National Bank of Ukraine

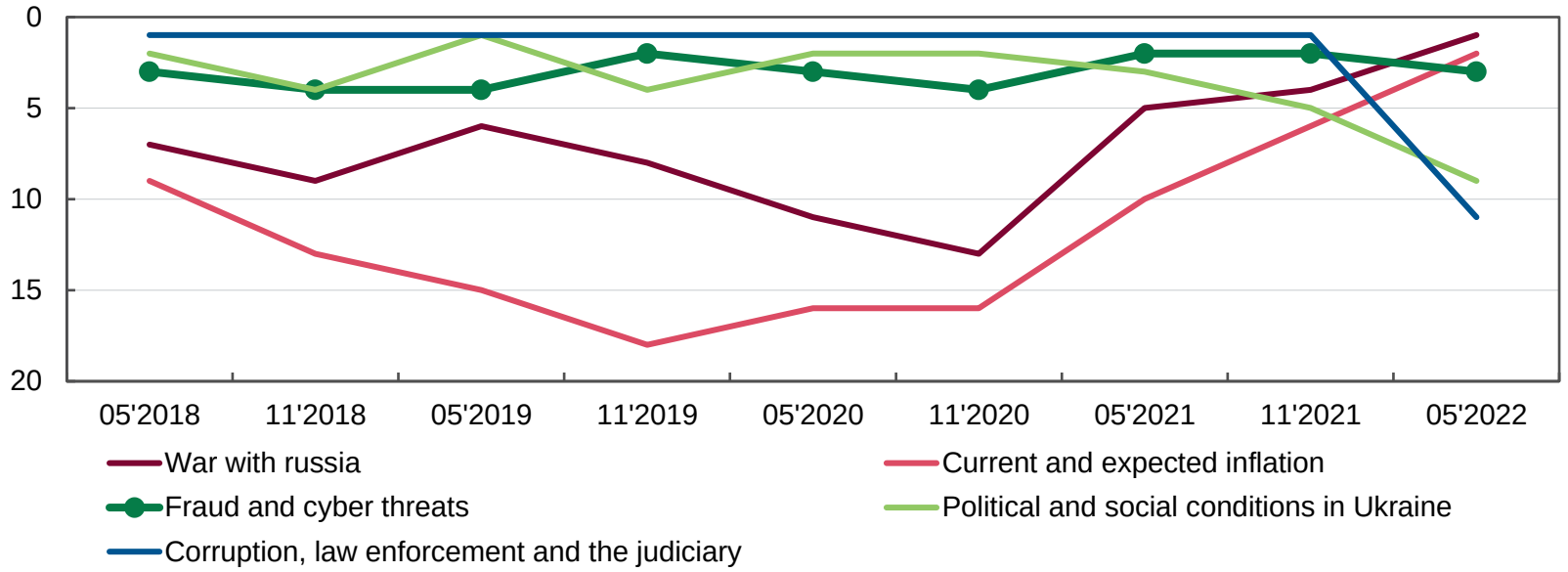
Cyber risks and banking system resilience in Ukraine in time of war

