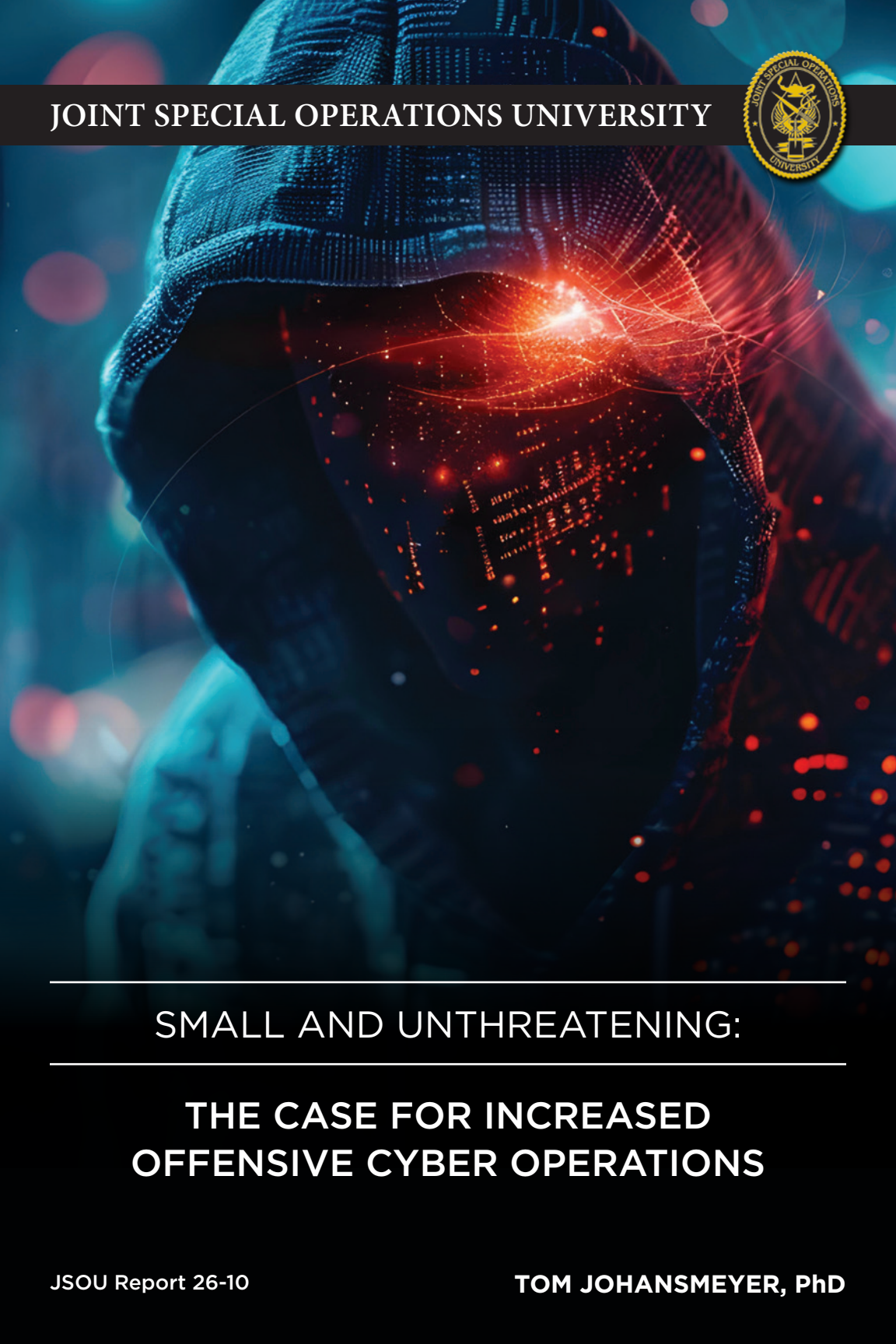


JOINT SPECIAL OPERATIONS UNIVERSITY

SMALL AND UNTHREATENING:

