The EU’s Response to SolarWinds

cfr.org/blog/eus-response-solarwinds

from Net Politics and Digital and Cyberspace Policy Program

While EU’s issuance of the declaration of solidarity in response to the SolarWinds cyber campaign is a sign of progress, it fails to provide clarification on what, if any, further actions can be expected from Brussels.

European Union flags flutter outside the EU Commission headquarters in Brussels, Belgium. REUTERS/Francois Lenoir/File Photo

Blog Post by Guest Blogger for Net Politics

May 26, 2021 7:35 am (EST)

Julia Schuetze is the Jr Project Director for International Cybersecurity Policy at Stiftung Neue Verantwortung e.V. Arthur de Liedekerke is a cybersecurity analyst with prior experience in the European Union institutions. The views and opinions expressed in this article are solely those of the authors and do not reflect the official position or policy of their employers.

On April 15, the same day that the United States imposed sanctions against Russia for the SolarWinds cyber espionage campaign, election interference, and other issues, the European Union (EU) published a declaration expressing solidarity with the United States. A month later, on May 14, the European Council extended the sanctions regime that guides response to cyber attacks that threaten the EU or its members until May 2022. As part of the EU's cyber diplomacy toolbox, a declaration falls into category three [PDF] of responses—stability measures—which express concern or condemn general cyber trends or certain cyber activities and could have a signaling function. While the EU's issuance of the declaration in response to SolarWinds is a sign of progress, it fails to provide clarification on what, if any, further actions can be expected from Brussels.

More on:

Cybersecurity

European Union

Sanctions

Russia

The declaration still matters because it shows that the EU's response process to malicious cyber activities is maturing. This declaration differs from previous responses due to its coordinated timing with the imposition of U.S. sanctions and reference to Washington's attribution of the campaign to Russia. This contrasts with previous EU responses where attribution was not mentioned explicitly or where member states independently coordinated their attribution efforts multilaterally with third states, avoiding attribution through a unified EU-wide response.

Net Politics

CFR experts investigate the impact of information and communication technologies on security, privacy, and international affairs. *2-4 times weekly.*

View all newsletters >

Digital and Cyberspace Update

Digital and Cyberspace Policy program updates on cybersecurity, digital trade, internet governance, and online privacy. *Bimonthly.*

Daily News Brief

A summary of global news developments with CFR analysis delivered to your inbox each morning. *Most weekdays.*

The World This Week

A weekly digest of the latest from CFR on the biggest foreign policy stories of the week, featuring briefs, opinions, and explainers. *Every Friday.*

Additionally, the language of the EU's recent declaration deviates from prior statements, like those responding to election interference in Georgia and cyber threats targeting the health-care sector during the pandemic. Instead of "condemning" the SolarWinds campaign, the declaration expressed the EU's solidarity with the United States "on the impact of malicious cyber activities."Simply expressing solidarity with the impact in the United States reflects that the European Union does not per se condemn this type of activity. Moreover, it treads carefully when referring to the impact the operation had on the EU and its member states.

This could have been more directly connected to where the EU explains its concern about malicious activities in general that are "affecting the security and integrity of information and communication technology (ICT) products and services, which might have systemic effects and cause significant harm to our society, security and economy." This vague description could be an attempt to show that, from an EU standpoint, the seemingly indiscriminate nature of the SolarWinds breach ("the compromise affected governments and businesses worldwide, including in EU Member States") and apparent disregard for collateral damage ("systemic effects with potential significant harm to our society, security and economy") could result in consequences for the perpetrator. However, by not being more concrete on the damage the campaign had on the EU, falls short of indicating whether those behind it crossed a red line that requires a strong response from the EU. As the rest of the statement focuses on preventative efforts that the EU is already undertaking, the text does not signal that such incidents could be met with a more assertive response, such as restrictive measures. The statement also ignores the fact that two days before the Declaration came out technical evidence seems to suggest that the EU's sanctions regime could be applied. In an answer to a parliamentary question on April 13, European Commissioner for Budget and Administration Johannes Hahn indicated that the EU's computer emergency response team (CERT-EU) had identified cases where IT networks and systems had been **"**significantly impacted" and personal data breaches occurred. "Significant impact" or "potentially significant effect" is one threshold covered in the sanctions regime.

Whether the EU will follow up with sanctions—like the United States—will also likely depend on two things: the collective determination to impose costs despite the risks of retaliation, and on the outcome of further investigation mentioned in the Declaration itself vis-à-vis the other required thresholds for sanctions..

Member states appear ready to act. Unofficial reports indicate that a number of EU member states are toying with the idea of introducing sanctions against Russian citizens who were allegedly involved in the SolarWinds campaign. Also, given the steady deterioration of EU-Russia relations in recent months, member states could be tempted to demonstrate their collective determination to push back against Russia and their commitment to the transatlantic alliance.

More on:

Cybersecurity

European Union

Sanctions

Russia

With the second issue, it's possible that sanctions have not yet been imposed by the EU because its investigation is ongoing. Historically, EU cyber sanctions have been imposed against Russian individuals and entities only after the collection of evidence and attribution by at least two EU member states. Attribution by the United States could be insufficient on its own to warrant such a response. It is also possible that the EU is taking its time to aiming to create a sanctions bundle. Like the United States, the EU has sanctioned different entities for various malicious activities at the same time.

The EU response process is maturing, showing steady improvement in its coordination with third countries. Still, it would have been better if the EU had explicitly described the impact the SolarWinds attack had on EU interests. Such clarity would, if Brussels does eventually follow through with a stronger response such as sanctions, signal that the attacks crossed a threshold. However, considering the time constraint of aligning with the U.S. response and the need for consensus-making in the EU, it is possible that the Declaration was only a first careful response and it will soon follow-up with stronger language and/ or other means.