Pervin Dadashova

30 September 2022

Cyber risk stays among TOP-5 for financial stability for years

Rankings of major risk factors in financial sector*

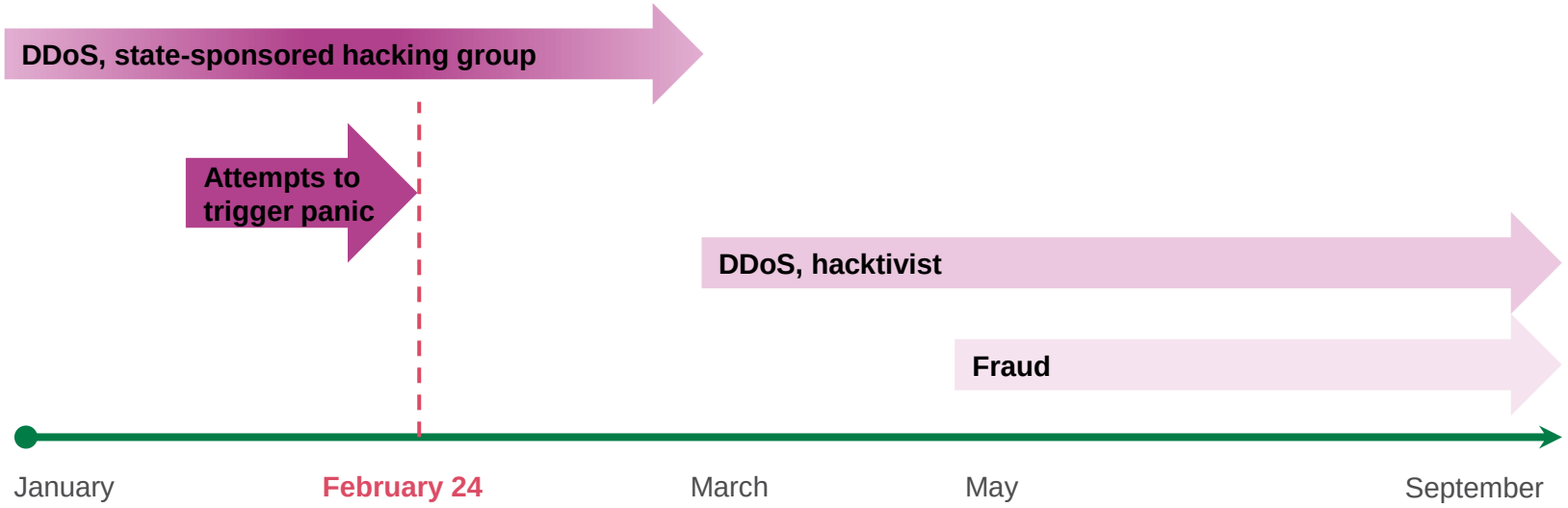


* Based on the balances of responses in the Systemic Risk Survey.

Source: NBU.

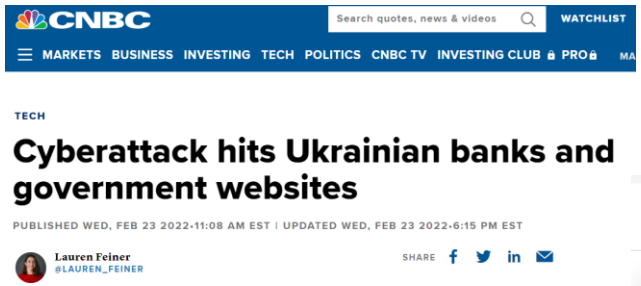
- Banks consider fraud and cyber risks to be among the TOP-5 risks for financial stability.
- High demand for online services raised attention to cyber security and banks investments in this area.
- For years, banks were working on services security; they were considering them in the course of development of new cashless online products.

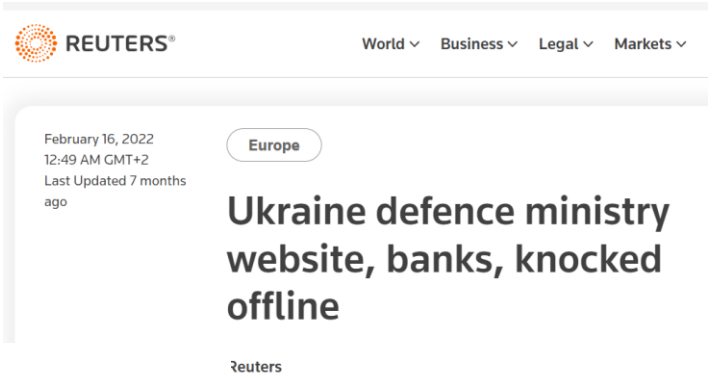
Nature of cyber attacks on Ukrainian banks continues to change



- Before the full-scale invasion started on February 24, the central bank and dozens of Ukrainian banks came under massive attacks, primarily DDoS.
- Russia used cyber-attacks to disrupt smooth functioning of the banking system and trigger panic, bank runs, and undermine stability of the financial sector.
- Types of the main cyber threats changed in time.