THE CASE FOR INCREASED OFFENSIVE CYBER OPERATIONS

JSOU Report 26-10

TOM JOHANSMEYER, PhD

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

SMALL AND UNTHREATENING:

The Case for Increased Offensive Cyber Operations

TOM JOHANSMEYER, PhD

JOINT SPECIAL OPERATIONS UNIVERSITY
MacDill Air Force Base, Florida | August 2026

JSOU Report 26-10

On the cover: Beyond the fear of the unknown lies a unique opportunity for U.S. strategic advantage. A deep dive into major state-actor attacks reveals that the "cyber taboo" may be holding back military potential. By moving past the stigma, leaders can embrace offensive cyber tools as a transitory, potentially de-escalatory alternative to traditional kinetic weapons. (AI-generated Adobe Stock image by Anastasiia)

Binary watermark design by Magnific. www.magnific.com

JSOU PRESS

Melanie Casey, Editor in Chief
Beth DeGeorge, Editor
Alina Alvarez Perez, Editor
Arianna Czesler, Designer
Rebecca Kurk, Designer

This work was cleared for public release; distribution is unlimited.

Published August 2026

ISBN 978-1-941715-87-1

jsou.edu/press

Table of Contents

About the Author

TOM JOHANSMEYER, PhD, co-leads the Economic and Legal Warfare project at the Irregular Warfare Initiative. He has a doctorate degree in international conflict analysis from the University of Kent, Canterbury, where he researched the role of insurance in economic and cybersecurity strategy. He is also a reinsurance broker based in Bermuda, where he focuses on alternative forms of risk transfer.

Abstract

The stigma associated with offensive cyber operations should be retired, as should attributing it to the fear of the unknown. The following research reviews the economic consequences of three major cyberattacks by state actors that are among the most economically impactful cyber catastrophe events in history to determine the extent to which unintended damage, long a cyber operations taboo, had any meaningful effect. A review of these three cases—Yaha, WannaCry, and NotPetya—shows that the potential impact of cyber operations is much smaller than previously feared, allowing for military leaders to get past the stigma associated with this form of engagement. Given the transitory nature of cyber weapons, the increased use of offensive cyber operations may in fact be de-escalatory, obviating the need for traditional weapons in some cases. The result is a unique opportunity to advance U.S. capabilities in irregular warfare through the improved use of cyber capabilities within the special operations environment

Introduction

Some have contended that cyber operations are packed with cataclysmic potential and a high risk of unintended consequences. From "[p]olicymaker skittishness" to "hyperbolic narratives" and inflammatory language, it is easy to see why the advocates for offensive cyber operations "struggle against a visceral discomfort" in those who do not.[1] Even though cyber operations have not led to vast unintended consequences with subsequent escalation, the threat of such a situation tends to be couched in the word "yet,"[2] as if to say that the arrival of profound cyber catastrophe is merely a matter of time. The view that a "war in the wires"[3] is on the horizon seems impossible to shake, and this has translated to a stigma associated with cyber operations—with public perception a major factor.[4] The notion that too much can go wrong too quickly has cost military leadership an important, useful, and de-escalatory form of irregular warfare (IW).

The notion that too much can go wrong too quickly has cost military leadership an important, useful, and de-escalatory form of irregular warfare.

Is the use of cyber operations unnecessarily constrained by the belief that it could cause too much harm, intentionally or otherwise? The question looks specifically at what has been called "spillover" risk[5]—i.e., the concern that a cyberattack can lead to unintended victims outside the intended target—also known as "cyber collateral damage."[6] This includes the risk that such spillover could lead to engagement by those inadvertently attacked or other forms of escalation. The probing of this question focuses on cyber operations intended to cause impact to the target, with that impact measured in economic form, given that loss of life and property damage have been thin at best, if present at all.[7] Given that the damage caused by cyber

weapons is seen as transitory and reversible, there could be significant benefit in removing the stigma and increasing the use of offensive cyber operations.

