficking in human beings and the development of policies aiming at tackling the root causes of migration. This

includes better use of Frontex, Europol and Interpol and all the tools under the GAMM. The latter should be developed as the overall EU strategic framework for external migration cooperation, with a focus on priority countries (including agreed country-specific strategies). A joined up policy approach foreseeing effective coordination and cooperation structures is required in negotiations with third countries (e.g. trade, development and other relevant policy areas). This will ensure that partnership on migration, including a “more for more” approach, is sufficiently prioritized and built into third country and regional dialogues. Swift implementation of the measures of the Taskforce Mediterranean are of a great importance.