Is Law Losing Cyberspace?

by Duncan Hollis

The **ALL CAPS headline** of the last few hours involves news that social security and other identifying information for some 4 million U.S. federal workers was compromised in a cyber exploitation that, if one believes the unofficial finger pointing, came at the behest of the Chinese government. Of course, it was just yesterday, that the Council on Foreign Relations' Adam Segal was reporting how China was crying foul over **"OceanLotus"** a cyber exploitation that counted various Chinese governmental agencies and research institutes among its victims (and where the fingers were pointed back at the United States). And that's to say nothing of the Snowden disclosures or the tens of millions of people whose personal data has been compromised via data breaches of an ever-expanding list of private companies (e.g., in February 2015 the U.S. health insurer **Anthem** admitted that up to 80 million people in its databases had their personal data compromised). Now, maybe such data breach stories are hyperbolic, offering big numbers of potential losses that do not necessarily mean actual data compromises, let alone consequences for the associated individuals. Nonetheless, the current zeitgeist seems to be the normalization of cyber insecurity.

As someone who believes international law has an (imperfect) role to play in preserving international peace and stability, I find the current scenario increasingly worrisome. The level and breadth of cyber exploitations suggests a world in which actors are engaged in a race to the bottom of every data well they think might be useful for their own purposes, on the theory that their adversaries (and their allies) are all doing the same. In such a world, law seems to be playing a diminishing role.

To be clear, domestic law certainly may constrain (or facilitate) a State's cyber operations, as all the anxiety associated with the expiration of the PATRIOT Act and this week's passage of the **USA FREEDOM Act** suggest. For those of us who care about international law, however, it seems increasingly marginalized in the current environment. We've spent much of the last several years, focused on *how* international law applies to cyber-operations with huge efforts devoted to questions of line-drawing in what constitutes a prohibited use of force in cyberspace under the *jus ad bellum* or where the lines are for an attack under the *jus in bello*. **The Tallinn Manual** is the paradigmatic example of this (often quite good) work. More recently, States and scholars have moved on to cyber operations below these lines, with attention shifting in **Tallinn and elsewhere** to which cyber operations may generate counter-measures and defining when cyber operations violate the duty of non-intervention.

Such efforts have (so far) had relatively little to say on the question of a cyber exploitation that is best characterized as espionage. With the exception of **U.S. efforts to decry "economic" cyber espionage** (as opposed to national security cyber espionage), most international lawyers have shrugged their shoulders on the legality of governments (or their proxies) stealing data from other governments or their nationals. The conventional wisdom suggests intelligence agencies will be intelligence agencies and we should let this play out via diplomacy or power politics. To the extent international law has long failed to prohibit espionage, the thinking goes, by analogy it should also leave cyber espionage alone. And if that's true, international law has little to say about China taking whatever data it can on employees of the U.S. federal government.

Of course, conventional wisdom is often conventional for good reasons. From a national security perspective, there are important interests that militate against regulating or constraining data collection from abroad. Yet, I worry that we're reaching a tipping point where in conceding international law can do little to nothing for the problem of cyber exploitations, we are effectively conceding the rule of law in cyberspace. It's understandable that, from a rational perspective, States will want to do as much of this activity as their technical capacity allows. But, such self-centered policies have generated a dramatic collective action problem. The current cyber system is certainly sub-optimal, whether you consider it in economic, humanitarian, or national security terms. The economic costs of the status quo are by all accounts growing, whether in terms of losses of data and IP, or the costs of cleaning up after exploits occur. Similarly, the ability of individuals to preserve their privacy is rapidly diminishing, and the right to privacy along with it. And, of course, national governments are fighting, and losing, the battle to keep their own data (and secrets) secure.

All of this leads me to ask whether it's time to revisit the question of how international law deals with data breaches? I recognize some may say "no" or that after long and careful thought the answer may remain the same. But, the rising importance and success rates of data breaches across the globe suggests it's high time for international law to at least engage these questions more closely.

What do others think? Is international law losing in cyberspace or is there still a chance that it can play a regulatory role over modern cyberthreats, even if only an imperfect one?

June 4th, 2015 - 10:48 PM EDT | **Trackback Link** |
http://opiniojuris.org/2015/06/04/is-law-losing-cyberspace/

One Response

> Given how ineffectual international law appears at punishing genuine abuses by powerful nations I find it very difficult to imagine a regime that could both actually get adopted and also do anything useful in this arena. Cyber espionage doesn't necessarily even have the messy problem of having to sneak people into the target nation, and so it becomes even more a matter of information defense rather than any chance at capture and trade.

6.05.2015
at 12:47 am EST

Soronel Haetir

Trackbacks and Pingbacks

There are no trackbacks or pingbacks associated with this post at this time.