Black Holes BV 

DETECTOR:
Legal Aspects of (Threats of) Intentional Interference with GNSS-Based Road Sector Services

Frans G. von der Dunk*

1. Introduction: Threats to Road Applications

The use of signals and services provided by Global Navigation Satellite Systems (GNSS) is vulnerable to different types of disruption, which can result in a degraded service or even in the absence of any service at all. Unintentional disruption can be caused through natural phenomena such as high levels of ionospheric activity and solar flares and the unwanted effects of other radio-frequency transmissions while intentional disruption more deliberately deprives the user of (useful access to) the signals.

As to the latter, it is increasingly likely that deliberate interference and jamming will increase due to the proposed roll-out of several high profile GNSS-based initiatives; principal among these are the plans for GNSS-based road user charging schemes. This situation is made worse with the appearance of multiple low-cost GNSS-jammer products that are now available on the Internet, as well as 'Do-It-Yourself jammer construction manuals' informing the public how to build their own GNSS-jamming equipment from low-cost consumer electronics parts.

Potential attacks on the use of GNSS technology for these purposes could come from sections of the public who see such use as an invasion of privacy – alternatively, simply wish to avoid taxation. Other attacks can come from terrorists, anarchists and criminals. Jammers could be located at static points (such as on rooftops or at airfields) or in a dynamic context (such as when located on board a vehicle). Attacks could target operations within rural settings, motorways, airfields and ports as well as within urban environments. The range of a high-power jammer can reach up to 50 km, while a micro-jammer range may be as little as 4 m, offering the prospect of having a personalised jamming capability that could go undetected. As a result of the plethora of different jammer technologies available, any detection system will need to provide widespread coverage as well as a high resolution of detection capability.

2. The DETECTOR Project: Detection, Evaluation and Characterisation of Threats to Road Applications – and Legal Aspects thereof

With a view specifically to the development of EGNOS and Galileo as the two European satellite navigation systems intended for widespread usage,[1] among others the GNSS Supervisory Authority (GSA), directly responsible for the roll-out of Galileo, the European Space Agency (ESA), acting as procurement agency for the system's space and space-related components, and the member states of the European Union and ESA have recognised the threat from jammer technology to the continuity and availability of GNSS services.

As a direct result several initiatives are underway within the European Union to develop GNSS-jammer detection, isolation and mitigation capabilities and technologies. The current paper addresses one of the most prominent ones, the DETECTOR project on Detection, Evaluation and Characterisation of Threats to Road Applications.[2]

---

[1] See Regulation 1285/2013/EU.

[2] See for more information http://www.gsa.europa.eu/news/detector-making-gnss-road-applications-even-safer.

* *Frans G. von der Dunk is Harvey & Susan Perlman Alumni/Othmer Professor of Space Law at the University of Nebraska-Lincoln. He also, in his capacity of Director of Black Holes B.V., The Netherlands, served as the legal partner in the NSL-led consortium which executed the DETECTOR project.* *The author is grateful for to Mark. Dumville, NSL Manager, for his comments and suggestions regarding an earlier version of the present paper.*

The DETECTOR project, which was implemented over the course of 2012 and 2013, thus developed a system for detecting, characterising and classifying radio-frequency interference sources which have the potential to disrupt GNSS services. That system consists of low-cost probes which can be installed at the roadside or around other infrastructure, and a back-office facility. The probes operate autonomously, continuously monitoring the radio-frequency spectrum around the GNSS L1 frequency. If radio-frequency interference is detected, the probes will store a sample of raw radio-frequency data, perform some preliminary analysis, and then communicate this automatically to the back-office. Further automated processing at the back-office determines the type of interference, making it possible to differentiate between deliberate jamming and unintentional interference.

An important element in this context was the analysis of key legal aspects of the implementation of DETECTOR. It is one thing to devise a system able to detect and characterise interference threats or actions, and even to pinpoint the various sources thereof; it is another to be able to prosecute the alleged perpetrators and enforce compliance with requirements to abstain from such interference. This aspect essentially falls apart in three further legal questions: (1) to what extent do existing regimes for radio-frequency management provide for legal protection against interference, (2) to what extent do existing road-tolling regimes provide for such legal protection, and (3) to what extent would, almost as a safety-net option, general criminal law offer workable legal instruments to governments to address interference threats or actions.

