Friendly Cyber Fire: How Much Did NotPetya Cost Russia?

Description

In June 2017, a cyber attack spread malware across government, utilities, commercial, and financial websites across Ukraine and more than 60 other countries. In February 2018, the UK and US governments attributed the attack, since dubbed â??NotPetya,â?• as a Russian military operation. Itâ??s been called (perhaps hyperbolically) â??the most destructive and costly cyber-attack in history.â?• Even if thatâ??s not necessarily true, it generated an estimated economic loss of $10 billion worldwide. Less discussed is the impact of this attack on the attacker itself. Reports suggest NotPetya also caused some amount of self-harm to Russia , although there has been no effort to quantify the damage. Doing so can begin to fill a large and important gap in the scholarship on the risks of offensive cyber operations going awry.

â??Spilloverâ?• risk is the potential for the effects of offensive cyber operations to reach beyond their intended targets and cause harm to innocent or uninvolved states or even to the perpetrator of the attack. This spillover risk, particularly the potential of extensive economic harm, engenders some risk aversion regarding offensive cyber operations, despite operational experience suggesting that the unintended negative effects of such operations remain limited.

A deeper understanding of NotPetyaâ??s effect on Russia informs fears over spillover risk and collateral economic damage. Though we should exercise caution when extrapolating from a single case, NotPetya was the most significant cyber event since 2008 and therefore worth close consideration. The depth of data in the public domain on NotPetya has not been used to estimate the potential economic harm Russia caused to its own companies and using it for this purpose can inform both narrow decisions on offensive cyber operations and broader strategic thinking about cyber operations.

Limited Economic Effect of Cyber Attacks

The effectiveness of cyber remains the subject of intense debate. On one side, Nicolo Bussolati calls the â??digital weaponsâ?• available to smaller and less sophisticated actors â??cheap, powerful, and easy to use, to obtain, or to manufacture.â?• Lucas Kello believes that, although there has not been a cataclysmic impact from cyber weapons yet, the â??potential for doing so is widely recognized,â?• to

include the risk of fatalities. Increasingly, though, opponents of the historical view that cyber weapons are cheap, easy, and effective have become the standard. Max Smeets, who argues that cyber weapons are transitory in nature, describes them as â??short-livedâ?• and â??temporary.â?• Further, Aaron Brantly observes, â??Cyber capabilities are less attractive to non-state armed groups because their cost-to-impact ratio is less than kinetic violence.â?•

Although there is a belief that cyber weapons could cause harm (even death), their limited usefulness is more consistent with Brantlyâ??s view. The cyber warfare conducted in support of Russiaâ??s 2008 invasion of Georgia, for example, â??had little effect on conventional forces and were not decisive to the outcome of the conflict.â?• The accumulated cyber attacks that Ukraine endured from 2013 through 2020 may have resulted in economic harm of only approximately $720 million (including as much as $560 million in the single NotPetya attack).

Among the 24 major cyber catastrophes since 1998, only three offensive cyber operations have resulted in losses of $800 million or more: Yaha (India, 2002-3), WannaCry (North Korea, 2017), and NotPetya (Russia, 2017). Together, they account for approximately $40 billion in inflation-adjusted economic loss, with half of that attributable to Yaha. The detailed reporting on NotPetya makes it uniquely useful in studying the effects of cyber operations, including spillover and self-harm.

NotPetyaâ??s Round Trip

Estimating the effect of NotPetya is difficult because there are no databases or research studies pulling specific economic impacts into one place. Publicly available information from media reports, cyber security analysts, and the insurance industry provide a reasonably reliable starting point. However, further assessing the economic effects of the attack on Russia comes with further complications. Itâ??s necessary to consider Russiaâ??s motivation for the disclosures made on NotPetyaâ??s effects.

Neither denying nor amplifying its effect brings Russia any significant advantage. If it were politically expedient to claim that Russia was not significantly impacted, then it would undermine its potential claim of victimhood (which Russia used to deny it was the aggressor). Conversely, if it were politically expedient to claim significant effect, the narrative could be undermined by trading activity with foreign partners.

Of the estimated $10 billion in NotPetyaâ??s economic impact, Ukraine accounts for up to $560 million, and insurance data reveals another $1.7 billion that can be traced to Merck ($1.4 billion in property insurance and $275 million in cyber insurance), and $1.3 billion across St Gobain, Mondelez, Reckitt Benkeiser, Nuance Communications, and others. That brings the total to $3.6 billion. Publicly available economic loss data shows that logistics firms Maersk and FedEx/TNT sustained economic impacts of

$300 million and $1 billion, respectively, bringing the tally to $4.9 billion. Many more companies have been named as NotPetya victims but do not have publicly reported economic loss estimates, forcing the assumption that their economic losses were minimal. Large publicly traded companies or public entities with material impacts would have been likely to disclose estimated impacts through the course of their reporting obligations.

With nearly half of the economic effect of NotPetya accounted for, it becomes easier to understand how much of the balance may have affected Russia. The countryâ??s victims include prominent companies like Sberbank and Rosneft along with others like Home Credit and Invitro.

A fuller estimate can be derived by starting with Group-IBâ??s identification of 80 total victimized companies in Russia and Ukraine and then assigning 75 percent to Ukraine, based on ESETâ??s finding that Ukraine accounted for 75 percent of NotPetya infections. This produces an estimate of around 60 Ukrainian victims, leaving 20 of the 80 still to be accounted for. With 10 victims in Russia already known, simply doubling the count may be methodologically ugly, but itâ??s likely to be at least indicative.

