Cyber Attacks in Perspective: Cutting Through the Hyperbole

Description

This article is part of Project Cyber, which explores and characterizes the myriad threats facing the United States and its allies in cyberspace, the information environment, and conventional and irregular spaces. Please contact us if you would like to propose an article, podcast, or event environment. We invite you to contribute to the discussion, explore the difficult questions, and help.

What would the most destructive and costly cyberattack in history look like?

The Department of the Treasury is exploring a federal mechanism for providing relief capital to the insurance industry in the event of a major cyber catastrophe. While the prospect of a cyber incident sinking the insurance industry and leaving society exposed is intensely remote, it highlights an underlying problem with our understanding of the destructive capacity of cyberattacksâ??hyperbole. If the terror attacks of September 11, 2001, represented a failure of imagination, then the fear we have of a significant cyberattack represents a failure to keep our imaginations under control.

History shows that it is easier to imagine a catastrophe than to produce it, but it fails to explain why. The last twenty-five years of economic loss data suggest cyberattacks arenâ??t nearly as costly as the annual hurricanes and hailstorms we experience.

https://irregularwarfareinsider.podbean.com/

So why are we so afraid?

In many ways, our fear can be attributed to the relative newness of cyber risks in human history, meaning they need to be better understood by the public and with many precedents. Additionally, our misunderstanding is related to the thin historical data we have on them and, more critically, that our historical data relies heavily on a few specific, recent casesâ??the most prominent being the 2017 NotPetya attack. With a $10 billion price tag and impacts across 65 countries,NotPetya was called â??the most destructive and costly cyberattack in history.â?• But the numbers tell a different story, and relying on NotPetya as our catastrophic example may mean researchers and analysts are staring down a paper tiger.

By exaggerating the effects of past attacks and framing them as but a taste of whatâ??s to come, the cyber domain inspires fear in policy-makers, commanders, and the general public that is normally reserved for the most severe forms of kinetic warfare, such as nuclear strikes. As a result, cyber capabilities have become difficult tools to use, simply due to a fear that has not materialized which is based on hyperbolic claims. A misguided belief in their destructive power has effectively stifled innovation at all echelonsâ??despite plenty of research suggesting the contrary. If there were ever a time for a hard reset on how cyber operations and their implications are perceived, this is it. If anything, cyber operations have proved to be de-escalatory, and by perpetuating a myth to the contrary, we lose access to an important alternative to traditional war. By setting the record on cyber straight, we take a step toward making the world a safer place.

How it started

NotPetya was born of war. Released three years after the start of hostilities in eastern Ukraine in 2014, NotPetya was one of several efforts by Russia to attack Ukraine in cyberspace. From 2014-2016, other Russian cyberattacks were operationally successful but often fell short of their desired impact. For example, the 2015 attack on the Ukrainian power grid is among the most effective attacks against an energy infrastructure. Still, only 230,000 people lost power for six hoursâ??far short of what even a minor hurricane routinely achieves.

What happened in 2017 was different. A tool developed by the Russian defense intelligence agency (GRU), NotPetya, was deployed after GRU hackers gained access to the servers of a small Ukrainian software company. The exploit relied on a Windows vulnerability and was embedded into the companyâ??s software products, like the Ukrainian accounting software MeDoc, and intended to cause damage to large swaths of the Ukrainian economy. Made to look like its ransomware predecessor, Petya, NotPetya locked the systems it encountered and demanded a $300 payment. However, the ransomware â??faceâ?• of NotPetya was another case of maskirovkaâ??the attackers had little interest in collecting ransom payments but instead used the feature to confuse forensic analysts, making it harder for them to divine who was behind the attack.

Although NotPetya has been attributed to Russiaâ??s GRU, the code was derived from a leaked National Security Agency (NSA) tool called EternalBlue. A proverbial skeleton key of an exploit, EternalBlue, was used as part of the 2010 Stuxnetattack on the Natanz nuclear facility. After the tool was leaked, it was used in both the WannaCry and NotPetya attacks during the first half of 2017 and later in BadRabbit. Throughout 2017, therefore, waves of attack came with â??roots [that] can be traced to the US.â?• The impact of those attacks underscores why the NSA sustained heavy criticism over hoarding zero-day vulnerabilities and developing powerful cyber tools that can be difficult to control. And itâ??s easy to see why.

NotPetya quickly spread beyond Ukraine to cause an estimated $10 billion in economic damage worldwide. The United States, France, Denmark, and Germany were among the 65 countries affected. The attackâ??s costs mounted quickly. According to its two insurance policies, pharmaceutical company Merck sustained nearly $2 billion in damage. Maersklost $300 million, and the newly merged FedEx/TNT lost roughly $1 billion. The insurance industry experienced nearly $3 billion in losses, indicative of the attackâ??s scale.