Finally, noting the interests in creating a European-wide system of GNSS-based road sector applications, it is adamant that the issue will be addressed in a harmonised manner across Europe. To the extent that indeed national variations in radio-frequency management, road-tolling regimes and criminal law present a further threat to effectively combating intentional interference in Europe, as well where such national regimes fall short of the desired level of protection anyway, the question thus arises: could the European Union step in and take the lead in developing a legal regime properly protecting GNSS-based road sector services against interference whilst recognising for example that, for a system like DETECTOR to be politically acceptable, sufficient guarantees need to be in place to allow appropriate protection of private information? This is the final question also addressed by the legal analysis undertaken within the DETECTOR project, as it quickly became clear that, indeed, the legal environment across the Union's member states is far from harmonised or even geared to appropriately protecting GNSS-based services at all.

3. A Crash Course in EU law as Relevant for DETECTOR

For the European Union's organs to politically *and* legally (be allowed to) take the lead in enhancing the legal environment within which DETECTOR devices and services should address intentional interference to GNSS-based road-sector services, it needs to have the relevant competences under the treaties establishing the Union and its functions.

As of yet specific clauses in the main EU treaties offering broad EU-level competences in the areas directly relevant to DETECTOR are absent, whilst in accordance with the key principle of 'conferral' "the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein".[3] Still, the Union more generally has an exclusive competence to legislate where it concerns the customs union and the competition regime necessary for the proper functioning of the Internal Market, protection and improvement of human health, industry, tourism and civil protection, which would each be relevant in a DETECTOR context. Furthermore, the Union has at least a legislative competence shared with the member states with regard to other Internal Market aspects than the more specific

[3] Art. 5(2), Treaty on European Union.

competition regime-related ones referred to above, environment, consumer protection, transport, Trans-European Networks and common safety concerns in public health matters, as all also relevant in the context of DETECTOR and the current analysis, especially as far as road tolling is concerned.

The key to using these competences then lies in the principles of 'subsidiarity' and 'proportionality', as defined by the Treaty on European Union and the Treaty on the Functioning of the European Union. 'Subsidiarity' means that "the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level"[4]. 'Proportionality' in turn requires that "the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties"[5].

In order to determine to which extent the European Union in the context of DETECTOR could actually take the initiative to develop legislation addressing the concerns noted above, it is necessary to analyse the current legal frameworks in the areas of radio-frequency management, road tolling and more generally criminal law, and determine where, how and with what level of detail the EU organs, notably the European Commission, could move in. The following provides a very basic summary of the extended analyses that were performed in this context in the course of the DETECTOR project.

It should be noted finally that, for reasons of efficiency and time- and resource-related constraints, in the context of DETECTOR only four domestic regimes of EU member states were analysed, to obtain a general assessment of the extent of the need or desirability to address relevant issues at a Union-level, as opposed to leaving it to national authorities to deal with them. The countries analysed were Germany, France, Belgium and Slovakia.

4. Radio-Frequency Management: Assessing the Current Legal Situation within the Union

When it comes specifically to the issues addressed by DETECTOR, the national regimes on radio-frequency management lack a harmonised approach in many respects, whereas the Union's competences have so far largely resulted in a harmonised legal framework in the realm of specific monitoring and enforcement competences only as regards Intelligent Transport Systems (ITS) or specific relevant frequency bands, and the accompanying tasks and obligations of National Regulatory Authorities (NRAs) under EU law.[6]

In this context, indeed there is a substantial amount of regulation available already at the international and EU levels to appropriately address especially the often-voiced concerns regarding privacy. In particular the Data Protection Directive as amended twice[7] gives shape to the principle of protection of privacy-sensitive data through obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out. All actors in the various operating chains of GNSS applications in the context of road transport would be concerned, and EU member states are required both to abide by those rules themselves and to ensure that private

[4] Art. 5(3), Treaty on European Union.

[5] Art. 5(4), Treaty on European Union.