Cyber risks surged before the full-scale war started

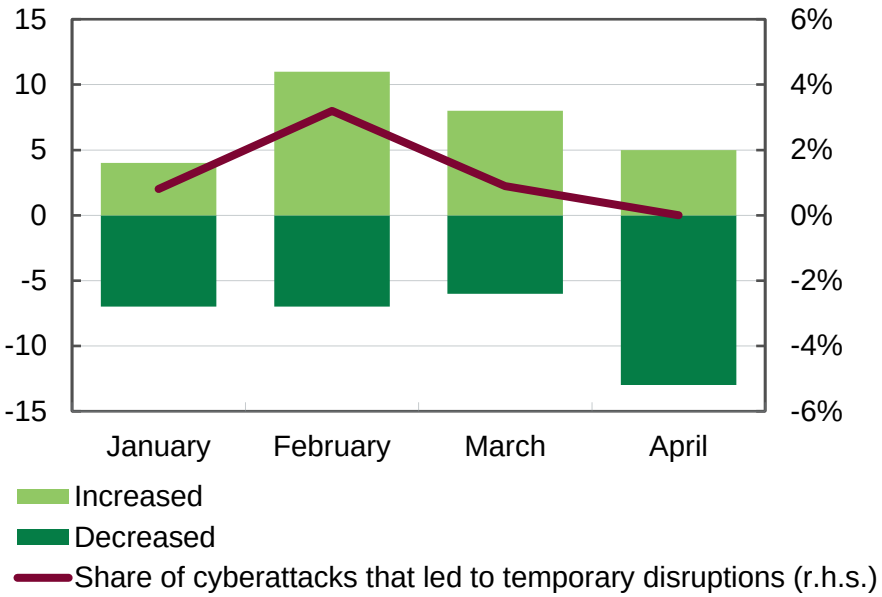




Back to slide 3

Number of cyber attacks fell since February

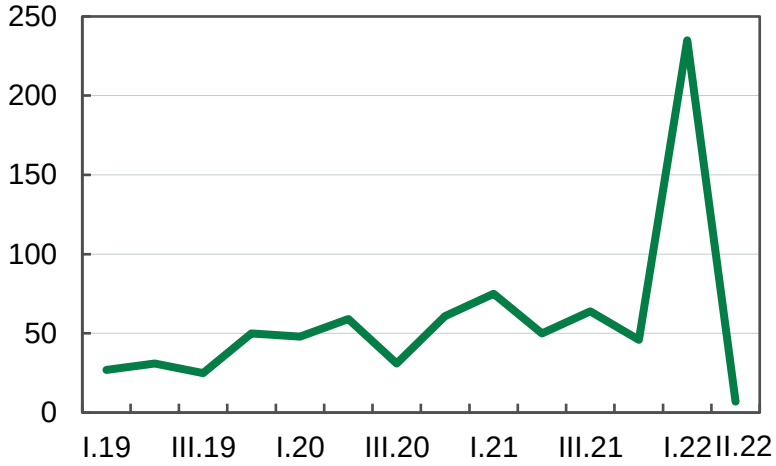
Distribution of banks depending on the change in the number of cyber attacks in 2022 compared to Dec 2021



During the period, 25 out of 68 banks experienced cyber attacks.

Source: Survey of banks, NBU estimates.

Quarterly number of attacks on the NBU informational resources (after anti-DDoS systems), millions

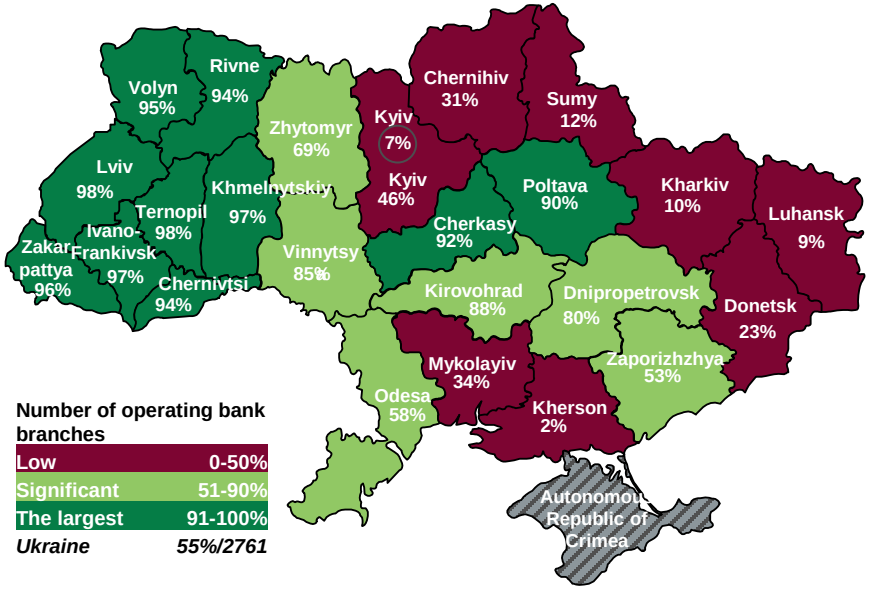


Source: NBU.

- Numbers of the cyber-attacks increased significantly in early 2022 and peaked in February.
- Cyber attacks were massive, unsophisticated, and became straightforward.
- Banks learned how to counteract cyber attacks quite fast, and now the attacks are almost harmless.

War brings threats of physical damage to data storage facilities

Share of operating branches of systemically important banks across regions as of 3 March 2022



Source: Survey of systemically important banks.

Banks survey results on the data storages

Indicator	Number of banks	Percentage of banks (out of 68)
Data storages located in Kyiv	53	78%
Backup storages located in Kyiv	53	78%
Realocated data storages	50	74%
incl. realocated to other cities	23	34%
incl. reallocated to the cloud	46	68%
Plan to use cloud permanently	24	35%

Source: Survey of banks, NBU estimates.

- The information was at risk of loss not only due to cyber attacks, but also because of possible damage to storage facilities.
- The NBU allowed banks to process personal data and client transactions using cloud services with equipment located abroad.
- Almost 50 banks (out of 68) opted to relocate or duplicate data to a cloud hardware located abroad.

Key takeaways from Ukrainian experience

- Cyber-risk is usually much more serious than previously thought, can potentially trigger other risks.
- Cyber-security requires continuous development and adjustments, management of the bank should be flexible to allow for it.
- Banking sector should be prepared not only to cyberattacks against individual banks but also to simultaneous attack on a number of SIBs and the central bank. Therefore, they should have contingency plans for such situations.
- Cyber-security should be imbedded into risk management culture of banks so that contingency planning is a well-established and continuous process, integrated into the product development, and supported with appropriate investments.