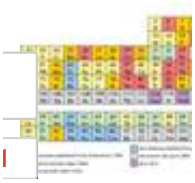
Automakers urge Congress to limit regulation on 'Internet of Cars'



Strontium hacking team targets NATO members, political advisors

Georgia office leaks data on six million voters

November 2015 Issue

Editorial

Pushing past shock and yawn

Threat of the month

Threat of the Month, November 2015

Subscribe

Next Article in News

Archive

Jeremy Seth Davis, Senior Reporter
Follow @heyjsd

December 18, 2015

Adobe update addresses security issues discovered in ColdFusio

Cybersecurity after the Paris attacks: Info-sharing in the spotlight

The U.S. expanded intelligence sharing with France in the wake of the attacks in Paris last week. Speaking at the Group of 20 Summit in Antayla, Turkey, President Obama announced the initiative to streamline information-sharing with France. Israel took similar measures: on Saturday, Israeli Prime Minister Benjamin Netanyahu ordered Israeli intelligence forces to assist France.

The U.S. expanded intelligence sharing with France following the attacks in Paris last week, as intelligence agencies use the attacks to push for expanded surveillance measures.

Meanwhile, intelligence agencies are using the Paris attacks to push for expanded surveillance measures. Yesterday, CIA director John Brennan said he thinks "this is a time for particularly Europe, as well as here in the United States, for us to take a look and see whether or not there have been some inadvertent or intentional gaps that have been created in the ability of intelligence and security services to protect the people that they are asked to serve."

However, France passed a surveillance law in June that already provides the government with the broad surveillance powers that Brennan seems to be advocating for. The "Intelligence Bill," adopted in response to the Charlie Hebdo massacre in January, allows French authorities to monitor mobile phone, email, and Internet communications of people suspected of connections to terrorist groups without judicial authorization.

Dyadic Security co-founder and chief scientist Yehuda Lindell told SCMagazine.com there are "many things would make the job easier for law enforcement agencies," including an ability to walk into anyone's house at any time or search any car with or without cause.

The U.K.'s GCHQ Chancellor George Osborne said the spy agency's budget will double, investing £1.9 billion to hire 1,900 new spies and expand cyber capabilities. He said, "To those who believe cyber-attacks can be done with impunity, I say that impunity no longer exists." He warned that ISIS is trying to launch cyber-attacks on airports, hospitals and on the National Grid.

A federal appeals court in Washington, D.C., denied a federal judge's attempt to immediately halt the NSA's bulk collection of Americans' phone records. The bulk collection program is set to expire at the end of the month.

However, on Tuesday Sen. Tom Cotton (R-Ark.) introduced legislation to delay the expiration of the controversial surveillance program. "The terrorist attacks in Paris last week are a terrible reminder of the threats we face every day," he said, in a release. "Now is not the time to sacrifice our national security for political talking points. We should allow the Intelligence Community to do their job and provide them with the tools they need to keep us safe."

This is not a new argument. In July, FBI chief James Comey requested back doors to tech companies' encrypted information to allow law enforcement agencies to more successfully monitor ISIS and other criminal groups.

However, the growing trend toward international cybersecurity cooperation increases the risk that information collected by intelligence agencies will end up in the wrong hands. The U.S. has feverishly pursued international cyber alliances. In addition to the U.S.' information-sharing agreement with France, the U.S. signed agreements to cooperate on cybersecurity with Cuba, South Korea, Japan, and Israel. The U.S. and China signed an agreement not to engage in cybertheft of intellectual property.

Lindell called the argument that private companies must provide access to unencrypted information to law enforcement and intelligence agencies "a joke," since terrorists already encrypt their communication.

"So you end up in a situation where the criminals encrypt their information and all of the rest of us do not," he added.

1