Cyberwar has not been prosecuted to profound effect,[8] and the consequences of cyber catastrophes in general (used as a proxy for war, absent the effective use of cyberwar) have been extremely limited.[9] However, the stigma has persisted, and it is time for that to change. Debunking the perception that cyber operations are potentially catastrophic—specifically by analyzing the economic harm caused by past events—challenges the belief that such weapons are inherently uncontrollable. This reassessment suggests cyber or kinetic retaliation in response to unintended impacts is not necessarily inevitable. Evidence of past economic experience provides a foundation for suggesting the increased use of cyber operations as an alternative to other forms of coercive statecraft or military activity.

There is no centralized U.S. agency or department tasked with analyzing and projecting the consequences of a cyberattack.

Simply put, the taboo associated with offensive cyber operations—because they could cause vast unintended consequences leading to diplomatic or military reprisals—is a dated concept that impedes the use of cyber capabilities to productive effect in statecraft and as an alternative to kinetic operations.[10] In reality, there is no centralized U.S. agency or department tasked with analyzing and projecting the consequences of a cyberattack.[11] Further, there is evidence that the unintended effects have been generalized and frequently overstated.[12] That said, cyber operations can be an effective tool to engage in IW activities against adversaries—or to supplement a broader military and diplomatic engagement. Because of this, even though "special operations and cyber operations may seem worlds apart from each other,"[13] there are "missions that span the gap between peacetime and war."[14]

Rather than shy away from cyber operations, states should contemplate using them more frequently to accomplish their diplomatic and military objectives without having to resort to more coercive tactics that may lead to dangerous consequences. The use of cyber operations to drive disproportionate outcomes through asymmetric and IW integrates closely into the special operations forces (SOF) toolkit as "ODAs also have an unparalleled capacity to integrate cyber and space assets with on-the-ground networks."[15]

Historical Context

What was offered with alarmism in 1993 was reduced to a whimper 20 years later. As conceived in the early days of the commercial Internet, cyberwar was believed to have the potential to affect vast worldwide physical and economic carnage through a few keystrokes. The original thinkers on this subject, John Arquilla and David Ronfeldt,[16] deemed cyberwar "likely"[17] and claimed that it "may be to the 21st century what blitzkrieg was to the 20th century."[18] They explained in great detail the subtle differences between 'netwar' (societal) and 'cyberwar' (military),[19] the historical context behind both, and the potential future implications of this "military technology revolution."[20]

The common cyberwar narrative often relies on hyperbolic imagery to suggest a level of physical and economic carnage that has never materialized in reality. Empirical data reveals that most economic impact from cyber events actually occurred before 2008, with modern state-actor operations like WannaCry and NotPetya resulting in manageable losses that pale in comparison to natural disasters. (Adobe Stock image by beebright)

Of course, the presumed godfathers of cyberwar had little in the way of experience and empirical evidence available to them, and historical analogies can only be stretched so far—a problem recognized for cyberwar in particular.[21] Without direct precedent, the use of non-war cyber catastrophe events becomes an effective proxy—a proxy and practice which necessarily continues through today for the same reasons (i.e., a lack of relevant precedent). For this, the "Morris Worm" is useful.[22] The 1988 cyberattack, of sorts, was really "an experiment gone awry," in which a graduate student at Cornell University crashed 10 percent of the world's internet-connected computers (approximately 6,000).[23] The worm's author, Robert Tappan Morris, became the first person "criminally convicted under the Computer Fraud and Abuse Act,"[24] resulting in 400 hours of community service and fines exceeding $10,000. If not directly inspired by the Morris Worm only five years earlier, the strategic environment contemplated by Arquilla and Ronfeldt is at least consistent with it. The rapid transmission of warlike activity via the cyber domain was virtually assured, with "combat waged fast and from afar,"[25] and little in the way to impede the onward march of goose-stepping bits and bytes. However, this was never going to be the case.

