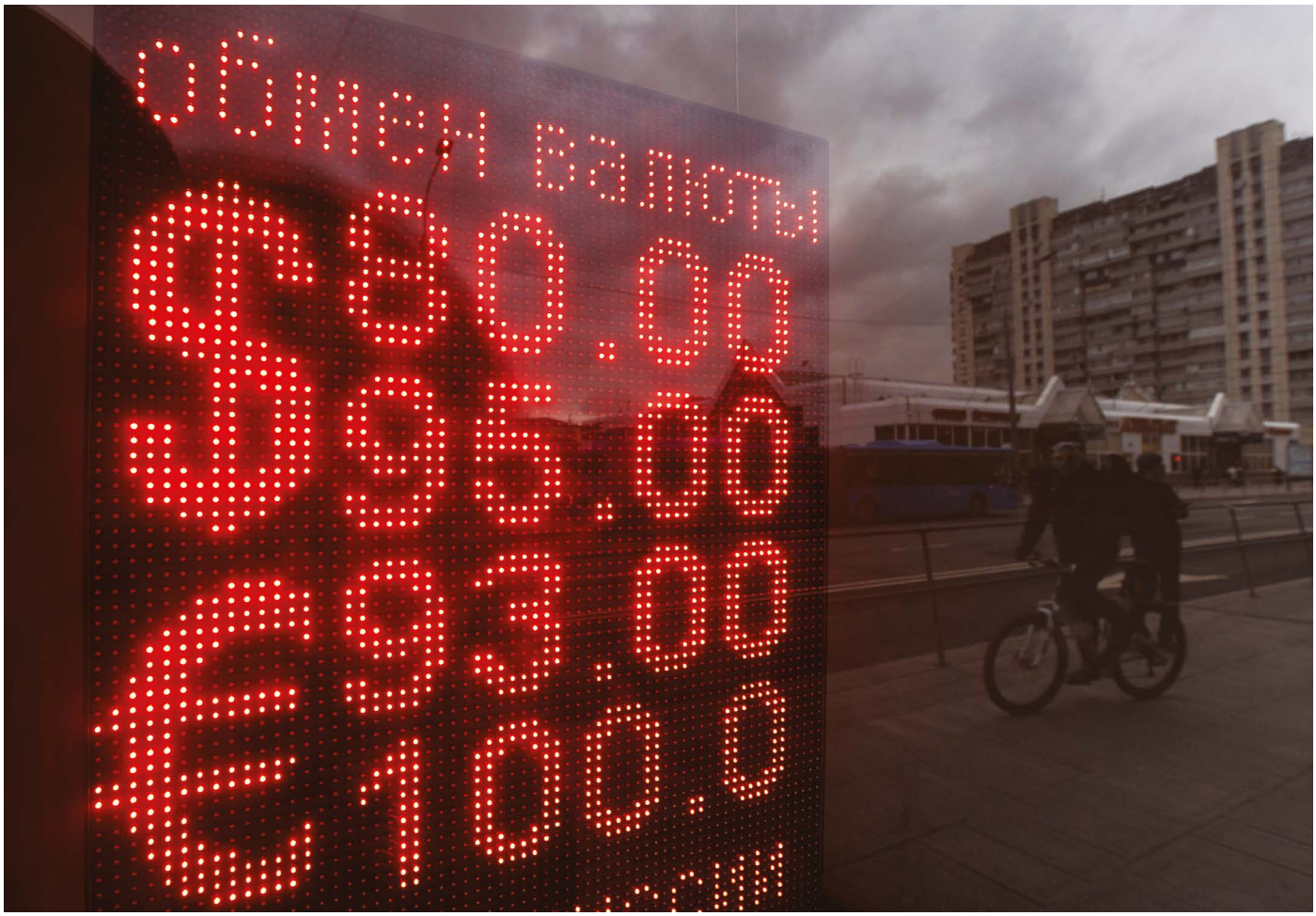
Comment



ANDREY RUDAKOV/BLOOMBERG VIA GETTY

A sign in Moscow displays currency exchange rates. Unpredictable economic consequences followed Russia's invasion of Ukraine in February.

Weak links in finance and supply chains are easily weaponized

Henry Farrell & Abraham L. Newman

Russian sanctions highlight how network analysis is urgently needed to find and protect vulnerable parts of the global economy.

