GlobalResearch
Center for Research on Globalization

US and its Allies Trying to Establish Total Control Over Internet Users: NSA's SIM Card Scandal Bigger Than You Think

By Vladimir Platov
Global Research, February 23, 2015
New Eastern Outlook 22 February 2015

Theme: Intelligence, Police State & Civil Rights

Stolen encryption keys are just the beginning. US NSA appears to have compromised big telecom, IT manufacturers, online banking, and even passports, starting on the factory floor.

Recent days have been marked by a record number of news stories regarding the US and its allies trying to establish total control over Internet users.

On February 16, researchers at the Moscow-based security group Kaspersky Lab announced the discovery of the ultimate virus which has virtually infected all spheres of military and civilian computing in more than 40 countries around the world. They've managed to discover a piece of malware that must have been installed on hard disks while they were still being manufactured, and due to its complexity and a certain number of features that it shares with Stuxnet, it's safe to assume that it was created by US secret services.

On February 18, The Guardian confirmed that for the last 7 years Government Communications Headquarters (GCHQ) had been sharing personal intelligence data *en masse* with America's national security agencies, regardless of the fact that it had intercepted millions of foreign citizens' conversations. The ruling of a UK court clearly suggests that these actions were illegal on top of being carried out in violation of the the European Convention on Human Rights.

On February 19, it was announced that the National Security Agency (NSA) along with its British partner in crime, GCHQ, has manged to steal encryption keys from Gemalto – the world's largest manufacturer of SIM-cards. This allowed the above-named intelligence agencies to tap any phone and intercept data from any mobile device that was using a SIM-card produced by Gemalto. This conspiracy was unveiled by The Intercept, which added that Gemalto was created nine years ago when the French company Axalto merged with Gemplus International which was operating in Luxembourg. Today Gemalto has more that 85 offices across the globe along with a total of 40 factories, working in close cooperation with leading telecommunication corporations, including AT&T, Verizon and T-Mobile, along with many others. Representatives of the three aforementioned companies refused to comment on this scandal.

One can easily count German Deutsche Telekom among the customers of the Gemalto group. Hence there is little doubt regarding the involvement of US intelligence in the tapping of Angela Merkel's mobile phone, an incident uncovered back in mid 2014. What is particularly peculiar in this situation is the decision of The Federal Attorney General of

Germany ending the investigation of the Chancellor's tapped phone – as reported by Focus Online – on the pretext of "zero possible outcome of the investigation." Well, the claims of the same Focus Online that "Merkel now has a new cell phone that cannot be tapped," looks ridiculous enough, since this "new phone" uses the same-old Gemalto SIM-card. So the NSA can spy on Madam Chancellor as long as they see fit, while the attorney general sees nothing wrong about it. Well, perhaps Germany has finally agreed to stand in line with the citizens of other countries and their political and business elite, eager to play the role of laboratory rats in the US intelligence surveillance game.

One would be surprised to learn that Gemalto is producing up to 2 billion SIM-cards per year, along with chips for bank cards and identity cards. According to many information security experts, US intelligence agencies – due to the encryption keys they've stolen – are able to retrieve any information from mobile devices, bank cards, and/or e-passports.

The Wall Street Journal reported the "successes" of US intelligence agencies in retrieving information from millions of US citizens' cell phones back in 2014. Most of America's citizens are under constant watch of US security, due to surveillance systems mounted on light aircraft and drones developed by Boeing, which allows them to collect private data from thousands of mobile phones. In addition to the ability to establish the whereabouts of a person, which can be tracked with the accuracy to within three meters, a phone can be remotely blocked, while all information stored on it can be easily stolen.

On February 20, the spokesperson for the United States Department of State Jen Psaki in her typical manner complained about how difficult it is for the US to confront thousands of hostile attacks in cyberspace. However, she has never mentioned the above-listed facts and Washington's paranoid desire to dominate cyberspace.

Vladimir Platov, an expert on the Middle East, exclusively for the online magazine "New Eastern Outlook"