The free flow of chaos experienced with the Morris Worm—which caused both "military and university functions" to slow "to a crawl"[26] — was a function of its era, where the internet was small, new, and limited to a niche cadre of users. Since then, the effects of broad cyberattacks have fallen, at least as evident from an analysis of the economic effects of cyber catastrophe, which have 92.7 percent of economic losses from such events from 1998–2024 occurring before 2008.[27]

Before 1998, though, the amount of activity (economic or otherwise) resident on the internet remained small, despite the rapid expansion of the internet into businesses and homes. From being able to 'communicate at-will with 10 million people all over the world' in 1993 to 24 million in the U.S. and Canada alone by 1995, fast growth came on a small base.[28] By 1999, internet activity in the U.S. could be measured in economic terms, rather than just by users, and it accounted for hundreds of billions of dollars.[29] The internet had

become big, important, penetrated, and familiar enough to represent a budding domain of operations, but it was still sufficiently small that potential distant future effects would remain more disconcerting than possible near-term impacts. Further, internet-related growth and prosperity came at a unique time in the international relations environment. Both the fall of the Berlin Wall (1989) and the dissolution of the Soviet Union (1993) led to a decade of U.S./western unipolarity,[30] limiting the likelihood that views on the nature and effectiveness of cyberwar would be tested. That would have to wait for Russia to reconstitute as a regional power.

RUSSIA WITHOUT RESULTS

The first signs of conflict via the cyber domain appear to have arisen in 2007 and 2008: Russia's cyberattacks on Tallin, Estonia, in 2007 have been described as the "first known cyber-attack on an entire country," and thus arguably, the first true attempt at cyberwar.[31] The claim offers more bravado than analysis. A NATO assessment observes "significant disruption, cost, and embarrassment" from the attacks and laments that "citizens who had enthusiastically adopted internet services were unable to access them reliably."[32] However, this perspective comes without any meaningful indication of scale. Perhaps more important is that the effects of the cyberattacks did not last nearly as long as NATO's response. After all, NATO used the 2007 event as the impetus to commit to cyber and launch the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn.[33]

Further attempts by Russia to exert its will across the former Soviet bloc via the cyber domain were similarly ineffective. In 2008, Russia integrated cyber operations into its invasion of Georgia, although the consensus is that those operations had almost no strategic impact.[34] The same was true of Russian attempts to engage in acts of cyberwarfare in Ukraine following its 2014 invasion. Finally, the 2022 invasion of Ukraine was expected to be the defining moment for cyberwar,[35] 30 years in the making, yet reality failed to deliver on those expectations.[36] The revolution expected in 1993 thus was tested in 2007 and had fizzled in all practical senses by 2022.

THE CURRENT STATE OF CYBERWAR

Against the backdrop of attempted cyberwar in the former Soviet bloc, it should come as no surprise that the next wave of scholarship on cyberwar was decidedly different from what had preceded it. Thomas Rid famously proclaimed in 2012 that the "[c]yber war will not take place!"[37] Anchored in the Clausewitzian tradition, in which war represents a continuation of politics by other means,[38] with those means violent and focused on a specific end result,[39] Rid's views note the inability of cyberattacks to cause the non-metaphorical violence specified by Clausewitz. Although Rid's claims that cyberattacks cannot destroy a building or cause loss of life[40] were later challenged,[41] the limited instances in which such losses occurred have served to demonstrate the inability of cyberattacks to scale as a destructive force. The cyberwar, it seems, really will not take place, as Rid claims. In fact, the limited capabilities of cyber weapons, operations, and war have become the focus of increasing scholarly attention.

For example, James Lewis explains, "A cyberattack is not a nuclear weapon, and it is intellectually lazy to equate them to nuclear weapons," adding that it "is easier to imagine a cyber catastrophe than to produce it."[42] The classical belief that cyber can be "everything, everywhere, all at once"[43] is more hype than reality, and the notion that widespread damage can be caused via cyber operations in a short span of time is not only unrealistic, as Lewis observes, but utterly without past impact. This is evidenced not just by Russia's experience but also in a review of the limited economic effects of attempted acts of cyberwar and non-war cyber operations since 1998.[44]

