SHIELDWATCH

FALLOUT FROM UKRAINE: THE IMPACT ON GLOBAL ENERGY AND CYBERSECURITY

MARCH 2022

- Billions at Risk for Pennsylvania Companies with Ties to Ukraine - US Officials Warn Against Increased Cyber Attacks following Russian Invasion

  Sourceree SHIELD Intelligence Services

- The Plot to Destroy Ukraine

  RUSI

- Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contract, Blunt, and Surge Lawyers of Competition

  RAND Corporation

- Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains

  Federal Reserve Bank of New York Staff Reports, no. 937

SOURCEREE

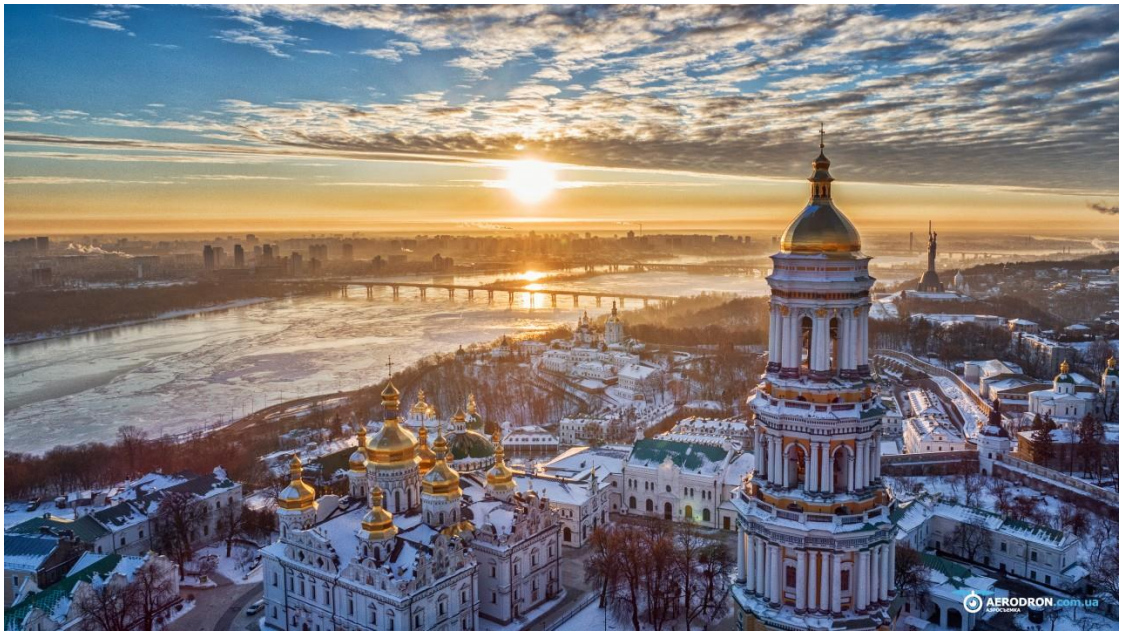
We close out February 2022 with the devastating Russian invasion of Ukraine. This SHIELDWatch touches on the potential global economic impact of the event, with a SHIELD original piece on how an increased cybersecurity threat could impact US businesses operating in Ukraine. The remainder of the articles give context to the Russian government's "soft" tactics leading up to military action, including energy security destabilization and trade disrupation. Finally there is a historical nod to the NotPetya cyberattack on a Ukrainian company in 2018, which had widespread global effects beyond the companies directly impacted, both up- and downstream.

Our hearts are with the people in Ukraine.

