File 20100310.0657: Notes from reading group this morning:

I told people about the paper by [1] and that it's very funny. I suggested [2] on homomorphic encryption for next week.

[Shamal] A strong feeling of *déjà vu*: I have been in meetings also where a group of practitioners get depressed because they realise that the problem, while very real, is not in scope and it's not in anybody else's scope either: it feels like it's unsolvable.

[Joe] (an earlier attempt to argue that the current state of development of cyber warfare is at a similar place now to where the new technologies of cannons and long-range ships were in the 1400s): countries experimenting with these new weapons would try them out on their neighbours in small and plausibly deniable engagements, testing the limits of new capabilities and learning what tactics and strategies seemed most applicable.

[Joe] Perhaps much more important than cyber warfare are cyber criminals; going back to my earlier historical analogy, are the cyber criminals of today equivalent to privateers of the 18th century [Shamal: letters of marque]? Much more devastating than shutting down a country's web sites for a few days, or even masking a particular sector of their air defence radar for a few critical hours, would be to transfer a few hundred billion dollars out of their economy, with all the right audit records left in place to make it extremely hard to undo. That is not unlike what Spain and England did to one another on the high seas in the 1700s, by intercepting shiploads of gold or silver bullion and preventing them getting to their destinations.

[Dr Martin: global payment networks]

[Joe] And if you can't transfer the money, just evaporate it and cause a hole in the victim's economy. Economic warfare?

References

[1] Al Bessey, Ken Block, Ben Chelf, Andy Chou, Bryan Fulton, Seth Hallem, Charles Henri-Gros, Asya Kamsky, Scott McPeak, and Dawson Engler. A few billion lines of code later: Using static analysis to find bugs in the real world. *Comm. ACM*, 53(2):66–75, February 2010.

[2] Craig Gentry. Computing arbitrary functions of encrypted data. *Comm. ACM*, 53(3):97–105, March 2010.