GlobalResearch
Center for Research on Globalization

Biden's Retaliatory Cyberattacks Against Russia Are Folly

By Prof. Anatol Lieven
Global Research, March 16, 2021
Responsible Statecraft 11 March 2021

Region: Russia and FSU, USA
Theme: Intelligence

***

The Biden administration is reportedly planning a "retaliation" against Russia in the next three weeks or so for last year's massive "SolarWinds" hack of U.S. cyber infrastructure, for which Russia was allegedly responsible.

The New York Times has written that U.S. plans include both new sanctions against Russia and U.S. cyber hacking of Russian state institutions. According to the Times, this will include "a series of clandestine actions across Russian networks," which U.S. intelligence has already prepared. According to **National Security Adviser Jake Sullivan**, the response is intended to show Russia "what (actions) the United States believes are in bounds, and out of bounds."

We hope that wiser counsels can still prevail, and in particular, that someone in the administration will notice both the logical incompatibility of these two responses, and the fact that they could set a precedent that will be used against America itself in future.

Because, as Sullivan's remarks indicate, the imposition of sanctions implies a belief that state cyber hacking is illegitimate in what the United States calls a "rules-based global order." The threat of U.S. retaliation in kind declares out in the open that the United States also plans to engage in these supposedly illegitimate actions, and is an implicit acknowledgement that Washington has indeed repeatedly engaged in similar actions in recent years.

More importantly, the planned action reflects two very serious errors in judgement, which left unchecked, could increase in scope under the new Biden administration. The first is a tendency, amplified by much of the U.S. media, to attribute blame to Russia for negative developments based on inadequate evidence, which the American public is hardly given a chance to view or assess. Furthermore, there is a proclivity to base U.S. policy on information that may be unclear, exaggerated, or simply untrue.

Concerning the SolarWinds hack, U.S. intelligence services can only say that the Russian state was "most probably" or "very probably" to blame for the hack. The New York Times has reported this as a certainty, but it is in fact extremely difficult to pin down for certain the national origins of such hacks, and even more difficult to determine if they were the work of state forces or independent actors. We may well reasonably assume that Russian

intelligence services were responsible, but action of the kind that the Biden administration is contemplating should be based on something more than probability.

The second error, as I pointed out in Responsible Statecraft on January 13, and as has been argued since in a paper by Major Juliet Skingsley for Chatham House in London, and in Wired by Andy Greenberg, is the use of the phrase "cyberattack," reflecting an extremely dangerous confusion between cyber espionage and cyber sabotage.

Cyber sabotage is like all forms of sabotage: a deliberate attempt to damage public or private infrastructure. If it leads to deaths, then it can well be considered an act of terrorism or of war. This is indeed action that violates all traditional rules of international behavior in peacetime.

Writing about a "Russian cyberattack" against the U.S. Energy Department and Nuclear Security Administration suggests actual damage to those institutions and the infrastructure they control. Among other hysterical political reactions, Democratic Senator Dick Durbin called the SolarWinds hack (which of course he described as a "cyberattack" and attributed unconditionally to Russia) as "virtually a declaration of war." This has been echoed by Senator Chris Coons and others.

No such attack happened. Nor is it at all likely that Russia would carry out such sabotage unless Russia and the United States were already on the edge of war. This suggestion is in keeping with the equally absurd warning last year from NATO officials that in time of peace, Russian submarines might attack undersea communications cables — in the process, by the way, doing great damage to Russia itself, and to Russian partners. This analysis appears to have emanated in the first instance from the British Navy, in an absolutely transparent attempt to save itself from budget cuts. As with most of the SolarWinds allegations, these suggestions involved a confusion —whether careless or deliberate — between espionage and sabotage operations

The SolarWinds hack was an act of espionage by contemporary means. As pointed out in the analysis for Chatham House, an interesting (and amusing) feature of the hack is that if it had not been voluntarily reported to the U.S. government by a private security firm, then — as with all the most successful espionage operations — nobody in America would ever have known that it had happened. Believe me, if Russia ever does decide to attack America, we will know about it.

All states conduct espionage, including most notably the United States itself. Edward Snowden revealed the massive scale of electronic and cyber espionage, not only against Russia and other U.S. rivals but against America's closest allies. In 2015, Wikileaks revealed that for decades, the National Security Agency had been spying on top German government communications, including hacking the phone of German Chancellor Angela Merkel.

Moreover, the United States is a global leader in cyber sabotage. As the Times itself has reported, not only has Washington carried out massive cyberattacks on Iran, it has planted malware in much of Russia's energy infrastructure — though supposedly only to be activated in response to a Russian attack.

Under the new "Defend Forward" cyber-strategy, the Trump administration decided that the United States would itself set out to disrupt any potential cyberattack before it occurred. This is a cyber version of the Bush administration's disastrous Preventive War strategy, and

like that strategy, involves Washington in exactly the sort of aggressive actions that it condemns and seeks to prevent on the part of others.

If the Biden administration does respond to espionage with sabotage it will take national rivalry in cyberspace to a wholly new level of danger, and start a potentially disastrous vicious circle of retaliatory attacks. It will give a green light to all future targets of American cyber-espionage to respond with cyberattacks on the United States.

Furthermore, to retaliate in this way would be a clear break with ancient international conventions and with the longstanding policy of the United States itself. For example in 2014, Russian intelligence was credibly reported to have hacked into the emails of the White House, State and Defense Departments. The Obama administration classified this as traditional espionage and did not retaliate.

The planned response to the SolarWinds hack reflects a much deeper problem in the Washington establishment's attitudes and policy: the belief that the United States can unilaterally set the rules of the international system, and yet set different rules for itself whenever it feels an urgent need to do so. This was never an approach that was going to be accepted by other powerful states. In the area of cybersecurity it makes even less sense, for the internet really is (in many bad ways, alas) a great leveler. To adapt a famous meme: on the internet nobody knows that you are the only superpower.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Featured image: Russian President Vladimir Putin (ID1974/Shutterstock) and President Joe Biden (Stratos Brilakis/shutterstock)

Articles by: **Prof. Anatol Lieven**