--Adam Murphy, Sourceree President

Billions at Risk for Pennsylvania Companies with Ties to Ukraine – US Officials Warn Against Increased Cyber Attacks following Russian Invasion

Christian Faranda, Foreign Policy Analyst
Sourceree SHIELD Intelligence Services
March 2022



Orange sunset and cloud over cityscape Kiev, Ukraine, Europe By slava2271

The world has been nervously holding its breath in anticipation of the Russian invasion of Ukraine for weeks. Global defense leaders strategized intervention efforts, the traffic out of Kyiv headed towards Poland intensified, and cybersecurity agencies warned businesses to brace for potential impact. Finally, in the early morning hours of February 24, 2022, Russian forces crossed into Ukraine, propelling world leaders - who had been working overtime to prevent the conflict - into an unavoidable Plan B. As we refresh our feeds optimistically, awaiting news of the preservation of Ukraine's sovereignty and safety for its residents, this post will examine how the Russian invasion could threaten US businesses' cybersecurity.

The anxiety surrounding the Russian threat to Ukraine prompted the US Cybersecurity and Infrastructure Security Agency (CISA) to sound the alarm for businesses and agencies to take "urgent, near-term steps" against cyber threats to critical infrastructure. Shortly after CISA's warning, the Department of Homeland Security published a memo stating, "Russia maintains a range of offensive cyber tools that it could employ against US networks." Businesses based in the United States that have partnerships or locations in Ukraine have an added risk. A 2017 Russian military intelligence cyberattack on a Ukrainian software provider spread, causing billions of dollars of damage worldwide. Pennsylvania businesses alone represent billions of dollars of US business activity in Ukraine:

- Westinghouse Electric, based out of Cranberry, signed an estimated $30 billion deal to build nuclear reactors at four separate sites in Ukraine in 2017, partnering with Ukrainian company Turboatom. Westinghouse was one of the multiple victims identified in the 2018 federal indictment of Russian government hackers threatening the victim's "most sensitive secrets and data."
- XCoal Energy & Resources of Latrobe began providing anthracite to Ukraine utility Centrenergo in a 2017 deal with a potential value of $79 million. The Reading Blue Mountain & Northern Railroad headquartered in Port Clinton was a major part of this deal, on deck to transport 700,000 tons of coal.
- GE Transportation of Erie signed a $1 billion agreement in 2018 to help modernize Ukraine's rail system.

The US-Ukraine Business Council (USUBC) aims to advance US trade and investment interests in Ukraine's emerging market; advocate for measures to improve conditions for bilateral trade and investment; and promote strong, friendly bilateral ties between the United States and Ukraine. As of February 2022, USUBC has 200+ entities engaged in their mission varying from non-profits, large corporations across multiple sectors, religious organizations, investment funds, law offices, and higher education institutes. All of these entities with a footprint in Ukraine, especially those with US critical infrastructure functions, will need to be on watch as Russia expands into the country. The full list of USUBC entities can be found here.

Just prior to the invasion, unaffiliated but suspected Russian hackers superficially attacked Ukrainian government websites, while also conducting a destructive malware operation against government, non-profit, and information technology organizations in Ukraine. The malware operation was discovered by the Microsoft Threat Intelligence Center which identified the attack as "designed to render targeted devices inoperable." A former Obama administration defense official remarked that Russia's invasion of Ukraine would be the first time "cyberspace operations" were part of an integrated offensive military invasion, further commenting that targets would be government senior leader communications and the military as well as Ukrainian national critical infrastructure, to include energy, manufacturing, and media.

In addition to US concerns, European partners are preparing for residual effects in Ukraine as well as direct cyber incursions by the Russians within their borders. The United Kingdom's National Cyber Security Centre warned large organizations to bolster their cyber security resilience amid the deepening tensions over Ukraine and the European Central Bank which has oversight of Europe's biggest lenders, is warning banks against the threat of cyber-attacks on banks launched from Russia.

US and global businesses are right to be concerned about potential cyber fallout from Russian hackers using the Ukraine invasion to expand the reach of their attack capabilities. The 2021 Colonial Pipeline ransomware attack perpetrated by Russian cybercriminals cost Colonial Pipeline a reported tens of millions of dollars to fully restore its systems after paying the $5 million ransom. The cost to American consumers was immeasurable. Russian hacking groups have also targeted the US government. In the SolarWinds breach of 2020, a hacking group believed to be associated with Russian intelligence gained access to at least 9 US government agencies and 100 businesses.