Further, cyberwar is nowhere to be found among the most economically impactful cyberattacks since at least 1998. Russia's cyberattacks against Estonia in 2007[45] and Georgia in 2008[46] are not known to have been profoundly economically damaging. The impermanence and reversibility of cyber damage and the fact that both are smaller and less economically developed countries (particularly at the time) support the contention that the economic impacts from Russian activity would fall short of the thresholds

delineated above. The 2015 Russian attack on Ukraine's power grid was minimally impactful, with only 230,000 people losing power for up to six hours, suggesting minimal economic effect.[47] Following the 2022 invasion of Ukraine, the economic effects of Russia's cyberattacks were minimal in comparison to the first-year estimated economic damage of $600 billion (according to the Kyiv School of Economics[48]), with recorded impact limited to the $200 million insurance claim by Viasat.[49]

The largest cyber catastrophe events have not been large in terms of economic impact (particularly compared to natural disasters[50]), and acts of cyberwar have failed to reach even the economic levels achieved by cyber catastrophes. Moreover, caveating the lack of historical precedent for cyberwar still tends to fail to live up to the standard defined by Rid. Cyberwar is unlikely, and if it does occur with any scale, it would still comprise a small portion of the economic impact of the corresponding kinetic activity. What begins as a "cyberwar" —or more realistically, a cyber operation—is likely to end in something more physical. Although there have been no compelling economic losses from cyberwar, a look at broader historical loss activity, to include what can be ascribed to state actors, provides the necessary framework for demystifying the potential effects of cyberwar and facilitating their more robust inclusion into the IW agenda.

Cyber has been called "borderless," with the lack of limiting geography used to imply that the risk is "everything, everywhere, all at once."

FEAR OF PROPAGATION

The mitigating factors associated with the history of cyberwar (whether successful or merely potential) remain counterbalanced by the fear of propagation. Cyber has been called "borderless,"[51] with the lack of limiting geography used to imply that the risk is "everything, everywhere, all at once."[52] Although the historical record with rapid and

mass propagation—to profound economic effect—is virtually nonexistent,[53] the notion that rivers and mountain ranges cannot contain the cyber domain is a persistent concern.[54] Further, this narrative has been fed by several instances of uncontrolled cyberattacks.

Stuxnet and NotPetya are among the cyber events that can lead to concern about unintended consequences and a loss of control. Stuxnet was used in a cyberattack on the Natanz nuclear enrichment plant,[55] in an effort to slow Iran's progress toward its nuclear ambitions. It was a "third option" sought, between doing nothing and engaging in kinetic activity.[56] However, the attack "spread, apparently accidentally, far beyond the targeted nuclear enrichment plant in Natanz,"[57] although without further effect and was discovered publicly in 2010. Seven years later, Russia's defense intelligence agency (GRU) targeted Ukraine with the NotPetya malware.[58] A wiper (intended to delete data) masquerading as ransomware,[59] NotPetya was of questionable effectiveness: 95 percent of NotPetya's economic effect could be characterized as off-target—a subject explored in more detail later.[60] Once a cyber weapon is off the leash, so to speak, the fear that it could spread rapidly and cause damage to accumulate significantly is the first step toward worrying about reprisals, escalation, and even the prospect of a kinetic response (although "none of these admittedly worrying cyberattacks has ever warranted an armed attack with kinetic weapons in response"[61]).

In addition to concerns about an uncontrolled cyber weapon is the prospect of a response by a victim of such an attack—whether intentionally targeted or accidentally impaired. The prospect that "a cavalier attitude toward cyberspace could lead to long-term disruption with serious economic and political consequences"[62] has led some to take a more cautious view. This is especially the case in the U.S., with the suggestion that "the United States should forego opportunities for OCO [offensive cyber operations] and cyberespionage, because the system is too fragile to survive if the dominant state is insensitive to the fallout from its own self-serving actions."[63] This stands in stark contrast to kinetic engagements where such fallout has occurred—

including the war in Afghanistan ("[F]or the United States … the most protracted war in history—longer than World War I, World War II, and Vietnam combined"[64]) and potentially $3 trillion in U.S. costs for the war in Iraq.[65]

The rather rich historical record mentioned tends to be overlooked when policymakers and stakeholders are faced with the fear of inviting retribution or even attack because a cyber weapon has overshot its mark. In fact, perhaps counterintuitively, the predictability of traditional capabilities—from economic coercion to kinetic strikes—may seem preferable in comparison to the perceived uncertainty of cyber weapons, even though cyber weapons have never caused mass harm or meaningful destabilization. States have far more experience with kinetic capabilities, even if that includes a risk of overreach, collateral casualties, or other unintended consequences.