[6] See Directive 2002/21/EC, Directive 2002/20/EC, Decision No. 676/2002/EC, Decision 513/2005/EC, Decision 771/2006/EC, Decision 432/2008/EC, Decision 381/2009/EC, Decision 368/2010/EU, Decision 829/2011/EU, Decision 98/2007/EC, Decision 131/2007/EC, Decision 343/2009/EC, Decision 671/2008/EC, Decision 766/2009/EC, Decision 251/2011, Directive 2009/140/EC, Directive 2010/40/EU and Decision 243/2012/EU.

[7] This concerns the original Data Protection Directive, Directive 95/46/EC, as amended by, first, Directive 97/66/EC, and, second, Directive 2002/58/EC.

operators within their respective jurisdictions abide by them. Thus, in the context of activities combating jamming and other interference activities as well as, of course, the original GNSS-based road sector applications to be protected thereby, any personal data can essentially only be processed in accordance with (largely) EU-level legislation, specifying the limited purposes for which such handling of personal data could be allowed.

Beyond that, however, the national regimes as they apply to radio-frequency management are rather individual, sometimes even idiosyncratic. In contrast to for example Germany, in France jammers are simply and explicitly prohibited in this context, except (1) if "authorised for the purposes of the public order, defence and national security, or judicial proceedings"; or (2) as installed in theatres.[8] Furthermore, in France four precise grounds have been recognised for refusing assignment and authorisation of the use of radio frequencies amongst which are sanctions incurred by the requesting operator with reference to preceding operations, for example if unable to stop or prevent harmful interference. Somewhat similarly to France, under Belgian law an exception to the inability to obtain a license for jammers concerns GSM jammers in prisons.[9]

The main conclusion from the analysis of the radio-frequency management issues is that the need for EU-level harmonisation with a view to addressing threats to GNSS-based interference is clear. At the same time the EU framework does offer a wide array of tools here potentially or actually helpful in minimising the threats by jammers and other interference devices, at least once the seriousness of the threats of jamming and the compliance of prospective EU-level legislative initiatives with 'subsidiarity' and 'proportionality' would unequivocally be established. In particular the areas where the Commission is endowed with specific monitoring and enforcement competences, regarding for example ITS or specific relevant frequency bands, and the accompanying tasks and obligations of NRAs under EU law, may be very helpful from this perspective.

However, it also must be acknowledged that most of this framework regime targets competition and market issues and other possible obstructions to *bona fide* service provision and intended 'active' usage of radio frequencies – not, or only occasionally and/or implicitly and/or indirectly, either such 'active' usage by international interference activities or 'passive' usage by DETECTOR for purposes of monitoring, enforcement and sanctioning. In most cases therefore, a clear need for an EU-wide harmonised regime substantially tackling interference with GNSS-based road sector services becomes evident.

5. Road-Tolling Regimes: Assessing the Current Legal Situation within the Union

As for road tolling within the European Union, the operational as well as legal environment is considerably more fragmented still than in the realm of radio-frequency management. Road tolling has always been very much a matter of national law, which means that also using GNSS in that context and possible interference with such services has very much been a matter of national law.

For instance, Germany stands out as the country within Europe where GNSS-based road tolling has developed most extensively, albeit only so far with regard to heavy goods vehicles using the interstate highways and a few parallel federal trunk roads.[10] Also, German law fundamentally lacks specific provisions on combating intentional interference with GNSS-based or other road-tolling systems, as a logical corollary for the absence thereof on the EU level – as the German regime was very much driven by Directive 1999/62/EC and follow-on EU regulations – and

[8] Art. L-33-3-1(II), resp. Art. L33-3, *sub* 'NOTA', Code on Postal and Electronic Communications.
[9] See Art. 4, Royal Decree on private radio communication and user rights for fixed networks and trunked networks.
[10] See the 2002 Motorway Toll Act as amended by the 2011 Federal Road Toll Act.

 

presumably for largely the same reasons. It is very much limited, as far as any enforcement and penalisation is concerned, to (individual) drivers trying to avoid paying tolls, not addressing for instance more fundamental terrorist or activist actions against road-tolling systems as such, including intentional interference.