The Plot to Destroy Ukraine

Jack Watling and Nick Reynolds
15 February 2022
Royal United Services Institute for Defence and Security Studies (RUSI)

RUSI published this article the week before the Russian invasion into Ukraine diagramming Russia's chessboard leading up to military incursion, identifying multiple overlapping objectives that would result if the Ukrainian government responded in multiple different ways to Russian tactics. Leading up to and during a military invasion, the Russian government attacke Ukraine's energy security to destabilize the government. The Russians use astroturfing, a disinformation tactic that stages fake "activists" online and in live protests, to build upon known civil pain points in Ukraine. This is a tactic the Russian government has also deployed against the United States.

Select excerpts from the piece:

…examining the timeline and subsequent activities against Ukraine, it becomes possible to see the mechanisms by which Russia is seeking to bring Kyiv to heel. In the spring of 2021, Russia began a military build-up along Ukraine's borders. The initial surge of activity provided an opportunity to observe what caused a reaction in Western capitals. After a lull in the summer and the completion of the Zapad exercises in September last year, Russia began rapidly expanding its military presence all along Ukraine's border. Unlike in the spring, the build-up was sufficient in size and had all the requisite enablers to effect an invasion. This brought about a sense of crisis in the West, with frantic diplomatic engagement to understand Russia's concerns.

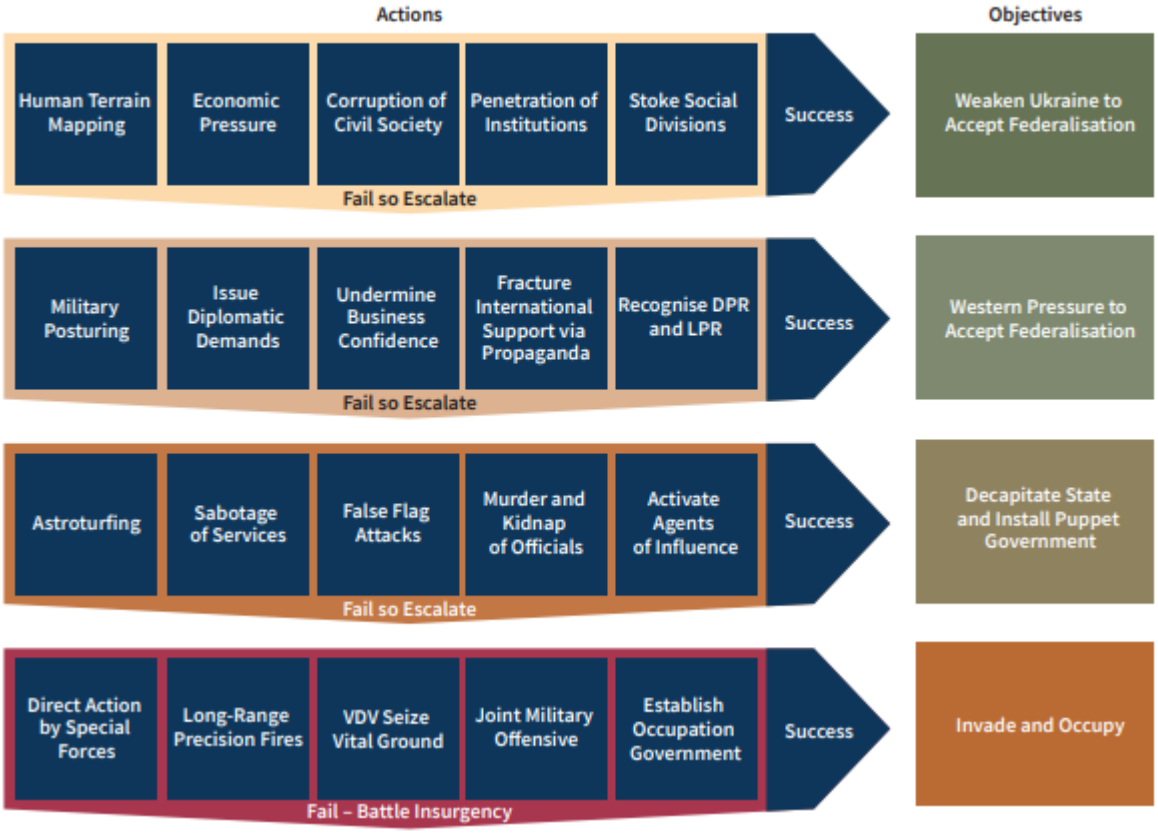
In Ukraine, meanwhile, the government started to observe disruption to its coal supply. After meetings with industrial leaders in the Kremlin, and instructions to Moscow's diplomatic posts in supplier countries, Ukraine noted a concerted effort to drive up energy prices over the winter. In the information space, Russian agents of influence began to attribute this rise to the incompetence of the Ukrainian authorities. The Ukrainian Security Service (SBU) began to track attempts to mobilise small business owners and civil society organisations to protest against the government's inability to stabilise the cost of living.