Methodology

More than two decades of immense focus on counterterrorism have impacted the ability of the U.S. government to refine its approach to national cyber security strategy—both in the military security space and more broadly. Independent research conducted in the academic community, though, suggests that cyberwar and non-war offensive cyber operations historically have not been economically impactful. However, the belief that they could be both widespread and uncontrollable—a fear fueled by the likes of NotPetya[66]—has led to concerns about the potential widespread use of cyber weapons, unnecessarily restricting their use. To help address this taboo and demonstrate that offensive cyber operations could be used more liberally without the prospect of unintended economic harm, a review of the economic effects of historical cyber catastrophe events can be used as a proxy (and a worst-case scenario) for cyberwar, given that no historical cases of cyberwar have risen to the levels necessary to be captured in the historical record for cyber catastrophes.

More than two decades of immense focus on counterterrorism have impacted the ability of the U.S. government to refine its approach to national cyber security strategy—both in the military security space and more broadly.

A review of the historical data set of major cyber catastrophe[67] revealed the instances in which such events were affected by state actors or proxies likely working on their behalf. Each of those events examined in case study form shows how they relate to a central research question: Is the use of cyber operations unnecessarily constrained by the belief that they could cause too much harm, intentionally or otherwise? The data set revealed only three cases of cyber catastrophe initiated by state actors or their proxies

that met the necessary criteria: Yaha (2003), WannaCry (2017), and NotPetya (2017). These three events represent the available historical record of state-induced cyber catastrophe. That record provides event characteristics and economic effects, event consequences as they relate to cyber operations taboos, and finally, lessons learned regarding the future use of cyber weapons.

Historical Economic Impact Analysis

The presumed potential for offensive cyber operations to cause extensive economic harm—intended or otherwise—is well established.[68] The notion that the interconnected nature of systems today facilitates transmission ostensibly implies that a bad actor's efforts can scale easily, causing economic damage to accumulate quickly and to deleterious effect. Although there have been few cases where state actors have affected widespread harm—and in fact, few cases where cyberattacks of any kind have caused widespread harm—the fear persists that the "big one" has "yet" to occur.

Among the reasons for this fear of propagation and impact is the 2017 NotPetya attack, although the concept can be traced back as far as the Morris Worm. Incorrectly called, even at the time, the "most destructive and costly cyber-attack in history",[69] NotPetya was actually a below-average cyber catastrophe as measured by economic harm at then-current $10 billion in damage (see Table 1). However, the risk of propagation as a potential driver of offensive cyber operations' unanticipated outcomes feared today is rooted in this lived experience, with similar concerns related to WannaCry. Of course, NotPetya is a rare (recent) exception; the vast majority of cyberattacks and operations have minimal impact.[70] The 873 items listed in the Council on Foreign Relations' (CFRs') Cyber Operations Tracker are both forgettable and forgotten.[71] That alone casts considerable doubt on the continued relevance of the cyber operations taboo. Furthermore, the 24 cyber catastrophes previously referred to (and detailed in Table 1) reflect a small (and sometimes non-overlapping subset of the CFR database) collection of events relevant per economic impact, although one could call many of them forgettable and forgotten, as well.