When Russia invaded Ukraine on 24 February, nobody expected that the United States, the European Union, the United Kingdom, Japan, Canada and other nations would isolate Russia from the global economy in retaliation. Instead of limited and largely symbolic sanctions, which were all Russia faced when it annexed Crimea and occupied eastern parts of Ukraine in 2014, this latest response has had devastating ripple effects.

Key Russian banks have been denied access to the US dollar, foreign reserves and the Society for Worldwide Interbank Financial Telecommunication (SWIFT) messaging system, which banks use to relay financial information to each other. The United States and its allies blocked the export of high-end semiconductors to Russia's technology and defence sectors, as well as software, oil- and gas-refining equipment and other items. As one US law firm put it, it is now illegal to knowingly supply a toothbrush to a company that occasionally helps to repair Russian military equipment.

Russia's economy is reeling. The value of Ukraine's currency, the hryvnia, has been knocked flat by the war. No one knows what will unfold.

The biggest surprise is how this has been done – by weaponizing the networks that bind the global economy together. Financial and supply networks have chokepoints, which powerful states can use to punish individuals, businesses and even nations. Some of these points are known; many have yet to be identified.

There has been too little academic study of these pressure points, however. Policymakers lack the necessary data to make informed decisions. Companies hold information on supply chains close; governments and the public don't have an overview. Data on financial and information networks and their vulnerabilities are similarly patchy.

For decades, policymakers have assumed that production and financial markets can largely look after themselves, with some oversight by regulators. These assumptions are poorly suited to a world in which hostile governments can weaponize the weak points in the global economy against their adversaries.

Data scientists, political scientists, economists and macrofinance scholars urgently need to map these networks to discover the points that pose the most threats and risks. As a first step, the United States has begun to survey supply relationships. More detailed knowledge would allow policymakers to close vulnerabilities where possible, and to mitigate them where it is not.

Some reforms, such as stress-testing banks to see whether they would survive unexpected turbulence, were enacted after the global financial crisis in 2007–09. These shored up the global financial system by discouraging risky speculation. But they are not enough to defend against targeted attacks.

Policymakers need to think about macrofinancial risks[1]. Some analysts have predicted that cutting Russian banks out of SWIFT might trigger the kind of global systemic collapse that nearly happened when Lehman Brothers, a financial-services firm in New York City, failed in 2008. They fear that Russian financial sanctions might destabilize payments between counterparties, creating a crisis of confidence that could feed on itself. Those early predictions have been wrong so far. But they highlight that there are uncertain consequences of removing major elements of a system whose deep workings and sources of stability remain unmapped.

Networks as weapons

Globalization has led to extraordinary economic efficiency. Money transfers happen in nanoseconds, not days or weeks. Global supply chains allow hundreds of suppliers in dozens of countries to build complex products, such as smartphones. Some supply chains are dominated by one country. For instance, China controls nearly all stages of photovoltaics manufacturing.

These links make economies more interdependent. Businesses in different countries might rely on a single supplier for the sake of efficiency – which creates risks if that supplier fails. As war has spread across Ukraine, German car factories have fallen idle because they cannot obtain electronic cabling systems, or 'wire harnesses', produced by Ukrainian suppliers.

The global economy isn't symmetric, an open system of links that offers many alternative routes when one closes, as conventional wisdom has supposed. It's asymmetric: the flows of trade and finance rely on a relatively small number of hubs or nodes with many connections[2,3]. Control over those hubs allows governments to deny adversaries access to key parts of global economic networks[4].

For example, in 2019, when South Korean courts found Japan potentially liable for forced labour during the Second World War, Japan threatened the South Korean electronics industry. Companies such as Samsung, based in Suwon-si, South Korea, relied on chemicals and components, including fluorinated polyimide and photoresists, to make their products. This made them vulnerable to pressure from Japan, which produced 90% of these precursors.

> **"There are uncertain consequences of removing elements of a system whose workings are unmapped."**

A few nations or companies have disproportionate sway over areas of finance and trade. For example, SWIFT is based in the EU, but is run by banks that rely on the US financial system. Transactions between non-US parties often rely on US dollars, which means that they have to be cleared through a small number of US-regulated financial institutions. And Silicon Valley in California controls much of the world's advanced technology and computing.

Targeted attacks against chokepoints can quickly disrupt the entire network. In 2012, the United States and the EU cut Iran out of the global financial system by denying its banks access to dollar clearing and SWIFT. Iranian companies found it hard to get paid for oil, leading to a dramatic fall in exports. Complicated barter arrangements emerged: oil was exchanged for tea, zips and bricks. The impacts can reach farther than those from general shocks, such as supply-chain disruptions from the COVID-19 pandemic. Now, the US denial of some Russian banks' access to the dollar effectively cuts them out of the global financial system.