The energy axis of Russia's unconventional operations was detected early by Kyiv and measures were taken to try to control its impact. Ukrainian officials believe that they have succeeded in countering this initial thrust, though Russia could go much further. Energy was one of many axes by which Russia was and is trying to undermine the credibility of the Ukrainian government. The aspiration is to create a domestic political crisis that Russia can capitalise upon to bring politicians willing to reach an accommodation with Moscow to power. Using extensive social surveys of Ukrainian citizens, the Russian government has been working out which pressures lead to a domestic reaction and which do not.

This threat is exacerbated by the widespread penetration of Ukrainian politics and governmental institutions by agents of the Russian services, handled by both the FSB and the SVR. A network of around 30 personnel linked to the SVR have been involved in building financial mechanisms

for astroturfing protests, ballooning the size of demonstrations relating to energy tariffs, tax reforms and other legitimate concerns. Meeting with Ukrainian security officials there is a widespread acknowledgement that many of their colleagues – even in some quite senior positions – are working for or sympathetic to Russia.

Figure 2: Russia's Multiple Paths to Victory



Multiple Paths to Victory

Russia has consequently laid the groundwork to achieve victory along several paths and is pursuing all of them simultaneously. Indeed, the combined threat has fixed Ukraine because the measures best suited to countering one Russian path to victory are precisely those that would precipitate defeat on a different axis. If Ukraine mobilises to deter an invasion, Russia can destroy its economy and break the cohesion of the Ukrainian state. If the Ukrainians move to break up the networks eating their country from the inside, their government will be weakened and vulnerable to pressure from the West to accept the sacrifice of Ukrainian sovereignty. If the Ukrainian government remains steady, and the West holds firm in supporting Ukrainian sovereignty, then Russia may resort to invading the country and using its covert networks to enact systematic repression.

Countering these threats will not be achieved through a breakthrough diplomatic summit. Nor will the delivery of small quantities of military aid change the conventional balance of forces. It is entirely plausible that, in their erratic lack of focus, Western governments have lurched into crisis mode too late to have many meaningful options. If Ukraine survives the next month, however, then Western policy must be multi-layered and coherent. The first requirement is to bolster the Ukrainian armed forces, and in particular the equipping, training, and command and control for territorial defence, which is the best route to deny Moscow a viable path to a swift military victory. The key is asymmetric deterrence. There are also key systems that must be bolstered, most significantly air defence.

The second requirement is to support Ukraine's political stability. In the first instance, this requires economic stability and consequently the transition of Ukraine's dependence upon Russia for fuel and energy to Europe. There is also a need for safeguards to stabilise investment in Ukraine. Job security and preventing inflation are vital to both the government's ability to prevent domestic instability and to pay and retain soldiers, especially military specialists, trained at state expense with transferrable skills. There is clearly a legitimate concern about corruption when it comes to financial aid to Ukraine. However, the Ukrainian government cannot effectively tackle corruption while it is being systemically destabilised by Russia. Aid will therefore need to be carefully structured to ensure that it expands the capacity of the Ukrainian state.

