FUTURE
for Advanced Research & Studies

Artical Name : Cyber Espionage

Artical Subject : Why would countries think of building national cyber networks?

Publish Date: 14/04/2015

Auther Name: Dr. Ehab Khalifa

Subject :

A number of countries revealed their intention of setting up national internet and telecommunications networks in the near future. This declaration came in the wake of the full-scale cyber espionage operations, carried out by the US, whether against enemies or allies. It was also due to the mounting cyber-attacks on critical infrastructure, along with the concerns about the infiltration of military networks.First: US Cyber-espionage against Information and Telecommunication NetworksThe documents leaked by the former US National Security Agency (NSA) contractor, Edward Snowden, revealed US espionage against several countries. It also showed how US collects phone calls and mail correspondences of the majority of leaders and politicians through a surveillance program called "PRISM", under the pretext of fighting terrorism. The "Washington Post" pointed out that there is a confidential, legal license, dating back to 2010, along with some other documents, confirming such leaks. They proved NSA's extensive powers and flexible ways of monitoring, not only communications belonging to its targets abroad but also any communications related to those targets. Such leaks caused many diplomatic crises for the US, especially with its allies, like Germany, France, and Brazil. This infuriated the leaders of the countries that were the victims of the American cyber espionage.In this regard, the German magazine, "Der Spiegel", mentioned that it obtained some documents about NSA's intercepting Chancellor Angela Merkel's phone calls since 2002. Consequently, the German Foreign Minister, Guido Westerwelle, summoned the American ambassador for the first time in the history of both countries, since World War II. The former demanded an explanation for the allegation that the US intelligence agency had tapped Merkel's cell phone. Thus, US president, Barack Obama, apologized to the German Chancellor, stressing that he had no idea about such espionage; otherwise, he would have stopped it.Similarly, the French Foreign Minister, Laurent Fabius, summoned the US ambassador in Paris to discuss a report published by the French paper "Le Monde". The report claimed that the US intercepted millions of private phone calls of French citizens. Some other press reports mentioned that NSA had spied on French diplomats in Washington and the UN, too.The British newspaper, "The Guardian", also released a report about Edward Snowden's leaking confidential documents to the American journalist, Glenn Greenwald, who lives in "Rio de Janeiro" and works as a columnist for The Guardian. The report revealed that NSA intercepted the phone calls of the Brazilian president, Dilma Rousseff, as well as the emails she exchanged with her advisors and ministers. As a consequence, Rousseff canceled her visit to the US, which was scheduled for October 23, 2012. Not only that, but she also criticized US cyber espionage against her country and against her at the opening session of the UN General Assembly, in the presence of the US president. Brazil's negotiations with the US on a 4-billion-euro fighter jets contract were suspended, too.The US president tried to defend his government, pointing out that the effectiveness of the American spying program is the reason why "the world is more stable now than it was five years ago". The US administration also justified the espionage operations, saying that they were intended to detect any terrorist attack before it happens.Second: The Rise of Global Trends in Internet LocalizationThe aforementioned incidents raised angry reactions from the side of the US allies on the official level. That prompted some countries to suggest setting up a European telecommunication network, separate from the regular internet. That network would prevent data and information from being transferred across the US, thus protecting them from falling into the hands of US intelligence services. The European Union (EU) and BRICS were the most prominent powers that favored this suggestion. This is illustrated by the following.1- The EU: During her meeting with the French president, Francois Hollande, the German Chancellor, Angela Merkel, highlighted the importance of building a European telecommunication network for transferring data, information, and communications. The purpose of establishing such a network is to avoid using the American networks and servers, and thus, such data will not fall into the hands of any agency (such as NSA) that might spy on, and infiltrate, this data. The suggestion was widely approved by the EU member states.In this regard, the German government launched a campaign in 2013, called "E-mail Made in Germany", through German state companies, such as Deutsche Telekom and GMXweb.de. In April 2014, EU legislators voted in favor of having strict rules for net neutrality. This would be achieved through availing equal opportunities for all companies, without favoring one over the rest. This came under the reforms of the European telecommunication sector that were proposed by the European Commission, in order to support the former to compete with its American and Asian counterparts.In November 2014 in Strasbourg, France, the European parliament voted on a resolution, ordering search engines to separate their search services from their other services. The lawmakers overwhelmingly approved the resolution, with 384 votes for and 174 against it. This resolution targeted Google Inc. which dominates over 90% of the search engine market share in some European countries. This resolution is not only symbolic and non-binding, but it is also unrealistic, given the weak competition between Google and other companies. However, it is still a sign of EU's disapproval of Google's dominance over the search engine market in Europe. It also reflects a subtle desire to encourage the European companies to set up a European search engine, away from the dominance of American Google.2- BRICS: The BRICS countries are planning to build their own cyberspace, which is independent of the current internet, in order to end the American dominance and cyber espionage. They have already taken practical steps, with Brazil building a cable system that can link it with Russia, China, and South Africa. The cable will be 34 thousand kilometers long, linking Vladivostok (in eastern Russia) to Fortalez (in Brazil) via Shantou (in China), Chennai (in India), and Cape Town (in South Africa). This project is also expected to provide internet services for 21 African countries. Thus, a new internet, parallel to the current one, is created. It will be a strong competitor to the US. The BRICS countries are also planning to pass legislations that force the major internet powers, such as "Google", "Facebook", and "Yahoo", to store all data generated by the BRICS locally, so that they are inaccessible by NSA.US criticized proposals of building a European telecommunication network that aims at shielding European information from the US. US authorities warned that such rules could breach international trade laws. In its annual review of telecommunications trade barriers, the office of the US Trade Representative said, "Recent proposals from countries within the European Union to create a Europe-only electronic network, or to create national-only electronic networks, could potentially lead to effective exclusion or discrimination against foreign service suppliers that are directly offering network services, or