Other nations could be brought into line. The United States also controls crucial intellectual property and design software for semiconductors. Fearing loss of access, non-US-based semiconductor manufacturers, including the Taiwan Semiconductor Manufacturing Company in Hsinchu, are complying with the US ban on exports to Russia. China-based manufacturers, such as the Semiconductor Manufacturing International Corporation in Shanghai, will face the threat of sanctions if they do not also cooperate.

Hidden weaknesses

Governments and firms need to prepare for disruptions from intentional, rather than random, shocks. And the fallout is hard to foresee.

Some vulnerabilities are well known. For example, China dominates the mining and refining of rare-earth elements, such as cerium and yttrium, used in many items, from mobile phones to wind turbines. In 2010, China halted shipments of rare-earth elements to Japan after a dispute over a captured fishing vessel – prompting fears that it could use its dominance in this market as a tool of coercion or retaliation. Since 2010, China's share of rare-earth production has dwindled from a near monopoly to slightly less than 60% of the global market, although it still has a central role in processing these elements.

Similarly, many cars, phones and watches rely on the US GPS to determine their geographical location. GPS has military origins and is subject to federal control – leading Russia, China and the EU to develop their own competing satellite positioning systems, at a cost of billions of dollars.

Other vulnerabilities are more obscure. Only businesses themselves know what their supply chains actually look like, and even their knowledge is imperfect. They often know their first-tier suppliers (those they have direct relationships with), and might know their second-tier suppliers (those on whom their first-tier suppliers rely). After that, things get murky.

More weak links might be discovered only when another war, disaster or pandemic haphazardly reveals them. Before the COVID-19 pandemic, few people noticed or cared that a single German manufacturer produces roughly 75% of the machines for processing the fabrics that high-quality medical masks require, for example. Vaccine manufacturing is dominated by a small club of mostly rich countries. Although not explicitly weaponized, this concentration of production power has brought rich countries to the front of the line for messenger-RNA-based COVID-19 vaccines while poorer countries still wait for adequate supplies.

Dark money

Key aspects of the global financial system resist understanding as well as regulation. The amount of money hidden in tax havens is possible to measure only indirectly[5], and offshore dollars are hard to assess or control. 'Dark pools', in which large volumes of complex financial instruments are traded, are opaque to outsiders.

ITAR-TASS NEWS AGENCY/ALAMY

A worker walks beside a gas pipeline near St Petersburg, Russia.

With so little to go on, impacts are difficult to predict. Even limited efforts to weaponize global networks can have big unanticipated consequences. For example, in 2018, the United States 'designated' Russian oligarch Oleg Deripaska and his companies — meaning US businesses were prohibited from having dealings with them, and businesses outside the United States could not facilitate their transactions. This put the customers and suppliers of enormous conglomerates, such as the aluminium processor United Company Rusal, based in Moscow, in legal jeopardy. It soon became clear that designating Rusal might devastate European car manufacturers and other businesses. The United States effectively wound down some of the sanctions by requiring Rusal and other companies to decrease Deripaska's ownership stake.

Domino effects

As powerful governments take advantage of chokepoints, they risk escalation, disruption and retaliation. The war in Ukraine is already affecting food markets. Ukraine and Russia together account for about 30% of global wheat production. Ukraine is a major exporter of barley and maize (corn) and produces nearly 50% of the world's sunflower oil by volume. Between them, Russia and Belarus produce roughly 31% of global potash — a key ingredient of fertilizer. Fertilizer shortages risk exacerbating food shortages and human suffering.

Russia has countered that it might itself block exports of nickel and stop gas flows to Western Europe. It has imposed its own (largely symbolic) financial sanctions against US officials. Such measures could backfire in the medium term. Russia needs to earn hard currency from exports; many of its products can be bought elsewhere. Even so, substantial economic disruption is likely to happen in the next few years.

Russian retaliation might give rise to a vicious spiral of counter retaliation. Debates on nuclear war and cybersecurity conflicts focus on whether a shared understanding of a 'ladder of escalation', from less to more extreme uses, can lower risks[6]. No common picture of weaponized economic networks exists.

