Obama declares “national emergency” based on alleged cyber threats from Russia, China

Thomas Gaist
3 April 2015

In yet another escalation of the drive by the US ruling class to establish unconstrained control over the world’s information networks, US President Barack Obama issued an executive order Wednesday declaring a “national emergency” over cyber attacks on US targets. The order authorizes economic sanctions and the seizure of financial assets and other forms of property from any entity considered a “security risk.”

Obama’s six-page order, “Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,” warns that the sweeping powers, are necessary to combat an “unusual and extraordinary threat to national security” stemming from cyberattacks against US infrastructure. The order also asserts new powers to impose travel restrictions against alleged security threats, which can be exercised against any “partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.”

The executive order also authorizes the US secretary of the treasury to impose financial sanctions on foreign entities accused of hacking American computer systems, clearing the way for escalated confrontation with the Russian, Chinese and Iranian governments, all of which US officials now regularly accuse of sponsoring hacking operations against Western banks and corporations.

The legislation “will give us a new and powerful way to go after the worst of the worst,” Obama wrote in an online post. In a strong indication that the order will be used as the pseudo-legal basis for new sanctions and other provocations against US rivals, Obama directly accused Russian and Chinese hackers of launching cyber attacks on American troops.

“The same technologies that keep our military strong are used by hackers in China and Russia to target our defense contractors and systems that support our troops. Networks that control much of our critical infrastructure—including our financial systems and power grids—are probed for vulnerabilities by foreign government and criminals,” Obama wrote.

“Our primary focus will be on cyber threats from overseas,” Obama wrote, vowing that the White House would move aggressively to ensure that full use is made of the expanded cyberpolicing powers.

Obama also boasted about his administration’s efforts to expand direct data sharing between corporations and the government. The US government is “working to improve our ability to quickly integrate and share intelligence about cyber threats across government and with our foreign partners” and “working to share more information about threats and solutions with industry,” he wrote.

The supposed threat of cyber attacks against US companies and infrastructure is a major component of US war propaganda aimed at preparing public opinion for war with a number of targets, above all China and Russia.

Following the lead of the Federal Bureau of Investigation (FBI), the US media and political establishment hyped accusations beginning in November that North Korea had launched a cyberattack on Sony Pictures. The US government subsequently imposed sanctions against North Korean officials supposedly involved in the attack.

Wednesday’s decree grants broadly defined emergency powers to the Treasury Department modeled on those give to the “counterterrorism” agencies in the wake of 9/11.

The order gives the government “a powerful new tool” against “those who would exploit the free, open, and global nature of the Internet to cause harm,”

according to Treasury Secretary Jacob Lew, and will enable the Treasury to project power against overseas US cyber-adversaries, according to John Smith of the US Office of Foreign Assets Control.

The US government requires “the full range of tools across the spectrum in order to actually confront the cyber threats that we face,” White House cybersecurity chief Michael Daniel told reporters Wednesday.

Claims of the US government to be defending legality are laughable. US cyber operations systematically violate democratic protections established in the Bill of Rights against arbitrary searches and seizures. The FBI has aggressively sought changes to Rule 41 of the Federal Rules of Criminal Procedure which would dramatically loosen Fourth Amendment-based warranting requirements for electronic hacking operations by the government, and effectively enable agents to implant malware on any computer they choose, without asking a judge for specific authorization.

As a result of programs initiated under the Bush administration and expanded under Obama, the National Security Agency and other federal bureaucracies already enjoy virtually complete access to data stored on the servers of the major telecommunications providers. FBI Director James Comey insisted in appearances last year that major cellphone providers grant back doors into their security systems to ensure that US agents free access to cellular data of US smart phone users. Obama has presided over the expansion of programs run by the NSA and FBI to collect, analyze and share personal data from the general population in vast quantities.

Rather than a concern for security, the Obama administration’s cyber-emergency decree is part of efforts by the US government to establish essentially limitless powers for its intelligence agencies to spy on and hack rival governments and working people around the world.

Numerous experts have warned that complex malware technology deployed by US agencies is accelerating the spread and evolution of weaponized software. Extensive purchasing by the US government of “zero day” hacking “exploits,” programs specially tailored to exploit previously unknown vulnerabilities in widely used software platforms, has fueled the growth of markets for new offensive hacking techs and other pathological forms of software.