

HOUSE OF LORDS

European Union Committee

17th Report of Session 2010–12

The EU Internal Security Strategy

Report

Ordered to be printed 17 May 2011 and published 24 May 2011

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 149

SUMMARY

The security of the Member States is often regarded as being their exclusive preserve, but since 1975 the interior ministers of the European Community have been discussing increased cooperation on internal security matters. Since the Treaty of Maastricht the Union has been given an increasing role. Now, following the Treaty of Lisbon, the Council has been given the power to adopt and implement an internal security strategy. It did so in March 2010, and this was followed in November by a Commission Communication setting out the priorities, and how to implement them.

The Communication sets out "Five steps towards a more secure Europe": the disruption of international crime networks, the prevention of terrorism, security in cyberspace, improved border management, and increased resilience to crises and disasters. We agree that these are the matters on which implementation of the strategy should be focussed. It is this Communication which has been the object of our inquiry.

Progress on these five fronts is designed to lead to a more secure Europe. In each case we have looked in detail at the actions proposed by the Commission to advance security. Most of these will involve increased practical cooperation between the Member States, and some will involve proposals for legislation over the coming three years. We hope that our recommendations may help the Commission when it comes to formulate its proposals. We hope too that the Government—and perhaps also other Member States—may find our views helpful when they come to consider the legislative proposals.

International crime, terrorism, illegal migration and natural disasters have been with us a long time. Cyber-security is a comparative newcomer. Even a few years ago, cyberspace was thought to provide an opportunity only for small-scale criminal acts. It is now clear that, in addition to increasing the outreach of international crime, it can lead to massive disruption of state infrastructure, and can be used for espionage, terrorism, even war. During the course of our inquiry there were major attacks against the EU institutions. It is not surprising that much of the evidence we received concerned the role which the EU might play in fighting cyber-attacks. The Commission's main proposal is to set up a new Cybercrime Centre. This might be no more than a talking shop, but it could become a useful tool for investigating and analysing past attacks, improving law enforcement, and preventing future attacks. Much will depend on whether it is given adequate resources for what could be an important role.

Security knows no borders. We have looked at the way in which the internal security strategy overlaps with national and international strategies, in the hope that they can be mutually supportive. And lastly we have looked at the implementation of the strategy. The Council has an extraordinary number of committees, working groups and other bodies whose tasks overlap and can conflict. It also has one new committee which, under the Treaties, has the duty of coordinating all the work on internal security. Unless it does so effectively, very little will be achieved; if, with the right membership and the right chairmanship, it properly fulfils its mandate, the EU may play a valuable role in protecting the security of its citizens.

CHAPTER 7: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

The EU's role in Internal Security

201. For the purposes of this report we are treating internal security as the ground covered by the Commission Communication, and believe this provides reasonable and pragmatic boundaries for a strategy and for its implementation. (paragraph 16)
202. The security of the United Kingdom does not begin or end at the water's edge, and cannot be defended independently of the security of other States. (paragraph 17)
203. Member States' national security and the EU's internal security are inextricably linked. We do not believe that these proposals intrude upon or threaten Member States' primary responsibility for national security. (paragraph 22)
204. We welcome the Communication as the first pragmatic attempt to articulate a comprehensive approach to the EU's internal security. (paragraph 23)
205. The five objectives proposed in the Communication, while broad and demanding, are sensible, practical and achievable, with the potential to raise standards among Member States and therefore to enhance the EU's security as a whole. All future proposals in this area should be developed on a sound evidential base, with priority given to tackling identifiable threats, and with full impact assessments and cost-benefit analyses. (paragraph 24)
206. We believe that it is shortsighted of the Government to criticise some Commission proposals solely on the ground that they go beyond what was agreed in the Stockholm Programme or the Internal Security Strategy itself. Achieving internal security is a moving target; over the five years covered by this Communication it may well require action beyond what is envisaged in the Stockholm Programme. Each proposal should be assessed on its merits. (paragraph 26)