[Russia's Hostile Measures: Combating Russian Gray Zone Aggression Against NATO in the Contact, Blunt, and Surge Layers of Competition]

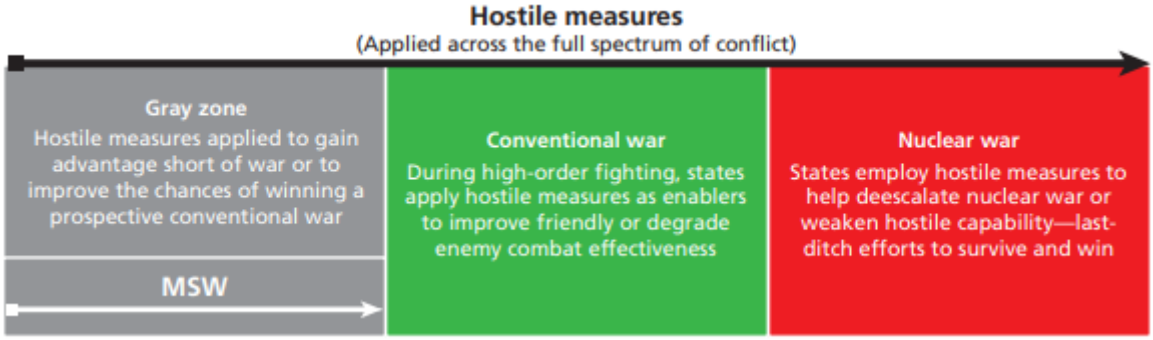
Ben Connable, Stephanie Young, Stephanie Pezard, Andrew Radin, Raphael S. Cohen, Katya Migacheva, James Sladden
RAND Corporation
5 January 2022

This article from RAND examines five states where Russia deployed "Gray Zone" tactics that expand upon what RUSI laid out as Russia's path to Ukraine in 2022. In four out of the five examples, the Russian government destabilized energy security as part of its strategy to gain ground just short of or prior to military incursion. In the country where energy insecurity was not part of the overall plan – Estonia – the Russian government still suspended its oil deliveries.

Select excerpts from the piece:

SOURCE: NATO, "NATO on the Map," webpage, undated.
NOTE: Russia is shaded red, including the Russian territory of Kaliningrad, located on the Baltic Sea along the northern Polish and southwestern Lithuanian borders. Russia forcibly annexed Crimea in 2014, but the Ukrainian government deemed this annexation illegal. Thus, we include Crimea as part of Ukraine. Kosovo is not affiliated with NATO but could be described as a NATO protectorate.

Russia's Gray Zone Threat The gray zone is not a specific defense and military challenge with well-defined parameters and boundaries. Instead, it is clear recognition of a universe of challenges lying in what amounts to a conceptual dead space in strategy development and strategic planning. This dead space exists from the highest levels of the U.S. national security community to deep into the Pentagon's strategy and planning process.
— Nathan P. Freier et al., Outplayed: Regaining Strategic Initiative in the Gray Zone



Patterns in Russian Hostile-Measures Behavior and Case Study Example

While Russia is adept at masking its tactical actions as they unfold, historical analysis reveals some consistencies in its contemporary approach. We drew these findings from our limited sample of five cases, our historical analysis, and our broader analysis of Russian behavior, cited throughout this report:

1. Russia consistently reacts with hostile measures when it perceives threats.

2. Both opportunism and reactionism drive Russian behavior.

3. Russian leaders issue a public warning before employing reactive hostile measures.

4. Short- and long-term measures are applied in mutually supporting combination.

5. Diplomatic, information, military, and economic means are used collectively.

6. Russia emphasizes information, economic, and diplomatic measures, in that order.

7. All arms of the government are used to apply hostile measures, often in concert

- Gray zone hostilities are nothing new, particularly for Russia.
- Russia will continue to apply these tactics, but its goals and means are limited.
- Deterring, preventing, or countering so-called gray zone behavior is difficult.

