Data Integrity – UNGGE Sidebar Event, Feb 20 2017

Madeline Carr, Cardiff University

Data integrity is already a key concern for global and state security. Military operations, global financial transactions, and a whole range of critical infrastructure with safety implications increasingly rely upon data streams. The consequences of interfering with the integrity of that data make it an increasingly attractive target. In the coming decade, however, the quantity and significance of data is set to grow exponentially as we move into the 'fourth industrial revolution' or the Internet of Things phase.

The Internet of Things can be characterized by three features; the vast increase in data generated and collected, the interoperability of systems and data streams, and the capacity for that data to actuate physical devices with real world effects. The potential for security vulnerabilities in the IoT is quite significant as the scale and scope of data collection combines with the proliferation of insecure devices in a commercial landscape that, as yet, has failed to settle on security standards. We've already seen some tentative, initial probing attacks that seek to harness the power of the Internet of Things – the Mirai attack last year, for example.

Some key questions that have been well established in the previous generation of Internet technology will be heightened in this context; these include issues of responsibility, liability and accountability and when it comes to data integrity, this can be complex.

Although many states have processes in place for securing and controlling data to mitigate against interference, these are often undermined by the international nature of Internet infrastructure, variances in approaches to Internet governance and the global trajectory of data flows. In some cases, there are a number of stakeholders who may claim ownership of data making collaboration and cooperation essential. This is the case for conventional state level issues but in the context of internationally significant data streams, these issues are further exacerbated.

Indeed, states may now need to consider whether some of these data streams are themselves, a form of inter or *transnational critical infrastructure.* Which data streams are becoming (or have already become) essential to the smooth functioning of international society? Again, this is particularly pertinent as we move rapidly into the Internet of Things phase and see the scale and scope of data generated, gathered, redistributed and utilized in complex and compound ways. How will we identify these 'critical information infrastructures' or 'critical data'? I would suggest a sectoral approach would be the first place to begin – perhaps the financial sector, the environmental sector, the insurance sector or the aviation sector.

The second question that this idea of 'international critical infrastructure' or 'international critical data' raises is how to protect it and when we talk of protecting

data – as Eneken has pointed out, one fundamental protection involves ensuring its integrity. While the private sector will certainly have a key role to play in many contexts, a purely commercial, market driven approach to guarantees of data integrity would be unsatisfactory - even if such a guarantee could be established among the myriad of actors with a vested stake in valuable and global data. The fact that there exist other actors with the capability and intent to manipulate data who fall outside of the commercial sector leaves the problem of data integrity as a challenge for states.

For state based approaches that recognize this as a global security challenge, we may look to the OSCE CBM adopted in 2013 in which we agreed that states will '…protect critical national and international ICT infrastructures including their integrity'. If we recognize some data streams as 'critical international infrastructure' then the expectation that states work to protect their integrity may already be regarded as in place. Indeed, without being able to ensure data integrity of critical systems (and that may include critical data), states must reconsider their responsibility in creating dependence on these critical data flows. Responsibility here (if we consider some data to be critical international infrastructure) is not only internal responsibility to a state's civil society but external responsibility as we increasingly participate in generating and using data for processes essential to the smooth functioning of international society.

This raises the prospect of the value of, or potential for, a more clearly articulated agreement that responsible state behavior does not allow for the manipulation of 'critical data'. Data integrity is and increasingly will be fundamental to some aspects of global security. Existing international law will already provide for the protection of critical data to some extent. Where this is the case, it needs to be clearly outlined and understood. If there are found to be gaps in the interpretation or application of international law, establishing new (or recognizing existing) norms around the protection of critical data will be in the best interests of all actors.