Meanwhile, the effects on NotPetyaâ??s intended targets were far more modest. NotPetya is estimated to have impaired 0.5% of Ukraineâ??s gross domestic product (GDP). That amounts to $560 million, a significant but manageable cost.

Further, in a twist of poetic justice, Russia also fell victim to NotPetya. After losing control of the malware, two of Russiaâ??s largest companies, the energy company Rosneft and the financial institution Sberbank, joined several Russian companies, including banks, travel agencies, and telecommunications providers, on NotPetyaâ??s list of victims. Although the source of the list of Russian victims is suspect (as a blog post comment that looks like it came from a troll farm), the effects on several of the named Russian companies are reported elsewhereâ??including The Independent, cyber security firm Group-IB, and of course TASS.

Context is crucial

The global impact of NotPetya led the U.S. government to call it â??the most destructive and costly cyberattack in history.â?• The declaration has since been amplified across the popular and academic press, cementing NotPetyaâ??s place at the top of â??most destructive cyberattackâ?• lists and ingraining it into the still-early study of â??cyber catastrophes.â?• The result is that NotPetyaâ??s prominence in the literature has skewed our understanding of the threats associated with cyberattacks.

Based on my calculations and categorization, there have been 21 cyber catastrophes since 1998 and up to $310.4 billionin losses, adjusted for inflation. And among them, NotPetya is not the worst. Sure, the attack was significant, but adjusted for inflation, its $11.9 billion price tag is roughly 30% below the 25-year average for cyber catastrophe economic impacts.

When the U.S. government announced NotPetya as â??the most destructive and costly cyber-attack in history,â?• it kicked off a narrative disconnected from the reality of NotPetya and our understanding of catastrophic cyber events. Everyoneâ??researchers, scholars, security professionals, journalists â?¦ etc. â??heard â??the most destructiveâ?• and ran with it. There are several reasons why.

Cyber warfareâ??and cyber operations conducted by nation-state actorsâ??are already shrouded in hyperbole. Whether you look at the 2015 attack mentioned above on the Ukrainian power grid or turn to the more recent cyber activity that preceded the 2022 invasion of Ukraine (and persisted after), the answer is the same. Cyber weapons, in practice, are more bark than bite. And itâ??s not just Russia. Operation Glowing Symphony offers a rare case of the US military confirming its offensive cyber operations against ISIS targets online. The operation was an interesting, clever, and successful case of offensive cyber activity until the offense stopped. In the end, cyber operations are most impactful when prosecuted, but their effects taper over time, and recovery and reconstitution often come quickly after an operation is finished.

None of this makes for great storytelling, but great stories about cyberattacks do existâ??take Cliff Stollâ??s *Cuckooâ??s Egg*, for exampleâ??but they also rely heavily on exaggeration and hyperbole to describe cyber threats and impacts. Part of this is simply reader engagementâ??cyber or otherwise. Everyone loves a bit of excitement, and the real-world implications of cyberattacks, real or imagined, get your heart pumping.

The NotPetya storyâ??rather than the NotPetya attackâ??is revealing. In late 2018, *Wired* Magazine published â??The Untold Story of NotPetya, the Most Devastating Cyberattack in History,â?• which bakes hyperbole into the headline and never lets up. Throughout the piece, the author amplifies complex issues with nuance and considerable finesse to give a true-crime story feel. In many ways, reporting on cyberattacks reflects how reporting on bullets and bombs is more accessible than reporting on bits and bytes the human eye canâ??t see. Incorporating exaggeration and hyperbole makes a story interesting.

The *Wired* article has gone on to feed academic journal articles and news stories worldwide. In many ways, the article did not contribute to the NotPetya narrative but became it. The article also amplified the original 2018 White House announcement about NotPetya, further entrenching the hyperbolic interpretation of the attack into the public psyche.

A more context-appropriate reading of the 2018 White House announcement would convey that NotPetya was an attack of global importance worthy of the â??international consequencesâ?• that followed, including sanctions and indictments. NotPetya was undoubtedly the costliest single cyberattack in more than a decade, and to date, it was the last cyber catastrophe event to exceed even $1 billion. The fact that NotPetya fails to live up to the exaggerated claim of being the costliest cyberattack in history does not diminish its importance, and a context-appropriate reading of the 2018 announcement would still drive that message home.