Map of Case Countries

Moldova

Russia's objectives in Moldova have been to maintain Russian influence and prevent the former Soviet republic from building strong alliances with the European Union and NATO. Russia's military presence in the frozen conflict over Transnistria allows it to threaten Moldova with internal destabilization and, possibly, territorial fragmentation. Moldova is highly dependent on Russia as an export market for its agricultural products, as a major source of foreign investment, as a job market for Moldovan workers, and as a provider of energy—particularly gas, which is needed to operate Moldovan electricity plantsRussia has operated a continuous, long-running hostile-measures campaign against Moldova. We traced a mix of nine short- and long-term hostile measures applied against Moldova.

8. manipulating energy supplies, including cuts to vital natural gas in winter

Russia has succeeded in executing hostile-measures tactics against Moldova for nearly three decades. However, this campaign of tactical successes has not generated strategic success. As of early 2019, Moldova was not on an official track toward NATO membership, but cooperation with NATO was improving.5 Moldova also increased trade with the EU to offset its trade losses with Russia, increased energy imports from the West to offset lost imports from Russia, and increased military cooperation with the West in at least partial reaction to a fear of Russian intervention. In 2014, Moldova and the EU signed a formal agreement aimed at improving both political and economic cooperation. If Russia's primary objective was to keep Moldova in its sphere of influence and to prevent a westward shift in Moldovan alliances, it has thus far failed. In fact, the entire long-running Russian hostile-measures operation appears to have backfired. Constant existential threats, economic punishment, vitriolic diplomacy, and insidious

manipulation of the Moldovan population were never matched by sufficient incentives that could have enticed Moldova's leaders or population in the opposite direction. In many ways, these results should have been foreseen. Russia might find ways to reverse this westward lean, but its efforts can best be described as a slow-burning, low-grade, and a mostly self-induced strategic failure

Georgia

Russia had four objectives in this case: (1) keeping Georgia within its sphere of influence and preventing its accession to NATO, (2) maintaining control over South Ossetia and Abkhazia, (3) discouraging European leaders from pursuing energy policies that would have reduced dependence on Russia, and (4) signaling a clear threat to other former Soviet states to keep them within the Russian sphere of influence.

We traced 12 Russian hostile measures in this case [including]:

1. pressuring the Georgian energy sector with price gouging and alleged sabotage

2. applying trade sanctions and undermining Georgian international trade

4. severing transportation and postal delivery services

10. conducting cyberattacks, specifically distributed denial of service attacks

Ukraine

8. increasing energy prices to squeeze the Ukrainian government

9. enacting economic embargoes and suspending free trade.

Turkey

4. enacting economic sanctions on food and natural resources

5. exerting pressure on the energy sector, including terminating collaborative projects

Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains
Matteo Crosignani, Marco Macchiavelli, and André F. Silva
Federal Reserve Bank of New York Staff Reports, no. 937
July 2020; revised July 2021

In 2017 malware delivered to a Ukrainian company's network expanded beyond Ukraine's borders, with billions of dollars in knock-on effects. This very technical article from the Federal Reserve Bank of New York attempts to truly calculate the scale of the damage. From over $1 billion in costs to firms directly affected by the hack to a visual of both upstream and downstream companies beyond the immediate attack, this historical case very clearly demonstrates how catastrophic cyberattacks in private companies – even outside the United States – can be.

Select excerpts from the piece:

More specifically, we examine the impact of the most damaging cyberattack in history so far (Greenberg, 2018, 2019). Named NotPetya, it was released on June 27, 2017 and targeted Ukrainian organizations in an effort by the Russian military intelligence to cripple Ukrainian critical infrastructure. The initial vector of infection was a software that the Ukrainian government required all vendors in the country to use for tax reporting purposes. When this software was hacked and the malware released, it spread across different companies, including large multinational firms through their Ukrainian subsidiaries. For instance, the shipping company Maersk had its entire operations coming to a halt, creating chaos at ports around the globe. A FedEx subsidiary was also affected, becoming unable to take and process orders. Manufacturing, research, and sales were halted at the pharmaceutical giant Merck, making it unable to supply vaccines to the Center for Disease Control and Prevention (CDC). Several other large companies (e.g., Mondelez, Reckitt Benckiser, Nuance, Beiersdorf) had their servers down and could not carry out essential activities.