dependent on them".In the wake of the European Russian dispute due to Russia's annexation of Crimea, Kremlin spokesman, Dmitry Peskov, declared that the authorities are considering measures to protect its internet from potential western sanctions. But he denied Russia's intention to disconnect its cyberspace from the global web. He added that the identity of the main global internet provider is known, and taking his improvised actions into consideration, Russia should contemplate a way to guard its security. The last statement was a clear reference to the US.Third: Referential experiences in controlling the InternetSome countries have taken some proactive measures, building their internet and telecommunication network. Some went over the line while protecting their national cyber security. The internet in China, for example, operates almost like a LAN. Although it can connect to the regular internet, it can easily disconnect and convert to the intranet in the case of cyber-attacks. The Chinese government is already playing the role of the server, and thus, it is responsible for protecting the network.The much controversial internet censorship in China could have some advantages regarding security issues. China uses techniques to filter emails, searching for what is considered to be a promotion for illegal trends. Such techniques can be benefited from as in infrastructure to block any malware, spyware, or phishing. China has embarked on a series of endeavors to install certain software on all computers in the country in order to prevent children from surfing pornography online. However, most experts believe that the purpose of such software is to enable the government to control every computer in China. But there could be other purposes, like blocking western attempts to use websites to raise political turmoil, turning people against their government.As a result, China built the "Great Firewall of China", officially known as the "Golden Shield". It is considered the most advanced technical project in censoring the internet and blocking unwanted websites. On the other hand, China provides its citizens with equivalents for the blocked websites, such as "Baidu" as a search engine, "Youku" for hosting videos, "Weibo" for short tweets, and "Sina Blogs" for blogging.In the same vein, Iran started building a national intranet, separate from the regular internet in 2011. The Iranian Minister of Economic Affairs and Finance, Ali Agha Mohammadi, announced it would be truly a "Halal" internet. He added that it would aim at serving Muslims on the ethical and moral levels. Perhaps the main goal of this kind of internet is to protect Iran's nuclear and critical infrastructure facilities, after being attacked by the computer worm "Stuxnet". Through this network, Iran will not take time separating its intranet from the global network once it receives any cyber-attack. This Halal Internet has other options that make it operate faster than the regular internet.The "Washington Post" got a draft of a report by the Center for Global Communication Studies, University of Pennsylvania. The report states that the research conducted confirmed the presence of copies of websites for Iranian ministries, universities, and businesses, normally functioning on Iran's national network. Hi-tech filtering programs were also found. "Filtering" here means the ability of the Iranian system to completely block whatever on the global network that it doesn't want from its intranet. According to the American report, the Iranian network is based on hi-tech equipment, manufactured by the Chinese communication company "Huawei". This company ensures a high level of global network filtration and accurate surveillance of the Iranians' navigations on both networks.Fourth: Assessing the Feasibility of Closed InternetThe global internet industry (hardware and software) is dominated by most American companies. Google, for example, takes over the search engines market, while Microsoft and Apple monopolize the operation systems sector. These three companies also dominate smartphones operating systems. And even when it comes to the traditional powerful wired and wireless telecommunications, one finds that the American "AT&amp;T" comes in second place (after the Japanese "NNT"). Also, the American "Cisco Systems" ranked first in the field of network equipment. In addition, the global market of social media is dominated by American corporate, too, like Facebook, Twitter, and Google.Add to this the fact that the system of domain names is also controlled by the (ICANN), which indirectly works for the US Department of Commerce. Moreover, most internet companies are registered in the US. Therefore, it can be said that it's currently hard to give up the American role in managing the internet assets completely. This American dominance is due to the lack of a ready substitute, and the weak competition among major American companies and their counterparts in Asia and Europe.With the global tendency to build national networks, whether operating along with or separate from the regular internet, the feasibility of establishing such networks should be studied. Edward Snowden believes that building national networks isolated from the regular internet won't help block NSA cyber espionage. This is due to the fact that NSA does not only share the information it gets with other collaborating intelligence agencies, but it also uses them when there is a common enemy."Stuxnet" can penetrate the internal network of the Iranian nuclear program, and can infect the centrifuge systems, even when they are not connected to the internet. This means that "Stuxnet" can easily spy on closed and military networks when they are offline, too. It happened before in 2008, when the Central Intelligence Agency (CIA) developed new software that penetrates offline computers through radio waves. It functions through installing a small program on the computer via the hard disk. It receives and sends data at the same time (Transceiver) across over 7 miles. In this range, there is a laptop allocated for receiving these waves and sending them to the central station from anywhere on earth. In this way, infiltrating offline devices became possible. Still, the human factor remains necessary in installing the spyware on the computer manually.Concluding Remarks:

Countries' tendency to build their national electronic networks reflects the gap between them and the US, for they cannot secure their citizens' data or their officials' calls against US cyber espionage. The matter exceeded the mere desire to secure one's data to a tendency to abandon the internet and the current telecommunications networks, and moving to new secured ones. This idea is not sound at all, because of the advanced American capabilities in the field of cyber espionage and online information tracking. On the other hand, countries around the world are likely to follow new tracks, the most important of which is forcing private companies to put their servers under the state control. These companies will also be requested to improve the capacities of their servers, adopt surveillence strategies and shield them from any infiltration. In case they rejected such conditions, these companies will be eliminated and forbidden from working in the country for national security reasons. Meanwhile, the state will work on developing national search engines and regional companies that are able to compete with their US counterparts. Nonetheless, the current conflict remains a hi-tech one, for the US (or any other country) may invent new ways of espionage that no national internet can withhold.