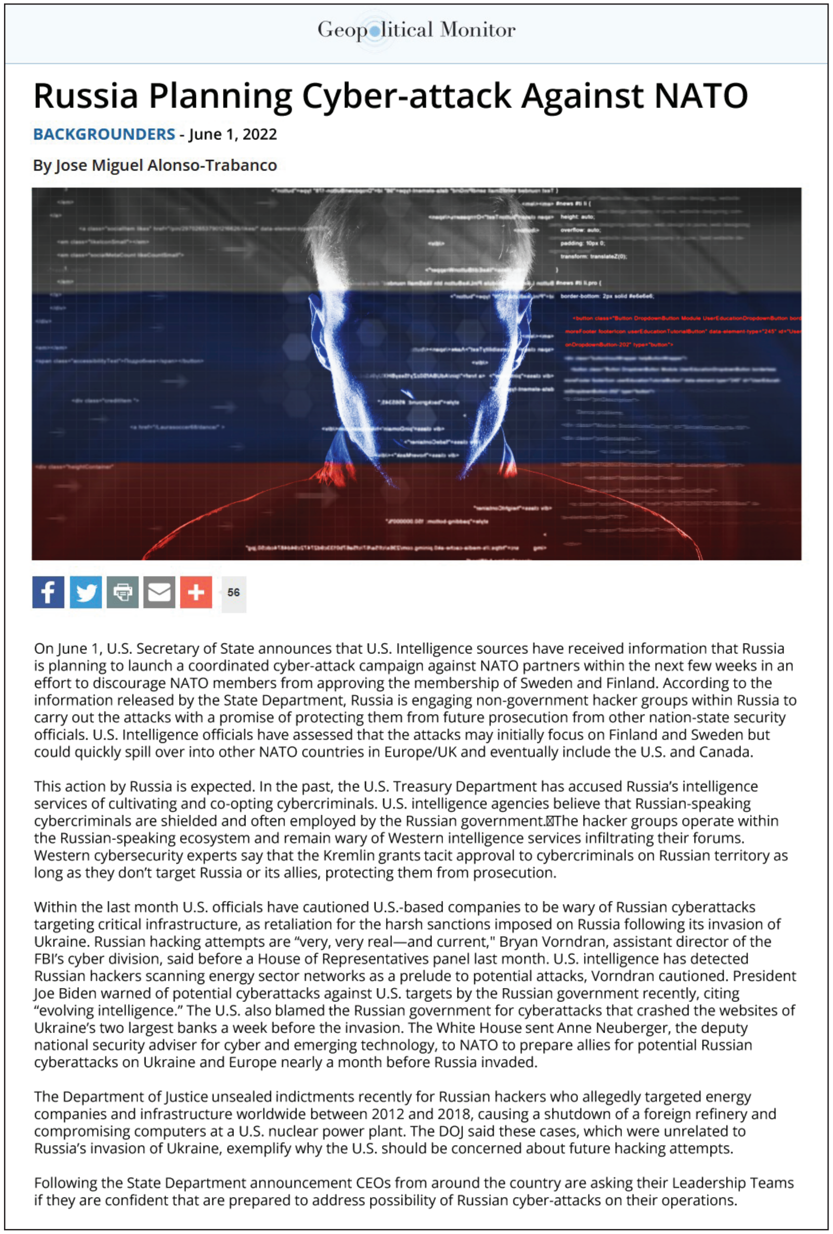
Inject Two

June 1, 2022

PREPAREDEX

BRPW - 2022

Geopolitical News



Geopolitical Monitor

Russia Planning Cyber-attack Against NATO

BACKGROUNDERS - June 1, 2022

By Jose Miguel Alonso-Trabanco

56

On June 1, U.S. Secretary of State announces that U.S. Intelligence sources have received information that Russia is planning to launch a coordinated cyber-attack campaign against NATO partners within the next few weeks in an effort to discourage NATO members from approving the membership of Sweden and Finland. According to the information released by the State Department, Russia is engaging non-government hacker groups within Russia to carry out the attacks with a promise of protecting them from future prosecution from other nation-state security officials. U.S. Intelligence officials have assessed that the attacks may initially focus on Finland and Sweden but could quickly spill over into other NATO countries in Europe/UK and eventually include the U.S. and Canada.