First, we show that the halting of operations among the directly hit firms had a significant negative effect on the productive capacities of their customers around the world, which reported significantly lower profits. A conservative estimate implies a $7.3 billion loss by the affected customers, an amount four times larger than the losses reported by the firms directly hit by the cyberattack.

Second, we investigate the role of supply chain vulnerabilities in driving these effects. We find that the downstream disruption caused by the cyberattack is concentrated among customers that have fewer alternatives for the directly hit supplier. This result holds both when considering how many other suppliers a customer has in the same industry of the directly hit supplier, and when focusing on suppliers of less substitutable goods and services—that is, suppliers providing high-specificity inputs.

Third, we analyze in detail the role of banks in mitigating the negative liquidity effects of the cyberattack on affected customers.

Finally, we examine the dynamic supply chain response to the disruption caused by the cyberattack. We find that affected customers are more likely to form new trading relationships with firms in the same industry as the directly hit supplier after the shock. This result suggests that the disruption caused by the cyberattack served as a "wake-up call" for the affected customers which responded by finding alternative suppliers. We also find that the affected customers are more likely to end their trading relationship with the suppliers directly hit by the cyberattack, thus suggesting that the temporary disruptions caused by the cyberattack had long-lasting effects by eroding the reputation of the directly hit firms as reliable suppliers.

Firm Name	Costs	Additional Details
Beiersdorf Assets: $7.69 bln	$43 mln	Various locations of the Beiersdorf pharmaceutical group were cut off from mail traffic for days. Beiersdorf said 35 million euros worth of second quarter sales were delayed to the third quarter and it was totting up the costs of the attack for items such as calling in outside experts, promotions, and using other production sites to make up for shortfalls.
FedEx Assets: $33.07 bln	$400 mln	Delivery service FedEx lost $400 million after NotPetya crippled its European TNT Express business. The reported costs came from loss of revenue at TNT Express and costs to restore technology systems. Six weeks after the attack, customers were still experiencing service and invoicing delays, and TNT was still using manual processes in operations and customer service.
Maersk Assets: $68.84 bln	$300 mln	Maersk reinstalled 4,000 servers, 45,000 PCs, and 2,500 applications over ten days. The company only experienced a 20% drop in volume, while the remaining 80% of operations were handled manually. Losses were about $300 million, including loss of revenue, IT restoration costs, and extraordinary costs. The company was hiring 26 new employees a week, planning to have 4,500-5,000 IT employees within 18 months. At Maersk terminals in the Port of New York and New Jersey, computers, phones, and gate system shut down, forcing workers to use paper documents.
Merck Assets: $98.17 bln	$670 mln	At Merck, NotPetya temporarily disrupted manufacturing, research and sales operations, leaving the company unable to fulfill orders for certain products, including vaccines. The attack cost Merck about $670 million in 2017, including sales losses and manufacturing and remediation-related expenses.
Mondelez Assets: $66.82 bln	$180 mln	The global logistics chain of the food company Mondelez was disrupted by NotPetya. The forensic analysis and restoration of all IT networks cost $84 million. Added to this was the loss of sales. Altogether Mondelez had to record $180 million of damage by the attack.
Nuance Assets: $5.82 bln	$92 mln	NotPetya affected Nuance's cloud-based dictation and transcription services for hospitals. Nuance estimated a negative impact of $68 million in lost revenues and $24 million in restoration costs.
Reckitt Benckiser Assets: $24.19 bln	$117 mln	Reckitt Benckiser was hit by NotPetya, halting production, shipping and invoicing at a number of sites. The British consumer goods company suffered $117 million in losses, 1% of annual sales.
WPP Assets: $41.55 bln	$15 mln	UK multinational advertising firm WPP was hit by NotPetya, costing about $15 million before insurance. The damage was limited by the fact that WPP's systems are not fully integrated.