One major legal difference between the French and German road-tolling systems is that in the former elements of criminal law and penalisation of intentional avoidance of toll obligations are explicitly addressed. A major 'flaw' from that perspective, however, is the absence of (unequivocal) applicability to interferers who are *not* drivers, or not drivers at the moment of undertaking their interference activities, which therefore presents one area where EU-level legislation and regulation should complement French legislation. Another problematic issue in this respect concerns the imposition of legal responsibilities in particular on toll road users, which moreover are not clearly delineated especially *vis-à-vis* those of the operators, and in turn to those of the authorities.[11] Generally, lack of clarity on respective responsibilities is a recipe for legal complications allowing those intent on doing harm considerable manoeuvring room to do so, in particular where the main issue of terrorist and activists turns out to be hardly impacted so far, if at all, by the legal regime at issue.

In Belgium there is currently only one major road subject to road-tolling, whilst the most eye-catching element of the Slovak regulatory regime for electronic road tolling concerns the extended and detailed handling of the On-Board Unit (OBU) contracts, including elaborate detail on the data to be collected, which points to the relevance of addressing potential data protection and privacy issues involved.[12] Furthermore, like in France the Slovak regime on road tolling pays considerable attention also to enforcement and penalisation issues.

Beginning to address such and other national divergences, there are some EU-law documents providing legal parameters within which national road-tolling systems would currently have to operate as within Europe toll charging is a fast growing and sizeable economic activity, having distinctive economic trans-boundary effects on road traffic. They arose from the principles of fair and free competition without discrimination within the Union,[13] both in the context of PPP approaches to road tolling (which should offer equal opportunities to be granted a concession as between providers interested from various member states) and in the context of tolling users (which should not discriminate, for example, between road users from various member states). In this sense, road tolls are essentially akin to taxes, whilst they would also touch upon issues of general economics and environmental degradation the Union is increasingly concerned with. Thus several specific pieces of EU legislation have now been enunciated on the issue, including one on the definition of the European Electronic Toll Service (EETS).[14]

However, while the EETS in particular goes a long way to establishing a harmonised EU-wide, (largely) GNSS-based road-tolling system, from the DETECTOR perspective it falls short in two respects. First, the EETS expressly operates complementary to national systems, meaning that it essentially offers an additional means for toll collection, rather than a substitute for nationally-divergent systems. Secondly, with the general lack of awareness of vulnerability of GNSS-based road sector services to jamming efforts and the relative novelty of such services technically, operationally and legally, so far such harmonisation does not at all address the issues perhaps of greatest concern here: how to effectively combat wanton interference with such activities, in particular if for terrorist or activist purposes.

[11] See Art. L121-1, Traffic Code.
[12] See Guide for Electronic Toll Collection in the Slovak Republic, 18-9.
[13] See esp. Arts. 101-109, Treaty on the Functioning of the European Union.
[14] See the aforementioned Directive 1999/62/EC, Directive 2004/52/EC, and in particular Decision 2009/750/EC.

The EETS should therefore ultimately be viewed as just a first stepping stone towards such a regime. Widespread and harmonised electronic tolling following from the establishment of the EETS allows for a clear focus of EU-level legislative initiatives to then tackle threats to GNSS-based road sector services also on a widespread and harmonised basis, by complementary regulation specifically addressing the criminality of such jamming efforts.

6. Criminal Law: Assessing the Current Legal Situation within the Union

One of the problems thus resulting from the analyses of the legal radio-frequency management and road-tolling environments was that criminalisation of wanton interference with GNSS-based road sector services was largely absent under at least several of the national and certainly the international and EU-law regimes handling radio-frequency management issues respectively road tolling.

However, legally speaking such intentional jamming might well be addressed also in other and/or broader criminal law statutes, such as those addressing general intentional interference with legitimate activities of others resulting in considerable economic harm and/or safety-risks, or addressing any threats against legitimate security activities of public authorities. Thus, an analysis of criminal law, as a generic instrument to back-up more specific legal countermeasures to threats to GNSS-based services in the context of radio-frequency management and road tolling, and its definition of criminalised behaviour and the mechanisms to adjudicate and sanction it, which may in principle also (come to) be applied in the specific context of interference with GNSS-based road sector services, had become appropriate.

Criminal law has, traditionally, much more than radio-frequency management and even more so than road tolling, been seen as a natural domain of national sovereignty and national law. The result is, not surprisingly, considerable differentiation also amongst the various EU member states as to how criminal law would apply, or could be applied, to issues of intentional interference with GNSS-based road sector services.