This action by Russia is expected. In the past, the U.S. Treasury Department has accused Russia's intelligence services of cultivating and co-opting cybercriminals. U.S. intelligence agencies believe that Russian-speaking cybercriminals are shielded and often employed by the Russian government.The hacker groups operate within the Russian-speaking ecosystem and remain wary of Western intelligence services infiltrating their forums. Western cybersecurity experts say that the Kremlin grants tacit approval to cybercriminals on Russian territory as long as they don't target Russia or its allies, protecting them from prosecution.

Within the last month U.S. officials have cautioned U.S.-based companies to be wary of Russian cyberattacks targeting critical infrastructure, as retaliation for the harsh sanctions imposed on Russia following its invasion of Ukraine. Russian hacking attempts are "very, very real—and current," Bryan Vorndran, assistant director of the FBI's cyber division, said before a House of Representatives panel last month. U.S. intelligence has detected Russian hackers scanning energy sector networks as a prelude to potential attacks, Vorndran cautioned. President Joe Biden warned of potential cyberattacks against U.S. targets by the Russian government recently, citing "evolving intelligence." The U.S. also blamed the Russian government for cyberattacks that crashed the websites of Ukraine's two largest banks a week before the invasion. The White House sent Anne Neuberger, the deputy national security adviser for cyber and emerging technology, to NATO to prepare allies for potential Russian cyberattacks on Ukraine and Europe nearly a month before Russia invaded.

The Department of Justice unsealed indictments recently for Russian hackers who allegedly targeted energy companies and infrastructure worldwide between 2012 and 2018, causing a shutdown of a foreign refinery and compromising computers at a U.S. nuclear power plant. The DOJ said these cases, which were unrelated to Russia's invasion of Ukraine, exemplify why the U.S. should be concerned about future hacking attempts.

Following the State Department announcement CEOs from around the country are asking their Leadership Teams if they are confident that are prepared to address possibility of Russian cyber-attacks on their operations.

CONTINUED

On June 1, U.S. Secretary of State announces that U.S. Intelligence sources have received information that Russia is planning to launch a coordinated cyber-attack campaign against NATO partners within the next few weeks in an effort to discourage NATO members from approving the membership of Sweden and Finland. According to the information released by the State Department, Russia is engaging non-government hacker groups within Russia to carry out the attacks with a promise of protecting them from future prosecution from other nation-state security officials. U.S. Intelligence officials have assessed that the attacks may initially focus on Finland and Sweden but could quickly spill over into other NATO countries in Europe/UK and eventually include the U.S. and Canada.

This action by Russia is expected. In the past, the U.S. Treasury Department has accused Russia's intelligence services of cultivating and co-opting cybercriminals. U.S. intelligence agencies believe that Russian-speaking cybercriminals are shielded and often employed by the Russian government. The hacker groups operate within the Russian-speaking ecosystem and remain wary of Western intelligence services infiltrating their forums. Western cybersecurity experts say that the Kremlin grants tacit approval to cybercriminals on Russian territory as long as they don't target Russia or its allies, protecting them from prosecution.

Within the last month U.S. officials have cautioned U.S.-based companies to be wary of Russian cyberattacks targeting critical infrastructure, as retaliation for the harsh sanctions imposed on Russia following its invasion of Ukraine. Russian hacking attempts are "very, very real—and current," Bryan Vorndran, assistant director of the FBI's cyber division, said before a House of Representatives panel last month. U.S. intelligence has detected Russian hackers scanning energy sector networks as a prelude to potential attacks, Vorndran cautioned. President Joe Biden warned of potential cyberattacks against U.S. targets by the Russian government recently, citing "evolving intelligence." The U.S. also blamed the Russian government for cyberattacks that crashed the websites of Ukraine's two largest banks a week before the invasion. The White House sent Anne Neuberger, the deputy national security adviser for cyber and emerging technology, to NATO to prepare allies for potential Russian cyberattacks on Ukraine and Europe nearly a month before Russia invaded.

The Department of Justice unsealed indictments recently for Russian hackers who allegedly targeted energy companies and infrastructure worldwide between 2012 and 2018, causing a shutdown of a foreign refinery and compromising computers at a U.S. nuclear power plant. The DOJ said these cases, which were unrelated to Russia's invasion of Ukraine, exemplify why the U.S. should be concerned about future hacking attempts.

Following the State Department announcement CEOs from around the country are asking their Leadership Teams if they are confident that are prepared to address possibility of Russian cyber-attacks on their operations.