Table 1: Firms Directly Affected by NotPetya. Firms directly affected by NotPetya, total assets, total reported costs associated with NotPetya, and additional details. Sources: SEC Filings and Dow Jones Factiva.

Originated by Russian military intelligence to hit the Ukrainian economy, the virus also infected Ukrainian subsidiaries of international companies and spread to their global network infrastructure, thus forcing them to halt operations for several weeks. As a result, the customers of these directly hit firms recorded significantly lower profits relative to similar but unaffected firms.

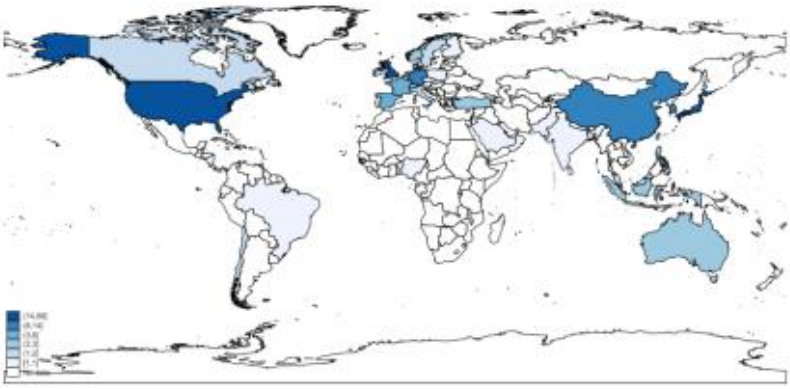


Figure A.3: Geographical Location of Affected Customers. This figure shows the geographical distribution of affected customers, i.e. customers of directly hit firms. Sources: Bvd Orbis, FactSet Revere.

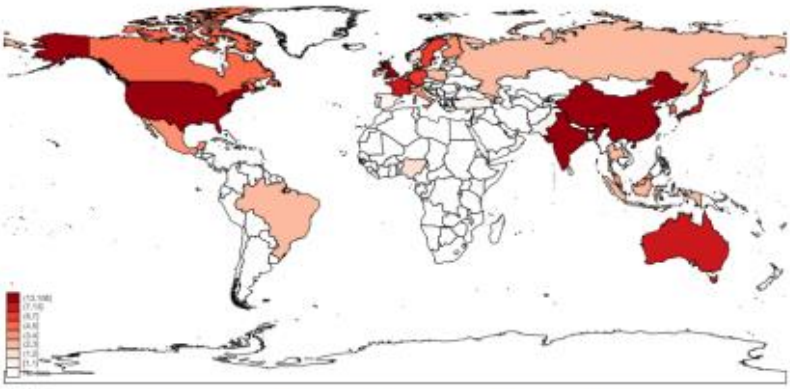


Figure A.4: Geographical Location of Affected Suppliers. This figure shows the geographical distribution of affected suppliers, i.e. suppliers of directly hit firms. Source: Orbis, FactSet.

We also document how the severity of the downstream disruption depended on the vulnerability of the supply chain. Specifically, we show that affected customers with fewer suppliers that can potentially substitute for the directly hit one experienced larger drops in profitability. This result highlights the importance of building more resilient supply chains to mitigate the effects of disruptive cyberattacks as well as other shocks, including the Covid-19 30 pandemic. Finally, we uncover evidence consistent with the fact that affected customers build new trading relationships with alternative suppliers immediately after the cyberattack and subsequently terminate relations with the suppliers responsible for the disruption in the medium-term.

Protected by SHIELDWATCH by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

- Software platform for on-demand supply chain risk assessments and financial intelligence data
- Analytical Support
- Business intelligence reports on critical suppliers