Fundamental rights

207. Enhancing security while at the same time safeguarding fundamental rights is best done by careful scrutiny of the individual legislative proposals as they are brought forward, to see whether too much freedom is being sacrificed to achieve a high a degree of security. The European and national Parliaments have an important role to play. (paragraph 37)
208. We look forward to considering the Commission's proposal for a comprehensive data protection framework when it is published later this year. However there is already some risk that the Council and the Government will pursue a line which could result in different principles governing different measures. (paragraph 40)

European External Action Service

209. We urge the Commissioner for Home Affairs and the High Representative for Foreign Affairs and Security Policy to work closely together to ensure the close alignment of internal and external security. We believe that structures

to ensure that alignment is made a practical reality should be established urgently. (paragraph 49)

210. COSI and the Political and Security Committee should hold regular joint meetings on a similar basis. (paragraph 50)
211. We welcome the appointment of JHA staff to work in some overseas EU missions, and hope that this will be extended so that the EEAS may become an effective means of achieving good cooperation between those responsible for the EU's internal and external security. (paragraph 51)
212. We welcome the recent appointment of the new director of SitGen. We hope that it will continue to develop a wider security assessment role within the new EEAS structure, and will make an effective input to internal security threat assessments. (paragraph 52)

Relations with the United Nations and NATO

213. Vigorous engagement by the EU with the international community on security matters is crucial in order to tackle new and developing security threats. The EU should use its negotiating weight to influence the agenda accordingly. (paragraph 56)
214. We have repeatedly urged that relations between the EU and NATO should be improved and developed. The current situation should not be allowed to continue. The Government, as a major actor in NATO, must take urgent steps to improve cooperation. (paragraph 57)

Relations with strategically important third countries

215. We note the continuing importance of EU-US cooperation on security matters, but believe that the EU should also step up its cooperation, however challenging this may be, with other strategically important third countries such as Russia, China, Turkey and Pakistan in order to mitigate the external risks to the EU's internal security. (paragraph 64)
216. We welcome the endorsement by the Council of a readmission agreement with Turkey, but regret the delay in its implementation. We also regret that the Government have decided not to participate in the Decision authorising negotiation of a readmission agreement with Belarus. (paragraph 65)

Serious and organised crime

217. We welcome the establishment of the organised crime "policy cycle" by the Council and commend SOCA's positive engagement with COSI on organised crime matters. (paragraph 70)

Passenger Name Record (PNR) data

218. We welcome the Government's decision to opt in to the draft Directive, and support their intention to continue to argue that the Directive should apply to intra-EU flights. (paragraph 72)

Money laundering

219. The Government's continuing failure to ratify the Warsaw Convention on Money Laundering and Terrorist Financing is inexcusable. We repeat our view that this prevarication sends out a negative message about the

Government's commitment to this important matter. We again urge the Government to sign and ratify the Warsaw Convention without further delay. (paragraph 74)

Confiscation of criminal assets

220. The establishment of functioning Asset Recovery Offices in each Member State should be given a higher priority before the conferral of additional functions is considered. (paragraph 76)

Joint Investigation Teams (JITs)

221. We share the Government's enthusiasm for the work of Joint Investigation Teams and support the greater use of this tool in the fight against cross-border organised crime. (paragraph 79)

Counter-terrorism

222. We commend the work of the Counter-Terrorism Coordinator but believe that his role needs to be clarified and reviewed following the entry into force of the Treaty of Lisbon. In the meantime, we believe that he could play a useful role as a bridge between the internal and external aspects of terrorism. (paragraph 84)

Radicalisation and recruitment

223. The proposal to establish an EU radicalisation-awareness network will be a positive step if its functions are clear and well-defined. However we believe that Member States should continue to have the primary role in this area. We are less convinced that production by the Commission of a "handbook of actions and experiences" would either be practical or add value. (paragraph 90)

