

Is this email not displaying correctly? [Try the web version](#) or print version.

ISSUE

05

Brussels Diplomat

An Update on Legal Developments for the Diplomatic Community in Brussels

December 2012

In This Issue

[Cyber attacks on embassies and diplomatic law](#)

[Statut de chef d'État et libre circulation dans l'Union européenne](#)



Cyber attacks on embassies and diplomatic law

In 2008 the French Embassy's website in Beijing was subjected to a cyber attack which flooded the site with requests, in effect disabling it. Between 2007 and 2009, at least nine Indian embassies across the globe were reportedly infected by cyber espionage. In 2011 the website of Russian embassy in London was disabled by a denial of service attack. Clearly, cyber attacks on embassies are not merely a hypothetical phenomenon. In recognition of new threats, the Bureau of Diplomatic Security in US Department of State, which has a division devoted to security assistance and

guidance to foreign diplomats in the US, lists cyber security as one of its specialised fields.

Amid news stories of politically-motivated cyber attacks and threats to diplomatic premises across the globe, we look at whether diplomatic law provides any answer to the obligations of a host state in the event of a cyber attack on an embassy. A cyber attack can take many forms, for example the interception and modification of information for espionage purposes, or the disruption of equipment by sabotaging infrastructure like a power grid or communications network. Another common form is a denial-of-service attack, which makes a machine or network unavailable to users, for example by overloading the system with information requests so it becomes very slow or frozen.

Relevant obligations may be those under international criminal law, for example the Council of Europe Convention on Cybercrime 2001, or the 1973 Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons. Furthermore, where a cyber attack can be attributed to a particular state, that state may be held responsible under international law. As it is difficult to attribute a cyber attack to any particular source, however, this field of law will often be redundant.

Diplomatic law takes a different angle, in that it looks at the protective obligations of host states in relation to foreign embassies on their territory, thus avoiding the thorny issue of attribution. As the International Court of Justice affirmed in *United States Diplomatic and Consular Staff in Tehran*, the Vienna Conventions on Diplomatic Relations and Consular Relations are of 'cardinal importance for the maintenance of good relations between States in the interdependent world of today'. A key obligation under the Vienna Convention on Diplomatic Relations is the special duty of the host state to 'take all appropriate steps to protect the premises of the

mission against any intrusion or damage and to prevent any disturbance of the peace of the mission or impairment of its dignity' (Article 22(2), see also Article 31(3), Vienna Convention on Consular Relations).

Host states have an obligation to protect the premises of a mission from a cyber attack causing intrusion or damage to the premises of an embassy, for example one which disables a security system. Less clear is what would be regarded as 'all appropriate steps' taken to protect the embassy. Where an embassy website is hosted by servers in the sending state, the host state may have few means at its disposal to monitor and respond to such threats. Further, most attacks carried out so far against embassy websites have not had serious tangible effects. Nevertheless, a denial of service attack could arguably still be regarded as a 'disturbance of the peace of the mission or impairment of its dignity' within the meaning of Article 22(2).

While recognition of an obligation to actively monitor cyber threats and react to attacks on embassy websites may be some way off, practice may develop which could later crystallise into law. If cyber attacks upon embassies continue and most states see the value in preventing them, providing cyber security could become a key part of complying with host state obligations under the Vienna Conventions.



Statut de chef d'État et libre circulation dans l'Union européenne

Le 16 octobre dernier, la Cour de Justice de l'Union européenne a rendu un arrêt de principe à la suite d'un incident survenu entre la Hongrie et la Slovaquie en août 2009. Les faits sont les suivants : la Slovaquie avait à l'époque interdit au Président hongrois de se rendre sur le territoire slovaque à l'occasion de l'inauguration d'une statue de Saint Etienne, premier roi de Hongrie, cette visite étant jugée inappropriée et pouvant potentiellement troubler l'ordre public au vu de la date choisie et des relations entre les deux pays.

La Slovaquie avait dans un premier temps justifié cette décision en se fondant sur les restrictions possibles à la liberté de circulation des citoyens de l'Union prévues dans la directive 2004/38/CE. Devant la Cour, elle a ensuite déclaré (soutenue en cela par la Commission européenne) que la qualité de chef d'Etat du Président hongrois le distinguait d'un simple citoyen et empêchait que le droit de l'Union puisse supplanter les règles de droit international, y compris celle en vertu de laquelle les Etats se réservent le droit de contrôler l'accès d'un chef d'Etat étranger à leur territoire, que ce chef d'Etat soit ou non un citoyen de l'Union.

La Cour a suivi l'argumentation de la Slovaquie, en affirmant que le statut de chef d'Etat présente une spécificité, découlant du fait qu'il est régi par le droit international, avec la conséquence que les comportements de celui-ci sur le plan international, telle sa présence à l'étranger, relèvent de ce droit, et notamment du droit des relations diplomatiques. La Cour en a conclu que la circonstance qu'un citoyen de l'Union exerce les fonctions de chef d'État est de nature à justifier une limitation, fondée sur le droit international, à l'exercice du

droit de circulation que le droit de l'Union lui confère.

On peut se demander si le principe énoncé par la Cour trouverait également à s'appliquer dans le cas d'une visite à caractère totalement privé et sans portée symbolique du chef d'un Etat membre sur le territoire d'un autre (vacances, visite à un membre de sa famille, etc.).

Par ailleurs, il n'est pas certain que la règle de droit international que la Cour identifie en l'occurrence, à savoir le consentement de l'Etat pour l'accès à son territoire, soit spécifique aux chefs d'Etat. Tout ressortissant étranger y est soumis. Sauf, précisément, dans le cadre de la liberté de circulation dans l'Union européenne. Et cette liberté paraît bénéficier aux chefs des Etats membres, car le droit de l'Union ne les en exclut pas.

You are receiving this newsletter because you
have subscribed to our newsletter.
Not interested anymore?

Lorenz | International Lawyers
Boulevard du Régent 37-40 Regentlaan
1000 Brussels

Phone +32 (0)2 239 2000 | Fax +32 (0)2 239 2002 | E-mail info@lorenz-law.com |

This newsletter does not constitute legal advice. Lorenz accepts no liability for any inaccuracies or omissions in this newsletter. Any decision based on information contained in this newsletter is at the sole responsibility of the reader