I would like to thank Maeve Dion, Mark Klamberg, Leif Thorsson and the participants in discussions during presentations at Modern International Studies Center (MISC), Dubai, 2012; the International Information Security Research Consortium Meeting, Baku, 2013; the Asian Society of International Law, Delhi, 2013; at Stockholm Center for International Law and Justice, 2014. Errors are mine. Said is, though, responsible for the choice of topic. He induced me to think about cyber intervention in peacetime, when he invited me to address this problem at the MISC in Dubai.


For reasons that will be presented below, I use the unusual expression ‘national cyberspace’. I am aware that it might appear to be a contradiction in terms, and I further do not consider

---

1 I would like to thank Maeve Dion, Mark Klamberg, Leif Thorsson and the participants in discussions during presentations at Modern International Studies Center (MISC), Dubai, 2012; the International Information Security Research Consortium Meeting, Baku, 2013; the Asian Society of International Law, Delhi, 2013; at Stockholm Center for International Law and Justice, 2014. Errors are mine.


4 For reasons that will be presented below, I use the unusual expression ‘national cyberspace’. I am aware that it might appear to be a contradiction in terms, and I further do not consider
That conclusion is arrived at from the point of view of a generalist through the application of existing international law.

Cyberspace and International Law

The definition of a state under international law is a territory and a population represented by an effective government. While all three aspects of the state are important – without a government there cannot be a state, and the reason for the state is the well-being of the population – it is arguably the territory that is the single most important delimiting criterion. The territory effectively determines the population, and the most important demarcation of the government’s legitimate power (its jurisdiction) is the territory. This territorial basis for political governance has been put in question by increased travel, migration and economic exchange, and governments now exercise at least some aspects of jurisdiction over considerable numbers of events abroad.

However, this complication is minor compared to those caused by the Internet. Even though governments are increasingly taking control over their national cyberspaces, and even though the principle of territoriality provides that a state has jurisdiction over servers and nodes within its recognized borders, communication between servers and computers is routed in international webs mostly operated by private networks, which are not controlled by any one government, and many virtual national assets are stored in servers abroad. Business offers, opinions and fraudulent messages sent from one country and stored in a server in another country may effect events in a third

---

5 Although I have concerned myself with cyber issues a few times since 2000, I do not consider myself to be a specialist. I am an international lawyer, and I apply the law to cyberspace just as I would to any other space.


7 They are, however, partly under the control of the US Government. The domain names – like gov.se or gov.az – are controlled by thirteen clusters of domain name servers, ten of which are controlled by various institutions in the United States, including three US government agencies. And the program for the top domains – .se, .ae, etc – is controlled by a US corporation (VeriSign) under an agreement with the US Department of Commerce.