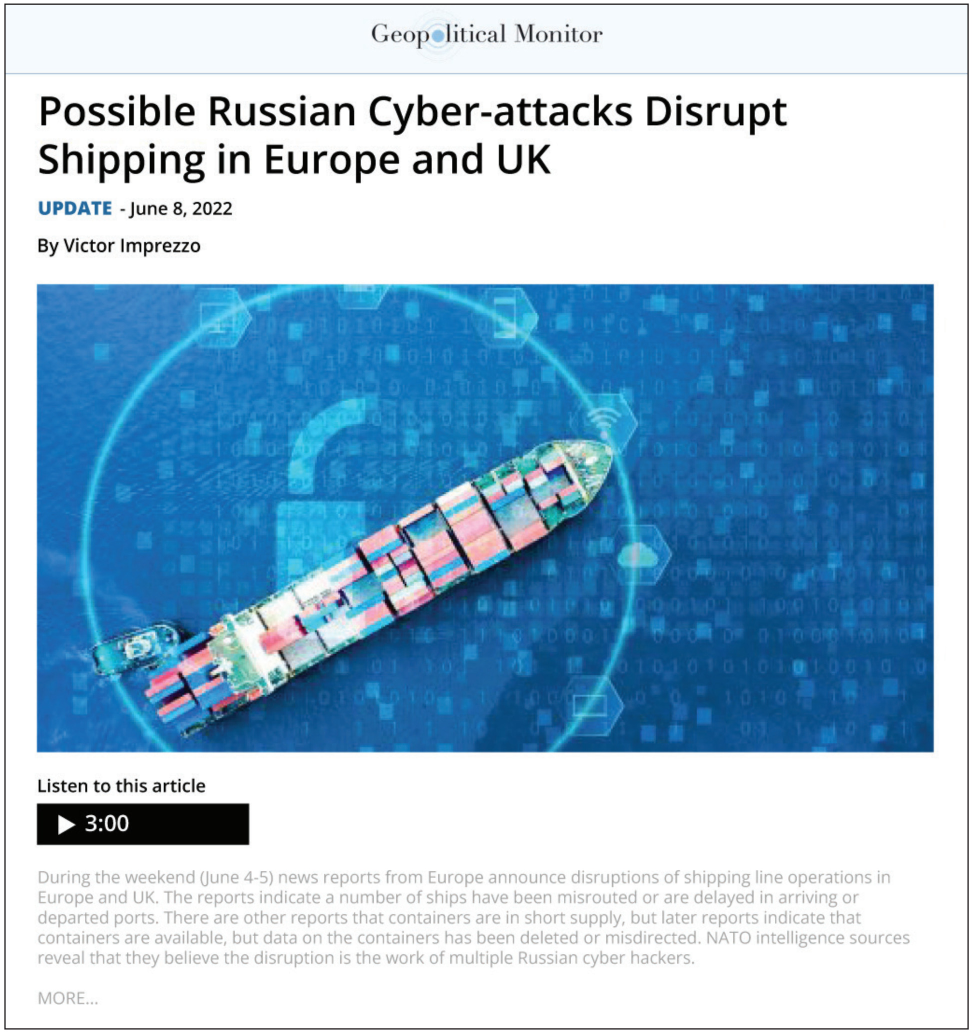
News Update



Geopolitical Monitor

Possible Russian Cyber-attacks Disrupt Shipping in Europe and UK

UPDATE - June 8, 2022

By Victor Imprezzo

Listen to this article

▶ 3:00

During the weekend (June 4-5) news reports from Europe announce disruptions of shipping line operations in Europe and UK. The reports indicate a number of ships have been misrouted or are delayed in arriving or departed ports. There are other reports that containers are in short supply, but later reports indicate that containers are available, but data on the containers has been deleted or misdirected. NATO intelligence sources reveal that they believe the disruption is the work of multiple Russian cyber hackers.

MORE...

CONTINUED

"During the weekend (June 4-5) news reports from Europe announce disruptions of shipping line operations in Europe and UK. The reports indicate a number of ships have been misrouted or are delayed in arriving or departed ports. There are other reports that containers are in short supply, but later reports indicate that containers are available, but data on the containers has been deleted or misdirected. NATO intelligence sources reveal that they believe the disruption is the work of multiple Russian cyber hackers.

Then beginning on June 6 and extending to June 8, U.S. and Canadian officials and company officials within the energy sectors in Manitoba, Ontario, Saskatchewan, Montana, North Dakota, and Wisconsin report local outages as well as large-scale blackouts in the power grid. The severity of disruptions varied, depending on the scale of the attack as well as the operational properties of the grid. The attacks were attributed to three and perhaps as many as four hacker groups from within Russia. Reports reveal that the attacks ceased at midnight June 8. It appears that the attacks were restricted to specific geographical areas and focused on the energy sector's operational technologies (OT) vulnerabilities.

Following the attacks, DNV (Det Norske Veritas group), shared their findings in their The Cyber Priority report. They found that while IT environments are protected, energy businesses need to boost security for its operational technologies (OT), which are the computing and communication systems they use to manage, monitor, and control industrial operations. The survey found that fewer than half of the respondents (47%) believe that their OT security is as robust as their IT security and less than one-third of those working with OT believe their company is making securing their supply chain a top priority. The lack of sufficient cyber security measures in power grid command and control systems, billing software, distribution and monitoring systems caused by introducing 5G as well as the adoption and installation of industrial Internet of Things (IoT) systems is not helping matters. "Our research identifies 'remote access to OT systems' among the top three methods for potential cyber-attacks on the energy industry. We would urge the sector to pay greater attention to assuring that equipment vendors and suppliers demonstrate compliance with security best practice from the earliest stages of procurement," said Jalal Bouhdada, Founder and CEO at Applied Risk, an industrial cyber-security firm acquired by DNV in 2021.

A top U.S. Intelligence official responding to outrage by congressional intelligence oversite committees of another intelligence failure, claimed that they had warned NATO and U.S. organizations about potential Russian cyber-attacks even before the Russian invasion of Ukraine. When asked by reporters if the intelligence community believes this was a precursor to a larger nationwide attack, he simply said, "no comment."

Inject Three

June 4 – 8, 2022

PREPAREDEX

BRPW - 2022

Review & Plan

Following the U.S. Intelligence report, CEOs and Board of Directors across the country called in their senior leadership teams and instructed them to provide their respective Boards with a comprehensive strategy to address the potential threat to the company's current operations. In particular they want the leadership to examine:

1. Company operations vulnerable to cyber-attacks and actions to minimize disruption of operations

- Actions to date
- Actions planned

2. Supply Chain vulnerabilities and plans to adapt to loss of critical material/ parts for:

- One month, six months or more

3. Communications with internal and external stakeholders on potential threats and plans of actions to deal with disruptions.

CONTINUED

1. **Breakout into Groups**
2. **Choose a Team Name (get creative)**
3. **Select Roles (don't worry about experience)**
4. **Discuss Questions**
5. **Return with a Brief (30 Minutes)**

Breakout Discussion Questions:

1. If outages impact Global Petroleum operations, what are the mid-to-long-term potential issues?
2. What and when would you tell your stakeholders? Who are your stakeholder groups?
3. How would a cyber-attack, like the NotPetya attack on Maersk shipping in 2017, affect today's supply chain, if it also included simultaneous attacks on 3-4 of the other large shipping lines and ports?
4. What other questions would you be considering?