It is possible that the strong network of countries in the North Atlantic Treaty Organization and their allies will deter countermeasures. Equally, targeted countries might consider other ways to retaliate. Between the First and Second World Wars, fears of economic sanctions helped to spur Nazi Germany to grab territory to insulate itself from external pressure[7]. After the United States isolated Iran from the global financial system in 2018, Iran allegedly attacked shipping in the Strait of Hormuz, a geographical chokepoint for global energy flows.

Economic coercion and the economic fallout from military coercion could wreak havoc in a globally interconnected world and might make it difficult or impossible for governments to work together to tackle international problems, such as climate change, pandemics and global health.

Next steps

Addressing weaponized networks requires the collaboration of researchers in disciplines across the natural and social sciences.

The first step is to map the networks that bind the world. US President Joe Biden's administration has already identified the lack of supply-chain data as an urgent policy priority. It is not yet clear whether Congress will provide sufficient funding to address it. Other governments, too, must gather data and consider how to minimize the security risks of sharing them. Preliminary mapping exercises in the United States and Europe highlight broad areas of dependency, including battery production.

Researchers should probe networks for vulnerabilities. Algorithms for network analysis can identify bottlenecks[8]. Economic models can test networks' robustness to external shocks or attacks[9]. A qualitative understanding must be built, including of alliances and the politics of global finance. Dependencies between networks require study. For example, although oil markets are relatively robust (because one source of oil can reasonably be substituted for another), oil shipping depends on financial networks[10] and shipping insurance, both of which have chokepoints.

Policymakers must assess how best to mitigate vulnerabilities before they are exploited. Strategies will depend on specifics. Substitutes and alternative suppliers might be found, as has happened for rare-earth elements. Some nations, including the United States and Australia, are beginning to accept the environmental consequences of mining and processing rare-earth elements to undermine China's dominance.

Governments might subsidize domestic suppliers, as South Korea did. This could be more difficult than it looks. Supply relationships are complex, and businesses might still prefer to work with established partners. South Korea has found it challenging to reduce its dependence on Japanese materials for electronics. In the United States and the EU, domestic political stand-offs make it hard to agree on whether to boost renewables, frack for gas and oil or expand nuclear energy. Understanding the consequences of a changed security situation for the energy transition and climate change following Russia's invasion is a major research and policy challenge.

Where possible, arrangements between like-minded governments might underpin supply relationships. The EU and the United States are increasing cooperation in the production of advanced technologies, and other countries could look to join them. If cooperation is impossible, materials scientists and engineers will have to find substitutes for key inputs.

Sometimes, the vulnerabilities are ineradicable. China depends on foreign manufacturing facilities, or 'fabs', to manufacture advanced semiconductors. Despite hefty industrial subsidies, it has failed to catch up with cutting-edge techniques and processes. Addressing such vulnerabilities will involve difficult — and political — trade-offs between economic progress and national security.

Shoring up financial networks will be even

harder. The SWIFT system and dollar-clearing networks were created during the cold war. For better or worse, few paid attention to their strategic implications. Countries that do not like the currently dominant networks will find it hard to create attractive alternatives under conditions of distrust. They might devise workarounds. For example, Iran built a clandestine financial micro-system to shelter itself from the US sanctions regime. Russia is trying to move away from transactions in US dollars. Some economists argue that India might try to maintain its neutrality and become a safe haven for politically risky financial assets.

A key question researchers need to ask is: under which circumstances might the network structures that the United States and the EU have weaponized start to unravel, to be replaced by alternative networks or a more fragmented global economy?

Answers will require exploring the hinterlands between economics, political science and macrofinancial history, as well as network science, complexity research, geography, materials science and other disciplines. Social scientists need to build integrated models to understand the interactions between these economic and political strategic decisions, and to gather data to test and refine.

The actions against Russia will accelerate the weaponization of global economic networks as countries look to exploit others' vulnerabilities, secure themselves or both. Understanding and mitigating these security risks requires forging links among researchers.

