Cyber threats to financial stability in a complex geopolitical landscape

Prepared by Benjamin Klaus and Jonas Wendelborn

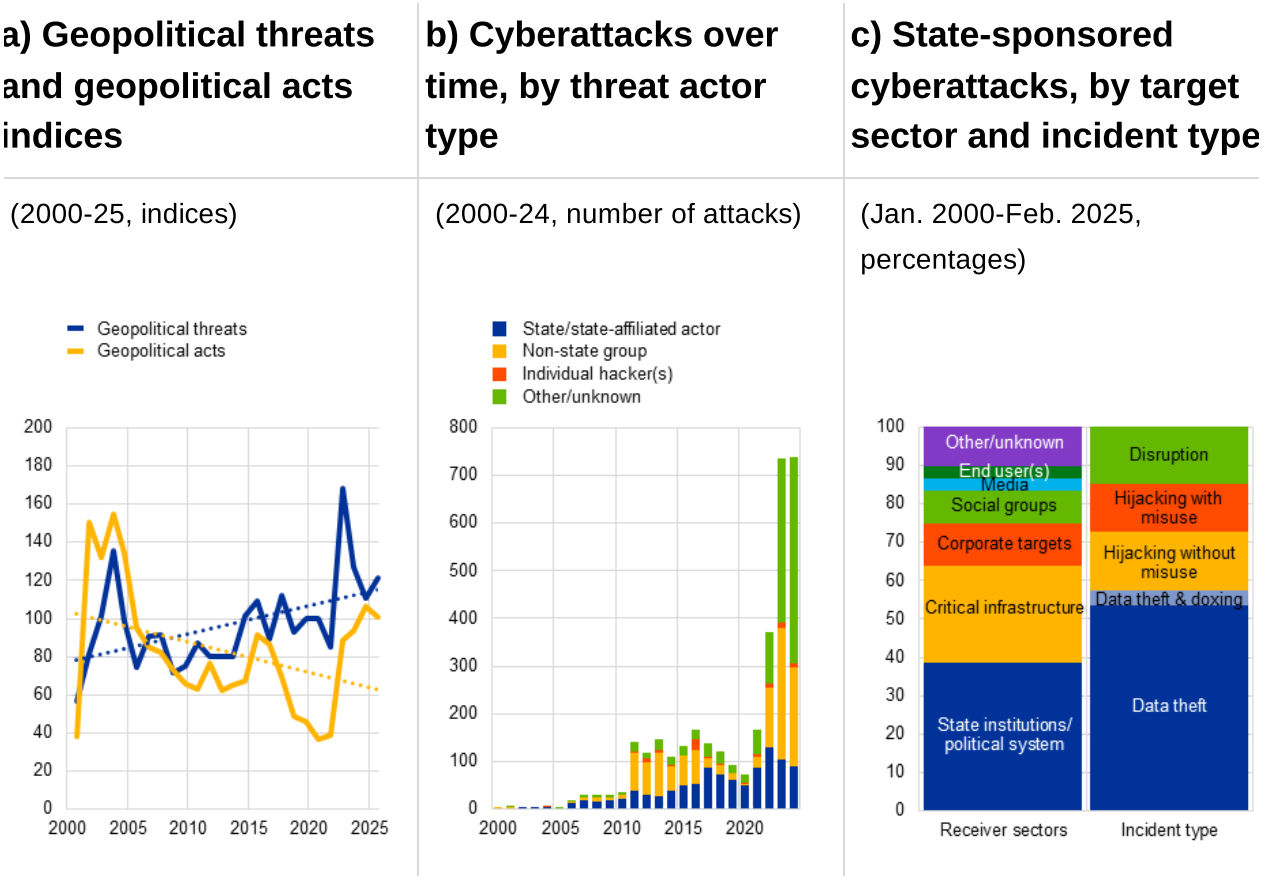
Published as part of the Financial Stability Review, May 2025.