In Germany, a host of potentially usable legal tools would be available for prosecutors, and occasionally for other parties involved, but none of them seems particularly tailored to the problems currently at issue. Whether such wanton interference activities would have to be addressed as misdemeanours or as felonies, and in the latter case, whether they should be considered for example to be of substantial significance so as to trigger additional criminal-law options, remains presently unsettled. Further uncertainties so far as to the applicability of specific definitions (such as of ‘computer sabotage’ or ‘data espionage’[15]) add to the general confusion and uncertainty as to applicability of German criminal law in this respect. One interesting feature particularly helpful from the present perspective however concerns the potential to seize devices implicated in jamming activities or efforts to undertake them,[16] especially where outright possession of jamming or other interference devices is not criminalised (yet).

One notable distinction of French criminal law as compared to German law is the larger measure of attention paid in the former to the procedures for applying and enforcing criminal law as opposed to detailing the substance of what is considered criminal or not. This distinction gives rise to less specificity of the categories referenced in the French legislation, and hence at least *prima facie* to greater ease in including the types of activities DETECTOR is addressing within those (broader) categories. In terms of substance furthermore the French regime applies a different sub-categorisation, not providing for a special sub-regime for privacy issues but subsuming this into the broader category of crimes against a person.[17] Whether that testifies to a

[15] See Secs. 303b resp. 202a, Criminal Code.
[16] See Secs. 73, 74, Criminal Code.
[17] See Art. 226, Penal Code.

larger sensitivity in Germany to privacy or not, it may give rise to some confusion and/or complications in any context broader than the exclusively-French one. Another notable distinction of the French criminal law regime as compared to the German one concerns the possibility for non-governmental entities to start a civil action against – for example – a jamming operation respectively operator.[18] This may be of profound interest for scenarios addressed by DETECTOR, as it allows private operators the use of legal tools to address interference with their own particular road sector services. Also the French regime as it currently stands, however, would benefit from some further clarification as regards the extent to which some of its concepts, such as automated processing systems respectively computer-related crimes,[19] would or may encompass the types of activities DETECTOR is targeting.

Also in Belgium, non-governmental entities such as possibly charged by governments to detect and counteract jamming activities and other wanton interference, under circumstances can ensure themselves that any such activities would become subject to court judgements, possibly at least giving rise to compensation and/or fines.[20] In this sense, Belgium rather resembles France. As compared to Germany, in Belgium the application of seizure to objects implicated in unlawful acts is automatic and quasi-permanent,[21] which would make criminalisation of devices targeted by DETECTOR if substantial suspicions arise of their being used for jamming or other interference so much easier, politically and legally speaking. Such rights of seizure as per the statute even apply in principle to objects not located in Belgium.[22] Another rather straightforward (as compared to France or Germany) feature of Belgium criminal law concerns the clear inclusion of cars in the objects possibly subject to seizure.[23] Also the Belgian criminal law regime has its definitional issues however when it comes to potential applicability to activities such as addressed by DETECTOR. For example, whether 'informatics fraud'[24] would encompass the wilful jamming or other interference with GNSS-based road sector services cannot be answered at this stage by merely referencing the applicable clauses in the Belgian Penal Code. Similar clarifications would be requisite with respect to the concept of 'private communications'.[25] Other than that, it seems interference with privacy is only as such a criminal act if it would give rise to smearing honour or good reputation of a person.[26]

A high-level analysis of the Slovak criminal law system finally does not show major discrepancies as compared to the foregoing analyses of German, French respectively Belgium criminal law systems, albeit that it has its own idiosyncrasies at a lower level, for example pertaining to particular serious felonies as compared to 'more serious' offences (which also results in issues of proper and precise definition, as was seen to be the case in the other three jurisdictions investigated),[27] the rather explicit references to international obligations of Slovakia[28] and the related provisions on extradition and cross-border enforcement of judicial decisions.[29]

As a result of the foregoing evaluation, it is clear that in a number of areas considerable benefits would derive from efforts to establish at the EU level a level of coherence amongst the national