Other clues are helpful. For example, Russia reportedly sustained $1.85 billion in economic harm from cyber attacks in 2017, a year that included not just NotPetya but also WannaCry and Bad Rabbit, both of which hit Russia hard. While the yearâ??s economic loss from cyber attacks may seem large, it represents only 0.12% of Russiaâ??s 2017 $1.57 trillion GDP. Even in aggregate, this still remains well below a severity threshold of 0.2 to 2.0% of GDP for a single event proposed by insurance scholars.

Finally, the ability of Russian victims to operate was not severely impaired. Rosneft was able to keep the oil flowing, and Sberbank had become cyber-savvy following a history of attacks. The other victims were not reported to have had any serious impairment to operations, a sign of manageability when impact could fuel grievance. Thus, estimating economic impact requires some creativity.

Western Victims as Proxy

Using the economic impacts of NotPetya on Maersk and Merck to try to gauge what happened to Sberbank and Rosneft may seem inherently problematic. The companies are not from comparable sectors or business environments. However, there are enough similarities for this comparison to be useful. The lack of operational impairment to the two Russian companies speaks for itself regarding economic impact. While the economic effects to Maersk and Merck were indeed likely much larger than those to Sberbank and Rosneft, they were still small when considered as a percentage of company revenue.

Maerskâ??s 2017 revenues were $31 billion, which puts the impact of NotPetya at 1%. Merckâ??s revenues were $40.1 billion, and the impact of NotPetya looks like 5%, but the companyâ??s disclosed $260 million economic impact is presumably net of the insurance recoveries. That brings the effect down to 0.65% of revenues. The result is a range of 0.65 to 1% to apply to Russiaâ??s victims of NotPetya.

Rosneftâ??s 2017 revenues were $106 billion, with Sberbank at $35.4 billion. Applying the factors from Maersk and Merck, the impact to Rosneft would be approximately $650 million to $1 billion, and Sberbankâ??s economic loss would range from $230 to 400 million. But there is a key difference between the experiences of Maersk and Merck relative to those of Rosneft and Sberbank. The former sustained impacts to their core operations, while the latter did not. Consequently, the losses for Rosneft and Sberbank would have to be a fraction of the $880 million to $1.4 billion (combined) above.

Itâ??s difficult to determine what the right fraction of the $880 million-to-$1.4 billion range should be, and any choice would seem arbitrary. However, even an arbitrary choice is tolerable as long as it is high enough to show that the impact isnâ??t being kept intentionally low. Further, for a factor that is conservatively high, applying it to the $880 million-to-$1.4 billion range should still result in an estimate for Rosneft and Sberbank that is still quite small in comparison to the $1.85 billion in economic losses from cyber in 2017, let alone the full $10 billion impact of NotPetya or Russiaâ??s 2017 GDP. A 20% proportionality approximation serves this criteria and provides a ballpark estimate. While taking 20% of $880 million could be overinflation, the impact to Russia is still small. An aggregate impact of $180 million means that Rosneft and Sberbank would share 9.7% of Russiaâ??s $1.85 billion in economic losses from cyber attacks in 2017, which is plausible given the extent of cyber activity against Russian companies that year.

Next, we return to the additional 18 Russian victims separate from Rosneft and Sberbank. Western losses again serve as a guide. Merck, Maersk, St Gobain, and FedEx/TNT represent $3.6 billion in economic loss from NotPetya, as shown earlier in this articleâ??comprising 73.5% of the known $4.9 billion discussed earlier. If that proportion is applied to the economic effects of NotPetya in Russia, then the $180 million sustained by Sberbank and Rosneft would imply a total impact to Russia of $245 million. The $65 million left to be allocated amounts to approximately $3.6 million per company.

Given the nature of the analysis, it is natural to question whether the result underrepresents the impact of NotPetya on Russia. Stressing the model by simply tripling the results above yields an economic impact of $735 million, which strains credulity by leaving only $1.1 billion for WannaCry and BadRabbit from the yearâ??s $1.85 billion. Yet, even at that implausible level, the GDP impact of 0.047% would still fall far below the 0.2% materiality threshold.

Is it Worth Crying Over Spilt Cyber?

As a spillover and self-harm concern, NotPetya was the closest weâ??ve come to a worst-case scenario. Russia attacked itself alongside companies in NATO countries. Yet the total effect of $10 billion was easily absorbed around the world, from nearly $2 billion to Merck to $560 million to Ukraine to perhaps $245 million to Russia. The fact that no meaningful publicly visible response followed from the victims outside the Russia-Ukraine conflict speaks to the lack of impact. This suggests that itâ??s time to revisit the taboo on offensive cyber operations within the context of potential spillover.

After all, the numbers above are clear: NotPetyaâ??s spillover in Russia did not reach material levels of economic effect and thus would not be enough to change their strategic calculus. Although itâ??s difficult to extrapolate this lesson into broader policy, the highest-profile case of self-harm from offensive cyber operations suggests the need for a new lens when examining this problem. The evidence available suggests that the prospect of cataclysmic self-harm is unlikely. The numbers are just too small relative to the overall economic harm caused by NotPetyaâ??and the damage caused by it was still relatively small on a broader economic basis. The risks associated with offensive cyber operations should be respected, but within context. Letâ??s not let a misunderstanding of past events constrain the future utility of offensive cyber operations.

Tom Johansmeyer is co-lead of the Economic and Legal Warfare Project and editor-in-chief of the Journal of Strategic Competition. Heâ??s a PhD candidate in international conflict analysis at the University of Kent, Canterbury, where he is researching the cyber insurance protection gap as an economic security problem. Tom is also a reinsurance broker in Bermuda, focusing on alternative forms of risk transfer in developing markets for emerging risks.

Main image generated by ChatGPT using DALLÂ·E, OpenAI (March 2026)

Date Created
2026/03/20