Preventing terrorists' access to materials and funding

224. We believe there is in principle a case for the establishment of an asset-freezing regime applicable to individuals resident within the EU. To be effective this will require the cooperation of third countries, in particular Switzerland and Liechtenstein. (paragraph 93)

Transport security

225. The security of transport networks is a vital component of the security debate. However we reserve judgment on the EU's role in this area pending the publication of the Commission's Communication on Transport Security Policy later this year. (paragraph 95)

Border management

EUROSUR

226. We welcome the Government's commitment to make an effective contribution to the development of EUROSUR and the future work of Frontex. Despite the United Kingdom's inability to participate fully in EUROSUR and Frontex, we believe that their work will make a positive

contribution to the protection of the United Kingdom and EU borders. (paragraph 102)

Civil protection and disaster relief

The role of the armed forces

227. We are surprised to find no reference to the armed forces in the Communication. They make a major contribution to civil protection and disaster relief, especially in the early stages. Their role must feature in the implementation of the strategy. We urge the EU institutions to give more thought to this. (paragraph 106)

The Solidarity Clause

228. The Solidarity Clause does not seem to empower Member States to do anything which they could not do without it, or require them to do anything they would not otherwise be required to do. It does however serve to emphasise the political will of the Member States to stand together in the face of adversity. (paragraph 108)

Risk assessments and cooperation between Situation Centres

229. We support more coordination between different Situation Centres and repeat our call for a closer working relationship between the EU and NATO Situation Centres. We also support a reduction in the number of existing rapid alert and notification processes for crisis management. (paragraph 111)

The development of a European emergency response capacity

230. We have practical concerns about the operation of a European Emergency Response Capacity. We believe that any pre-commitment of assets should be on a voluntary basis, and that Member States should retain a discretion to decide how their assets are best deployed. (paragraph 114)

Cyber-security: the challenge

231. We congratulate the Government on the priority they give to cyber-security in the United Kingdom National Security Strategy. But there is no room for complacency. All Member States, individually and collectively, must devote greater resources and urgency to meeting this challenge, given that their overall security is only as strong as the weakest link. (paragraph 122)
232. The EU institutions should take the lead by ensuring the security of their own networks and agencies. They are a natural target for malicious and criminal attack; weaknesses have been and will be exploited. They must take responsibility for their own cyber-security; it is in the interests of the United Kingdom to help them to do so. (paragraph 123)

Cyber-security: the role of the EU

233. We strongly welcome the emphasis on cyber-security in the Communication and believe that this is an urgent and fast evolving challenge in which the EU can play an important part in raising standards and awareness in the Member States. (paragraph 126)

The Budapest Convention

234. We welcome the Government's commitment that the United Kingdom will ratify the Budapest Convention on Cybercrime before the end of this year. (paragraph 131)

Cybercrime Centre

235. The establishment of a Cybercrime Centre will enhance the EU's ability to contribute in this area. This is not an end in itself, but only one of many measures that must be deployed. (paragraph 146)
236. Europol would be best placed to host such a body. However, we believe that finding staff with the necessary expertise may not be easy. Additional staff and funding will be essential if the Cybercrime Centre, wherever it may be situated, is to achieve its key aims. The Government's view that this can be done within existing resources is unrealistic, and inconsistent with their making additional resources available for the United Kingdom's programme. (paragraph 147)
237. We believe that the Centre should form a close working relationship with ENISA, and we support the extension of that agency's role and mandate to cooperate with law enforcement agencies. (paragraph 148)
238. The dispersal of agencies dealing with cyber matters is especially unfortunate. In particular, we continue to have concerns about ENISA's ability to operate effectively from its geographical location. We endorse the European Parliament's proposal that the agency's operations could be "frontloaded" in Athens. (paragraph 149)