[18] See Art. 1, 2, Code of Criminal Procedure.
[19] See Art. 323, Penal Code, resp. Art. 695, Code of Criminal Procedure.
[20] See Art. 4, Code of Criminal Procedure.
[21] See Art. 43, Penal Code.
[22] See Art. 43ter, Penal Code.
[23] See Art. 46quinquies, Code of Criminal Procedure.
[24] See Art. 504quater, Penal Code.
[25] See Art. 314bis, Penal Code.
[26] See Arts. 443-446, Penal Code.
[27] See Sec. 11, Criminal Code.
[28] See Sec. 7(1), Criminal Code, also Sec. 478, Criminal Procedure Code.
[29] See Secs. 479, 515-516, Criminal Procedure Code.

criminal laws. This then raises the issue of where and to what extent the European Union, in spite of the classical national character of criminal law, has been able to enter that realm.
The gradual transfer of sovereign and semi-sovereign competences in many areas from individual member states to the EU level has hardly resulted so far in any Europeanisation of criminal law. In this area, European integration in legal terms has remained largely confined to efforts to counterbalance the opportunities offered to criminals by the Internal Market and the general deletion of border controls by more opportunities for – still *national* – police and juridical authorities to work together. This has resulted in a Title V within the Treaty on the Functioning of the European Union on an 'Area of Freedom, Security and Justice', focusing very much on cooperation and exchange of information between national judiciary and police authorities and thus, *inter alia*, allowing the Commission to initiative legislative action (and the Court of Justice of the European Union to adjudicate).[30]
This 'Area of Freedom, Security and Justice', while respecting fundamental rights and the different legal systems and traditions of the EU member states, aims to ensure a high level of security through measures to prevent and combat crime, including coordination and cooperation between police and judicial authorities of member states as well as through the mutual recognition of judgments in criminal matters and, if necessary, actual approximation of criminal laws. Especially the latter clause would provide an important underlying legal basis and justification for EU-level legislative efforts in the area of GNSS-based road sector services and any 'harmonised' criminalisation of jamming and other wanton interference activities throughout the Union.
This judicial cooperation shall focus on criminal matters having a cross-border dimension and particularly serious crimes. The cross-border dimension would easily apply to GNSS-based road sector services as addressed by DETECTOR whereas the reference to serious crimes would apply especially once terrorist and similarly serious attacks on GNSS-based road sector services would come to be conducted.
An extended set of clauses of Title V deals with cooperation in regard of the investigation and prosecution of possible crimes with the help of Eurojust. Similarly extended clauses deal with inter-member state police cooperation, and the competence of EU organs to draft legislation in this area, including as necessary involving member state police, customs and other specialised law enforcement services with regard to the prevention, detection and investigation of criminal offences. Also the role of Europol is integrated into this general approach to criminal law issues, including terrorism and forms of crime which affect common interests covered by EU policies. Ultimately, however, the vestiges of national sovereignty in the criminal domain still limit Europol's competences: any operational action must be carried out in liaison and agreement with relevant national authorities, and the application of coercive measures remains the latter's exclusive responsibility. Again, this would lead to the conclusion that it would lie with the individual member states to actually *implement* and *enforce* any prospective EU-wide legislation on the issue, to better serve the ultimate aim of DETECTOR of addressing threats to GNSS-based road sector services.

7. Towards EU-Level Legislative Initiatives Promoting Legal Protection Against Intentional Interference with GNSS-based Road Sector Services

Following this summary analysis, in many instances compliance with the legitimacy requirements of 'subsidiarity' and 'proportionality' for using EU-level competences to undertake EU-level legislative initiatives addressing intentional interference with GNSS-based road sector services and applications could indeed be readily argued.

[30] See Artt. 67-89, Treaty on the Functioning of the European Union.