Both the prevalence of geopolitical risks and their actual manifestation have been rising in recent years. Geopolitical threats have waxed and waned since the turn of the millennium, at times escalating into hostile action. This situation has been accompanied by a longer-standing trend of increasing geopolitical tension and global fragmentation (**Chart A**, panel a). In this context, cyberattacks are playing an increasingly important role in the perpetration of hybrid conflicts. While the precise number of cyberattacks – both successful and unsuccessful – remains unknown, publicly disclosed data indicate that the volume of such attacks has increased substantially over the past decade, with a significant number of state-sponsored attacks seen in some years (**Chart A**, panel b)[1]. Moreover, a number of countries conduct cyber activity not just via dedicated military or intelligence units but also via groups of cyber criminals acting on their behalf.[2] Against this backdrop, this box explores the threat to financial stability arising from state-sponsored cyberattacks.

State-sponsored cyberattacks primarily target state institutions and critical infrastructures and are mainly aimed at data theft. The principal targets of state-sponsored cyberattacks are state institutions such as governments and ministries, the armed forces and public administration (**Chart A**, panel c). Primary targets in critical infrastructures include the telecommunications, energy and financial sectors as well as defence and transport companies. In addition, other companies and social groups are targeted, including activists and political opposition groups and, to a lesser extent, the media and end users (e.g. individuals). Attacks on specific sectors (e.g. the financial industry[3]) tend to be clustered over time. There are many reasons why sovereign states engage in malicious cyber activities, although attacks are aimed predominantly at data theft, potentially linked to espionage. However, and especially in times of open conflict, the goal of sabotage and data destruction is to cause maximum disruption by interfering with an opponent's military operations or by destabilising civilian life. Disruptive attacks can also be used to exert pressure in the hope of forcing a change in behaviour or political position. As such, some cyberattacks can be a part of influence campaigns around important elections, for instance. In addition, some cyber activities are aimed at expropriation, in particular via ransomware attacks or the theft of crypto-assets.

Chart A

Geopolitical tensions are increasingly accompanied by state-sponsored cyberattacks



Sources: Caldara and Iacoviello*, EuRepoC database and ECB calculations.
Notes: Panel a: the chart shows annual averages for the monthly geopolitical threats and acts indices. For 2025 the average covers January to April. Panel b and c: "State/state-affiliated actor" refers to attacks conducted by nation-state actors or non-state actors for whom a state affiliation is suggested. They are the same attacks as those labelled "state-sponsored cyberattacks" in panel c. Panel b shows the annual numbers of cyberattacks up until 2024, while panel c only shows the subset of state-sponsored cyberattacks, but for the full sample period of the EuRepoC database between January 2000 and 25 February 2025.
*) Caldara, D. and Iacoviello, M., "Measuring Geopolitical Risk", *American Economic Review*, Vol. 112, No 4, April 2022, pp. 1194-1225.

Geopolitical rivalry is increasingly playing out in cyber space, with most state-sponsored cyberattacks originating from a handful of countries. Historically, the main tool used to settle geopolitical disputes between countries has generally been armed conflict. However, the toolkit employed alongside diplomacy to achieve strategic goals without resorting to physical force has evolved. The effectiveness of the tools employed depends heavily on the geoeconomic and political position of the countries involved. At the same time, hybrid techniques, including espionage, infrastructure sabotage and influence campaigns, are

increasingly being used to pursue conflicts by other means. While such techniques are not new, the rise of the internet and digitalisation since the 1980s has turned cyber space into a key battleground where such activities may be carried out and has opened up new avenues of attack. As such, the degree to which countries have used cyberattacks to further their national interests varies greatly, with a relatively small cluster of countries, often classified as authoritarian regimes, being responsible for the majority of state-sponsored attacks (**Chart B**, panel a). Such cyberattacks are clearly linked to geopolitical risk factors, but policy uncertainty in both sponsoring countries and targeted countries also seems to play a role at times. The frequency of state-sponsored cyberattacks tends to increase when sponsoring countries encounter geopolitical risks or economic policy uncertainties. Similarly, target countries experience more attacks under conditions of heightened geopolitical risk or economic policy uncertainty (**Chart B**, panel b).