Improving response capabilities

239. Many Member States already have an adequate emergency response capacity and do not need to change their existing CERT structure. But it is essential that every Member State should have an adequate emergency response capacity, and this may need to take the form of a national CERT. Where this is lacking, it should be addressed as a matter of urgency. Individual weaknesses will undermine the collective security of the EU. (paragraph 155)

Raising public awareness

240. A strong working relationship between the public and private sectors will be crucial in raising awareness of the threats from cyberspace. This needs to happen at both Member State and EU level through joint forums involving all of the key players. The EU can and should add value in this area by improving public awareness. (paragraph 159)

International cooperation

241. The global nature of the cyber threat requires an international response. Proactive collaboration within the international community, including the EU, UN and NATO, will be indispensable if agreement is to be reached on the nature of the threat, and on whether it can realistically be addressed. (paragraph 164)
242. We commend the United Kingdom initiative to host an international conference on cyber-security, and hope that a wide range of countries and

organisations with a legitimate interest will be invited. We look forward to considering the outcome and the effect it may have on the EU. (paragraph 166)

Implementing the Strategy

243. We note the Government's emphasis on practical cooperation, but do not believe that this should exclude further EU legislation if that should prove necessary. We reiterate the importance of adopting a flexible approach in order to respond in an effective manner to unforeseen events raising issues of internal security. (paragraph 169)

Council and Commission structures

244. A fundamental culture change within the EU institutions is needed to achieve a more effective approach to working practices, including in particular more integrated working and investment in the necessary training. (paragraph 170)
245. The work of Council groups involved in internal security should be further streamlined, with a reduction in their number as an overall objective. We also urge the different parts of the Commission to coordinate their work more closely. (paragraph 175)

The Standing Committee on Operational Cooperation on Internal Security (COSI)

246. We trust that over time COSI will emerge as the lead organisation in all matters of EU internal security, and that this will provide the opportunity for other groups and bodies to be rationalised and their number reduced. (paragraph 179)

Membership

247. We believe that COSI would benefit from having greater consistency and continuity in its membership. The Home Affairs Commissioner should be invited to attend each meeting of COSI as a matter of course. (paragraph 181)

Chairing arrangements

248. COSI would benefit from less frequent changes in its chairmanship. It is a less political body than the Council, so there is no conceivable logical connection between the nationality of the person best qualified to chair COSI and the identity of the Member State holding the Presidency. We believe that a suitably qualified chairman of COSI should be appointed for a minimum period of two years, renewable once. (paragraph 183)

Transparency and parliamentary oversight

249. There should be greater openness about COSI's activities so that it does not appear to be secretive and lacking in transparency. (paragraph 185)
250. We have recommended that inter-parliamentary oversight of the work of Europol could be by bi-annual meetings of the Chairmen of the home affairs committees of national parliaments and the LIBE Committee of the

European Parliament. We believe that such meetings could also consider the work of COSI. (paragraph 186)

EU agencies

251. We welcome the moves already being made for better coordination and cooperation between EU agencies, and hope that the Government will press for further action on this front. (paragraph 190)

The Internal Security Fund and security research

Funding

252. We welcome the proposal for the creation of an Internal Security Fund and endorse the proposed amalgamation of the ISEC and CIPS funding streams. We believe that a case may be made for increasing the level of funding for the Internal Security Fund under the next Multi-annual Financial Framework, contingent upon reductions being made in other budget headings. (paragraph 195)

Research

253. EU-funded research projects will continue to play an important role in underpinning future EU internal security action and initiatives. Future funding allocations should be informed by the threat assessments and should also be more closely aligned with the priorities of the relevant Commission Directorates General and EU agencies. (paragraph 198)
254. Priority research areas should include cyber-security and the behavioural aspects and technology involved, as well as the ideological foundations of terrorism. (paragraph 199)

Conclusion

255. We believe the Commission has chosen the right priorities for an internal security strategy, and that these deserve support. (paragraph 200)
256. We recommend this report for debate. (paragraph 13)