Firstly, there is a large measure of absence of coherence, transparency and clarity on the national level regarding the extent in which and under which specific set of rules jamming activities and/or jammers are prohibited or conditionally allowed, as has already become clear from the summary analyses of the case studies of Germany, France, Belgium and Slovakia.
Radio-frequency management regimes provide at best for a non-descript general obligation to combat jamming; road-tolling regimes similarly are by and large not geared towards protecting GNSS-based road sector services and appropriately addressing threats to them – especially not when broader terrorist and activist threats have to be countered – and criminal law finally and by contrast may offer *too* many individual legal tools to undertake such combat for any consistency to arise, leaving a number of gaps and complicating overlaps and divergences.
Secondly, the fundamental problem tackled by DETECTOR itself is of an EU-wide nature, logically leading to the assumption that tackling it by legal and regulatory means – whether, strictly speaking, as part of radio-frequency management regimes, road-tolling or criminal law regimes – should indeed logically be something to be coordinated or even handled at an EU level. The GNSS systems (to be) used for road sector services themselves are of European-wide (EGNOS) or even global scope (Galileo, GPS, GLONASS). Any consultation of, and cooperation with, the operators of those systems for maximising the benefits of using their signals and services in the road sector within Europe would thus logically be coordinated or handled by the Commission. Cross-border uses of radio frequencies are also subject to regimes of world-wide respectively EU-wide scope. Furthermore, the road sector services within the Union are equally of an overarching EU character, legally speaking as per the Transport Title of the Treaty on the Functioning of the European Union, in particular the concept of Trans-European Networks.
Whilst moving beyond the existing EU regime on radio-frequency management and the regimes related to (electronic) road tolling to properly tackle the threats DETECTOR is addressing means moving into the realm of general criminal law, the arguments that preventing and combating intentional interference with GNSS-based road sector services, or indeed with any electronic road services, are crucial from a security, safety and economic perspective for the European transport sector and the public at large would justify overriding any hesitation to allow EU organs to enter the realm of legally combating such activities, illegal or to be made illegal.
Thirdly, more in particular with respect to specific existing EU-level legislation and regulation relevant for GNSS-based road sector services and applications, a range of examples have been analysed where the Commission has already exercised relevant competences to ensure EU-wide approaches, obligations and rights, in conformity with the principles of ‘conferral’, ‘subsidiarity’ and/or ‘proportionality’ as discussed above. More comprehensive and intentional interference-targeted EU-level legislative initiatives would merely constitute an extension of such existing EU-level law and regulation, and should therefore not meet with any principled obstacles.
Fourthly and finally, any legislative initiative in the area of combating intentional interference (threats) with GNSS-based road sector services should logically also give rise to further judicial cooperation in civil matters and in criminal matters at an EU level since these are also already being developed at a more generic level. These also apply throughout to any legislative initiatives to be taken under the Transport Title of the Treaty on the Functioning of the European Union, relevant here as DETECTOR addresses road-sector services and applications, as well as to telecommunications, falling under the heading of Trans-European Networks, relevant here as DETECTOR addresses GNSS-based services integrating telecommunications. To that extent, it could encompass also criminal-law and road-tolling elements and aspects of such initiatives.
The above high-level analyses gave rise to a preliminary, broad recommendation to take legislative initiatives at the EU level to ameliorate the current general lack of coherence and effectiveness in the legal realm in terms of the general criminalisation of jammers and jamming. This could include such mechanisms as stricter regulation on the sale, possession and operation

of jamming devices; better enforcement of existing legislation; and raising public awareness that jammers marketed as privacy protection devices can degrade GNSS over much wider areas than advertised and are in fact illegal.

Taking the above into account, legislative efforts at an EU level should start by addressing those issues which are considered less sovereignty-sensitive and less invasive of traditional criminal law regimes. Rather, therefore, than focusing on harmonising criminal law procedures or precisely determining sanctions to be applied, the focus should be in particular on addressing some four key areas where progress could perhaps relatively easily be achieved.

The first area would be that of definitions. It would be already helpful to clearly define the type(s) of intentional electronic interference with GNSS-based road sector services, preferably by including these services in provisions regarding public services of great importance, which is/are to be addressed. In this context, an effort should also be made to define key concepts such as 'intent', 'negligence', 'harmful interference', 'complicity', 'multiple offence' and 'on-going offence'.

The second area would be that of proper and principled criminalisation. It would be adamant to impose, one way or another, an obligation on member states to ensure that intentional interference would indeed be generally, broadly and unequivocally criminalised. Whilst it would not be possible or even appropriate to precisely determine penalties to be imposed for violations of such a regime, it could be envisaged that at least ranges of penalties could be indicated for various levels of transgression, in terms of levels of 'intent', 'negligence' or 'harmful interference' for example. More importantly, the contours of the criminalisation would have to be elaborated in a number of respects to take the distinct features of the environment into account.