The authors

Henry Farrell is a professor in the Stavros Niarchos Foundation Agora Institute and the School of Advanced International Studies, Johns Hopkins University, Baltimore, Maryland, USA. **Abraham L. Newman** is a professor in the Edmund A. Walsh School of Foreign Service and the Department of Government at Georgetown University, Washington DC, USA.
e-mails: hfarrel1@jhu.edu; aln24@georgetown.edu

1. Tooze, A. *Crashed: How a Decade of Financial Crises Changed the World* (Viking, 2018).
2. Danzman, S. B., Winecoff, W. K. & Oatley, T. *Int. Stud. Q.* **61**, 907–923 (2017).
3. Brintrup, A., Wang, Y. & Tiwari, A. *IEEE Syst. J.* **11**, 2170–2181 (2017).
4. Farrell, H. & Newman, A. *Int. Secur.* **44**, 42–79 (2019).
5. Zucman, G. *The Hidden Wealth of Nations* (Univ. Chicago Press, 2013).
6. Kreps, S. & Schneider, J. *J. Cybersecur.* **5**, tyz007 (2019).
7. Mulder, N. *The Economic Weapon* (Yale Univ. Press, 2022).
8. Elliott, M. *et al.* Preprint at https://doi.org/10.48550/arXiv.2001.03853 (2022).
9. Carvalho, V., Elliot, M. & Spray, J. *Supply Chain Bottlenecks in a Pandemic.* (Univ. Cambridge Faculty of Economics, 2021); available at go.nature.com/3sadf6
10. Hughes, L. & Long, A. *Int. Secur.* **39**, 152–189 (2015).

The authors declare no competing interests.

Unclear units stymie science

Robert Hanisch, Stuart Chalk, Romain Coulon, Simon Cox, Steven Emmerson, Francisco Javier Flamenco Sandoval, Alistair Forbes, Jeremy Frey, Blair Hall, Richard Hartshorn, Pascal Heus, Simon Hodson, Kazumoto Hosaka, Daniel Hutzschenreuter, Chu-Shik Kang, Susanne Picard & Ryan White

Here's how to make measurements clear and machine-readable.

In 1999, when NASA's Mars Climate Orbiter missed its intended orbit and burned up in the Martian atmosphere, the media had a heyday over the reason: one team had used metric units in its thrust calculations, another, imperial. The navigation software that exchanged this information lacked a built-in process to check units. So when one team's software produced data in imperial units rather than the expected metric ones, the spacecraft was set on the wrong trajectory. The result was the loss of five years of effort and hundreds of millions of taxpayers' dollars.

Two decades on, such problems persist. Researchers across fields often assume that their colleagues understand details without specifying them, and are therefore remiss when documenting units. Sometimes they leave them out entirely, provide ones that have multiple definitions or use units of convenience that have never been formally recognized.

Humans struggle to interpret numbers with sloppy or missing units, and it is much more difficult when computers are involved. Most software packages, data-management tools and programming languages lack built-in support for associating units with numeric data (with the exception of the language F#). This means that information is essentially stored and managed as 'unitless' values. Disciplines including bioscience and aerospace engineering have adopted conventions for unit representation, such as the Unified Code for Units of Measure (UCUM) and the Quantities, Units, Dimensions, and Types (QUDT) Ontology. But there are no broadly agreed technical specifications for how to represent quantities and their associated units without confusing machines.

There have been many calls in recent years to make data sets FAIR (Findable, Accessible, Interoperable and Reusable; see www.go-fair.org/fair-principles), and to ensure that open data abide by the 5-star deployment scheme suggested by World Wide Web inventor Tim Berners-Lee, which aims to make them findable, free and structured (see https://5stardata.info/en). Many researchers are now committed to depositing data in free and open repositories with appropriate metadata.

Chaos around units undermines these efforts. Already, many scientists invest more time in wrangling data than doing research. When data are not interoperable or machine readable, researchers' individual informatics approaches are thwarted. The benefits of data sharing shrink.

Unless we take steps to ensure that measurement units are routinely documented for easy, unambiguous exchange of data, information will be unusable or, worse, be misinterpreted. All global challenges, from pandemics to climate change, require high-quality data across multidisciplinary, international sources. Mistakes and lost opportunities will cost humanity much more than hundreds of millions of dollars for a single crashed spacecraft.

We are a group of scientists who are tackling this challenge, with backgrounds in chemistry, computer science, metrology and more. In 2018, the global collaboration CODATA (Committee on Data of the International Science Council) formed the Task Group on Digital Representation of Units of Measurement (DRUM). The goal of DRUM is to work with international science unions under the International Science Council to raise awareness of units and quantities in digital formats and to enable their communities to represent them. In 2019, another group — the International Committee for Weights and Measures (CIPM), an intergovernmental association — formed the Digital International System of Units (Digital SI). The Digital SI Expert Group has goals that are complementary to those of DRUM, focusing on worldwide agreed norms for unit representation in the metrology community. All authors of this Comment article are members of one or both of these groups.

Now, a few years into our mission, we need the community's help. We ask scientists,