Issued 6/6/18

A War in Cyberspace is Already Raging and could Lead to Armageddon if Banks get Hit

A war is being fought in cyberspace with “ones and zeros” instead of bullets and too-big-to-fail banks are major targets, experts with cyber security and intelligence backgrounds have told Business Insider. US and European authorities are concerned about a possible “armageddon” event caused by a successful cyber attack on western banks and other critical areas of infrastructure by hostile nation-states and other actors. A successfully coordinated attack on a too-big-to-fail bank could have “cataclysmic” consequences for the global financial system and deal significant damage to the national security of the west, experts said. Major threats originate from groups like hackers, hacktivists, organized criminals, terrorists and nation states like Russia and China, but attribution is notoriously difficult in the cyber world. Dr Victor Madeira, a senior fellow at the Institute for Statecraft, and former strategic advisor on national security reform said that Russia and China have been aggressively developing and using their cyber capabilities against the west. “The true battleground is usually the boardroom, it’s not the battlefield,” said Madeira. “Russia and China would look to undermine or even outright paralyze the international financial system if push came to shove. That’s really what’s underpinning a lot of this, it’s economic and financial competition, and two very different and competing worldviews, as to what those systems should be,” he added. There has also been concern in the west surrounding the use of Russian and Chinese electric equipment such as phones and routers which could potentially compromise national security. Chinese company ZTE was accused in

a US court of being used solely to spy on other countries, and Britain's GCHQ is currently analyzing the dangers of allowing Huawei's products to be used across the UK's digital infrastructure. According to Statista the value of cyber insurance worldwide has increased by around $2.8 billion since 2014 and is projected to inflate by another 2 billion by 2020. The consequences of weak cyber defenses in critical infrastructure like water, wastewater, energy transport and financial services are severe if there's a breach. "If you're not securing your life support sectors from a cyber attack, cyber security becomes real in a very different way. It's no longer about stolen data and passwords or health information. It's about not being able to feed your family or go to work or turn the lights on, and we want avoid that kind of armageddon scenario," said Tom Finan, WTW cyber strategy lead in the US, and a former senior cyber strategist at the Department of Homeland Security. Banks are particularly vulnerable to attack because of the speed that trades are made, the amount of cash and data they hold, and the extreme sensitivity of financial markets. As corporate spending on cyber defense has increased the dominant threat now comes from "insiders" who are employees or other trusted parties that either negligently or purposefully use privileged access to breach an organization's cyber defenses. Security of the banks is treated as national security issue because "economic security is national security," said Finan. That's why the US Department of Homeland Security is responsible for protecting 16 pillars of critical infrastructure which includes water, energy, transport and finance.