

# The Network and Information Security Directive: Opening the Gates of AHN'QIRAJ or Preparing for Battle.net

**Martina Gillen, UWE**

This paper considers the current Directive and attempts to critically access its nature and likely effects using two key critical tools.

1) The battle of the analogy – how best to think about the INS Directive in terms of the wider global discourse in cyber security.
2) The impacts of its provisions.

In simple terms this paper poses the question of whether the EUs actions constitute a potential template for international co-operation and governance in this area – justified by the impact of digital technologies on the internal market and EU citizens (what we will term a co-operative or public health model) or is it in fact in a product of the "war" analogy which creates a state of "cyber preparedness" more properly addressed under the Common Security and Defence Policy. Although not specifically raised by the debates around the directive the author believes this is a strong analytical metaphor for the controversy within the Union institutions during the passage of the Directive. As recorded in the Information on the State of Play dated November 2015

"3. On substance, the main outstanding issue between the two institutions concerns the scope of the proposal. Whereas the Council text would allow Member States to assess, on the basis of defined criteria, whether or not certain operators in identified sectors would be subject to the obligations regarding security requirements and incident notifications in the Directive, the EP envisages an approach whereby all operators in all of the sectors identified are subject to the obligations but with a possible varying degree of providing evidence of effective implementation of security policies. The identification and inclusion of certain sectors, to be listed in an Annex, also remains an open issue, including the question whether Internet enablers should be added to the list, as the Commission advocates.

4. Other outstanding issues concern the architecture, objectives and extent of strategic and operational cooperation and the modalities and criteria for national incident notification and for notification in the EU context."

We will then consider the potential efficacy of the Directive as it now stands in light of our conclusions.

Since the final text of the Directive is not yet known the paper will only tentatively explore the potential impacts but special attention will be paid to some of the more unusual features of the Directive, in particular its applicability to non-EU digital service providers who are deemed to offer services within the Union and the rather unusually prescriptive approach to what constitutes a digital service provider which caused such contention above.

The paper will conclude by considering some of the broader implication of the principles underpinning the Directive for the Union in a wider global context. Essentially we ask if this places Europe on the road to the "open free and secure Internet" envisaged by the Cybersecurity Strategy of the European Union or in a much darker and more troubling direction.