The third area concerns evidence. While not further addressed in the present paper, also the issue of evidence is rather fundamental to national systems of criminal procedure, and has been addressed in detail by the DETECTOR legal analyses. Here, at least an EU-level initiative could address the fundamental need to include in such domestic regimes a proper recognition of electronic evidence as that to be gathered for instance using DETECTOR devices and services. In particular if such evidence would be properly calibrated, verified, certified and/or audited, if allowing for scrutiny by both experts if required and opposing parties in the legal proceedings and if issues of privacy and data protection are properly taken care of, explicit reference for example along the lines of French law could be more easily achieved.

The fourth area would consist of practical measures underpinning successful application of the above suggested more legally-defined measures. Here, an EU-level initiative should in particular incorporate development of a central database which would provide national prosecutorial authorities with certified electronic information once a case of jamming would become prosecuted, and would include exchange of information on such occurrences between national authorities.

8. Specific Recommendations to the European Commission

Following the analyses and conclusions presented above – and evaluated, analysed and argued in much greater detail in the DETECTOR project's respective deliverable – it is effectively recommended to the European Commission to start initiating the process to arrive at a Directive, subsidiary a few Directives and/or Decisions, which should:

- Define key terms in the context of intentional interference with GNSS-based services, including road sector services;
- Further to general ITU-framework principles and EU law, in principle outlaw intentional interference with authorised usage of radio frequencies within the European Union, including in

particular such interference with road sector services and applications using such radio frequencies, including but not limited to GNSS-based services and applications;

- Ensure that member states outlaw in principle the production, trading and possession of devices using radio frequencies whose production, trading and possession can be reasonably expected to be used for harmful intentional interference throughout the European Union, unless specific licenses or other exemptions apply, such as required for counter-jamming operations;
- Introduce a proper distinction between interference to be prohibited (jamming properly speaking) and interference to be used as a defensive or countermeasure, notably including Active Signal Cancellation;
- Ensure that interference both for individual private and for broader terrorist or activist motives is appropriately addressed by EU law or, as appropriate, national law;
- Establish a legal framework for handling issues of general responsibility of various key categories of players and particular liability for damage caused by services and applications using radio frequencies as well as by intentional and non-intentional interference with such activities within the European Union;
- Ensure that appropriate opportunities are offered by private operators of GNSS-based services to assert civil claims against jammers;
- List EGNOS and Galileo as critical infrastructure, including protecting ground monitoring stations, uplink stations and command and control facilities such as to be developed further to DETECTOR to include them as appropriate in the scope of protection mechanisms as per the present recommendations;
- Introduce as appropriate distinctions between public and private GNSS-based services, including road sector services;
- Further to existing EU law on radio-frequency management, allow for specific protection measures with respect to frequency bands that are considered particularly vulnerable from the perspective of duly authorized activities or services using radio frequencies;
- Further to existing EU law on radio-frequency management, allow for specific protection measures with respect to operations or technologies which make use of radio frequencies and are considered particularly vulnerable to intentional interference;
- Further to existing EU law on road tolling, develop an EU-wide legal framework for all major road-tolling systems, where for example the maintenance or establishment of such a system for regional/social or environmental purposes would require compliance with EU law on regional/social respectively environmental policies;
- Provide the NRAs with the necessary competences to monitor the application of EU law as recommended in their respective national domains;
- Charge the NRAs with developing on a national level the necessary instruments for combating intentional interference, in line with the aforementioned provisions;
- Mandate the NRAs either to themselves undertake the development of devices and operations which would legally, transparently, comprehensively and effectively combat intentional interference, or to properly mandate other entities to undertake such activities;
- Develop policies and regulations to achieve consistency in electronic data formatting and storage, including the establishment of audit trails, to promote acceptability of such data as evidence in relevant judicial proceedings;
- Ensure a comprehensive archiving system or system of systems of relevant data, properly protected against intrusions and ensuring appropriate levels of access to those data;
- Ensure that all activities further to these recommendations would be conducted in accordance with applicable law EU-wide, such as on human rights, data protection and privacy; and

- Ensure that no EU-law document, national law or regulation interferes with the fundamental principle of technological neutrality.