The lesson

The NotPetya attack is an excellent example of why words matter. At face value, calling NotPetya â??the most destructiveâ?• cyberattack set a benchmark for how we think about future cyberattacks on US systems *and* how policy-makers think about future cyber operations against adversary systems. It categorized the nexus of economic security and cyber catastrophe risk into a false and misleading model, which could lead to years of missed opportunities to refine how the US researches, develops, and employs offensive and defensive cyber capabilities.

Understanding the accurate scale of NotPetya (and the broader history of economic losses from cyberattacks) will help to reset expectations and breathe new life into cyber operations at all echelons simply by giving a relatable sense of the destruction caused. This only works for the set of targets, though, where the economic impact is the consequence. Not all attacks are about money.

Nation-states are also highly vulnerable to cyber espionage, theft of intellectual property, and other efforts to gain and use private information. Events like the SolarWinds cyberattack have shown the significant societal implications of espionage. SolarWinds exploited a vulnerability in the Orion network management system, which is used by nearly 30,000 public and private organizationsâ??including local, state, and federal agencies to manage their IT resources. Despite having devastating national security implications for SolarWinds, the total economic impact fell short of $200 million, making it more than 90% smaller than the Equifax breach alone. Nonetheless, the attack caused a loss of trust in government-run cybersecurity effortsâ??an essential national and societal security impact.

Because of measures like â??loss of trust,â?• itâ??s difficult to estimate the total cost of cyber espionage campaigns. While itâ??s prudent to make â??economic impactâ?• one measure among a collection of measures used to gauge the severity of a cyberattack, non-financial implications must be contemplated, too.

Why this matters for US military cyber operations

The enduring lesson of NotPetya and the US governmentâ??s public statements about the attack is straightforward: hyperbole constrains military cyber operations. Overstating NotPetyaâ??s impact adds to the â??cyber Pearl Harborâ?• myth and fosters a misguided understanding of offensive cyber capabilities as decisive weapons of mass destruction. Helping the public (and government stakeholders) understand how cyber operations can beâ??and have beenâ??used for de-escalation will not only reduce the temperature of cyber fears but could provide new flexibility in a domain of limited action. Despite the expanded authorities granted to US Cyber Command in the 2018 NDAA, offensive cyber operations continue to be constrained by the mistaken belief that cyberattacks will precipitate an escalation ladder similar to nuclear strikes. However, research continues to demonstrate otherwise.

Unfortunately, operational use of the cyber domain is also impeded by relatability. We understand concepts like â??lethality.â?• When I walked through Sarajevo a few years ago, its 30-year-old battle scars possessed intuitive meaningâ??I could *see* the impact of war. A similar, tangible representation of cost or loss doesnâ??t exist for cyberspace operations. Therefore, without something concrete to touch, see, feel, or see, an aura of novelty remains around cyberattacks and cyberspace operations that leave the door open to storytelling and hyperboleâ??with it, the exaggerated claims that make for a click-able headline. The first step, therefore, is presenting a clear and accurate representation of the damage caused by past cyberattacks.

In addition to improving our reporting on cyber operationsâ?? impacts and data collection efforts, we must find ways to make cyberspace more relatable. While a good story can solve the relatability problem when it is accurate, inflated accounts and hyperbole only give commanders and policymakers pause. Whether by comparing the damage caused by cyberattacks to natural disasters (which are much worse) or to the effects of kinetic warfare (also much worse), providing reference points for understanding the consequences of cyberattacks is long overdue for what was identified as a domain of warfare back in 1993. Analogous impacts on other domains may be imperfect. Still, they offer a first step toward eventually making the impacts of cyberattacks as intuitively relatable as bomb craters and war ruins.

Moving forward, researchers, journalists, government officials, and the public need to recognize how hyperbole is shaping the discussion about cyberattacks. Even seemingly gold-standard sources benefit from healthy skepticism and a grain of salt. Doing so could lead to a shift in US cyber strategy by enabling a more accurate assessment of risk and allowing for more aggressive pursuit of malicious cyber actors around the globe without the risk of escalation more common in traditional warfare.

Tom Johansmeyer is a Ph.D. candidate at the School of Politics and International Relations at the University of Kent, Canterbury, researching the role of insurance at the nexus of cyber and economic security.

The views expressed are those of the author(s) and do not reflect the official position of the Irregular Warfare Initiative, Princeton Universityâ??s Empirical Studies of Conflict Project, the Modern War Institute at West Point, or the United States Government.

Main Image: Screenshot of the splash screen of the payload of the original version of Petya. (Unknown via Wikimedia)

If you value reading the Irregular Warfare Initiative, please consider supporting our work. And for the best gear, check out the IWI store for mugs, coasters, apparel, and other items.

Date Created

2024/06/25