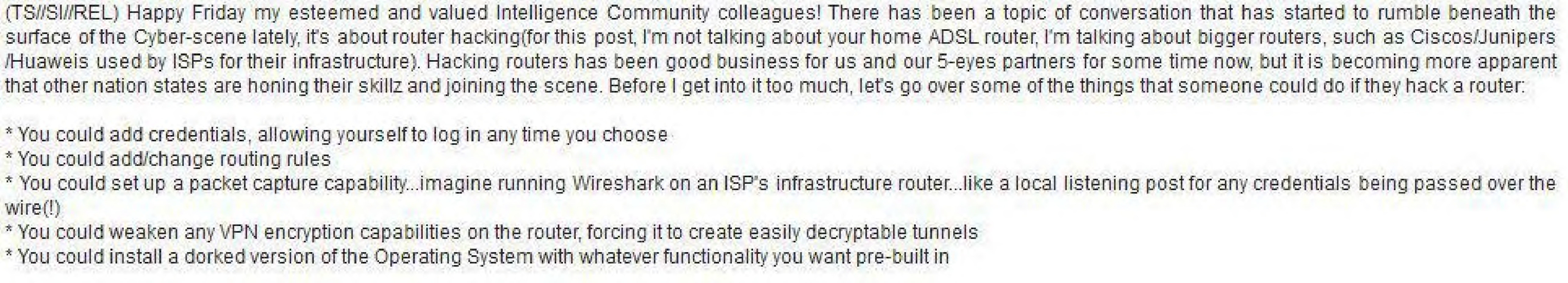

(TS//SI//REL) Happy Friday my esteemed and valued Intelligence Community colleagues! There has been a topic of conversation that has started to rumble beneath the surface of the Cyber-scene lately, it's about router hacking(for this post, I'm not talking about your home ADSL router, I'm talking about bigger routers, such as Ciscos/Junipers /Huaweis used by ISPs for their infrastructure). Hacking routers has been good business for us and our 5-eyes partners for some time now, but it is becoming more apparent that other nation states are honing their skillz and joining the scene. Before I get into it too much, let's go over some of the things that someone could do if they hack a router:

* You could add credentials, allowing yourself to log in any time you choose
* You could add/change routing rules
* You could set up a packet capture capability...imagine running Wireshark on an ISP's infrastructure router...like a local listening post for any credentials being passed over the wire(!)
* You could weaken any VPN encryption capabilities on the router, forcing it to create easily decryptable tunnels
* You could install a dorked version of the Operating System with whatever functionality you want pre-built in