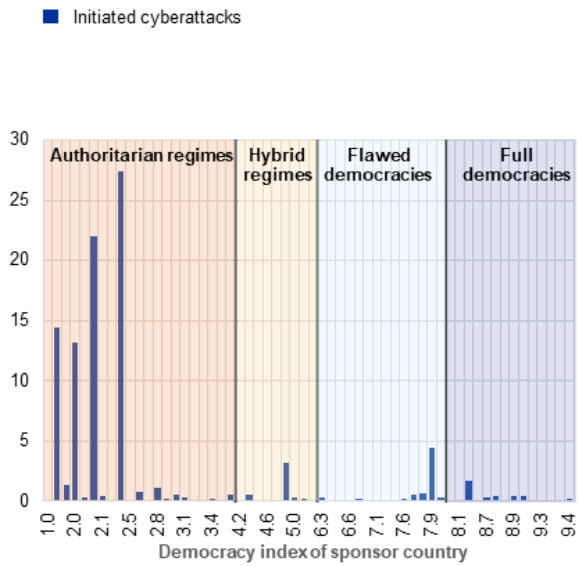
The threat of cyberattacks to financial stability is significant, given the growing digitalisation and interconnectedness within the financial system.[4] Cyberattacks can pose systemic risks by potentially disrupting critical financial services and operations, especially if an attack has an impact on a critical entity or if interconnections between non-critical entities lead to cascading effects. The propagation channels of these attacks include operational, financial and confidence avenues which can amplify the impact of attacks until they impair key economic functions. The potential for cyberattacks to threaten financial stability depends on the scope and severity of the impact, along with factors such as substitutability, risk correlation and interconnectedness. Attacks on infrastructures without ready substitutes or that expose vulnerabilities in other services can propagate widespread stress. As such, increasing dependence on third-party offerings, including centralised cloud technologies, opens up channels through which cyberattacks can cause stress in the financial system, even without targeting financial entities.

Chart B

Cyberattacks are predominantly deployed as geopolitical tools by a small set of autocratic states

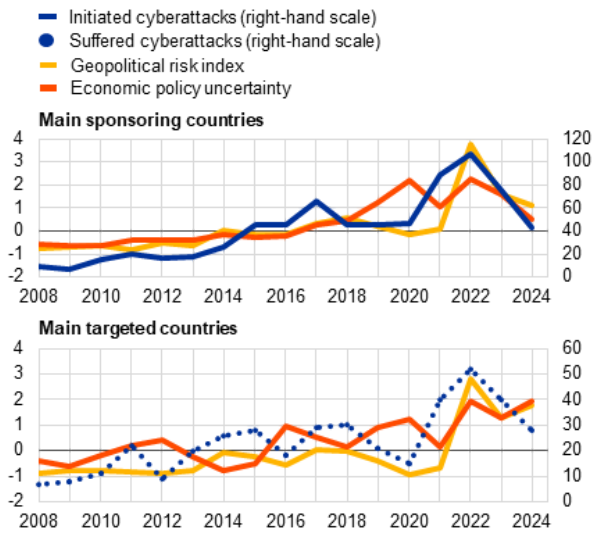
a) Initiated cyberattacks and democracy index of sponsor countries

(percentage shares)



b) Cyberattacks, geopolitical risk index and economic policy uncertainty index

(2008-24; left-hand scale: z-scores, right-hand scale: number)



Sources: Baker, Bloom and Davis*, Caldara and Iacoviello**, EuRepoC database, Economist Intelligence Unit, Our World in Data and ECB calculations.

Notes: Both panels only show cyberattacks conducted by nation-state actors or non-state actors for whom a state affiliation is suggested. Panel a: the democracy index and classification of political regimes refers to the 2024 democracy index of the Economist Intelligence Unit. It scores countries on a scale from zero to ten, based on 60 indicators from the following five categories: electoral process and pluralism; functioning of government; political participation; political culture; and civil liberties. Initiated cyberattacks include all attacks covered by the EuRepoC database between January 2000 and 25 February 2025. Panel b: the main sponsors are a group of four countries; the main targets are a group of seven countries. The number of cyberattacks initiated/suffered is the sum across these groups. The geopolitical risk index and the economic policy uncertainty index are available for two of the main sponsoring countries. Of the main targeted countries, the geopolitical risk index is available for all seven, while the economic policy uncertainty index is only available for five. Indices are averaged and standardised for each group across the countries for which the indices are available.

*) Baker, S., Bloom, N. and Davis, S., "Measuring Economic Policy Uncertainty", *The Quarterly Journal of Economics*, Vol. 131, No 4, November 2016, pp. 1593-1636.

**) Caldara, D. and Iacoviello, M., op. cit.