CYBER CATASTROPHE ECONOMIC IMPACT ANALYSIS

Since 1998, there have been 24 instances of cyber catastrophe, hewing to the definition in the research methodology, above. In aggregate, they represent $357 billion in economic damage,[72] at an average of $14.9 billion per event and $12.7 billion per year. By comparison, natural disaster economic damage from 2024 alone reached $320 billion,[73] 89.6 percent of the aggregate cyber loss

Table 1: Historical Cyber Catastrophe Losses (1998–2025)

Event	Year	Loss at the Time	Inflation-Adjusted Loss (2025)
MyDoom	2004	$38,000,000,000	$72,811,929,537
SoBig	2003	$37,000,000,000	$73,022,700,912
Klez	2001	$19,800,000,000	$41,456,803,007
ILOVEYOU	2000	$15,000,000,000	$32,348,869,013
Yaha	2003	$11,100,000,000	$21,709,451,622
Swen	2003	$9,200,000,000	$18,058,316,577
StormWorm	2007	$10,000,000,000	$17,535,060,531
Minmail	2003	$8,900,000,000	$17,466,240,623
Conficker	2008	$9,100,000,000	$15,913,067,432
NotPetya	2017	$10,000,000,000	$13,047,731,838
Zeus	2007	$3,000,000,000	$5,260,518,159
WannaCry	2017	$4,000,000,000	$5,219,092,735
CodeRed	2001	$2,400,000,000	$4,711,000,342
Melissa	1999	$1,500,000,000	$2,887,675,707
Chernobyl	1998	$1,000,000,000	$2,287,927,676
Nimda	2001	$1,500,000,000	$3,140,666,894
SirCam	2001	$1,250,000,000	$2,617,222,412
SQL Slammer	2003	$1,200,000,000	$2,368,303,813
Crowdstrike	2024	$1,700,000,000	$1,700,000,000
Change Healthcare	2024	$1,600,000,000	$1,600,000,000
CDK	2024	$12,000,000,000	$1,000,000,000
MOVEit	2023	$1,000,000,000	$1,000,000,000
CryptoLocker	2013	$665,000,000	$976,574,919
Sasser	2004	$500,000,000	$958,051,704

Source: Author, "Rewriting History: Understanding Historical Catastrophic Cyber Economic Losses," *Journal of Strategic Competition* 2, no. 1 (2026).

in Table 1. While these numbers may look substantial, they pale in comparison to other economic losses associated with other forms of disaster (e.g., natural disasters[74]), and a recent analysis of cyber catastrophe losses relative to gross domestic product (GDP) shows that the events in Table 1[75] largely fail to meet materiality thresholds.[76]

Of the 24 events listed, only three (12.5 percent) involved or likely involved offensive cyber operations affected by state actors or non-state actors acting on behalf of states (absent ransomware gang activity) in order to advance a political or military agenda: WannaCry, NotPetya, and potentially Yaha; although Yaha may have been the work of non-state actors seeking to show support. Table 2 shows the drivers or causes of each of the events in Table 1, revealing just how infrequently state actors or their proxies cause significant economic harm via the cyber domain.

As Table 2 shows, the economic impact of state-affected cyber operations has been quite small. The three events from Table 2 discussed above—NotPetya, WannaCry, and Yaha—amount to an inflation-adjusted $40 billion, only 11.2 percent of the aggregate economic loss from the 24 events in Table 1. Interestingly, Yaha accounts for more than half that amount, despite receiving far less media and academic attention than WannaCry and NotPetya. Of course, one could ascribe the higher loss sustained from Yaha (2002–2003) to the prevailing threat and economic loss environment at the time, recognizing that 91.4 percent of the economic damage captured in Table 1 came before 2009. The drop-off in impact per event after 2009—with NotPetya and WannaCry the only major economic losses since then—suggests that economic scale has become harder to achieve through cyber operations.

State-affected cyber catastrophes represent a small subset of cyber catastrophes, cyber operations, and catastrophic forms of economic loss. Non-catastrophic events are smaller still, in economic terms. As mentioned, there are no historical instances of cyber operations that have caused meaningful economic harm, aside from the three captured in Table 1 and discussed in detail following.

Table 2: Drivers/Causes of Major Cyber Catastrophe Events

Event Name	Year	Actor/Cause	State Actor	Notes
Crowdstrike	2024	System failure	No	This event was the result of internal error.[1]
CDK	2024	BlackSuit[2]	No	Ransomware
Change Healthcare	2024	BlackCat/ALPHV[3]	No	Ransomware
MOVEit	2023	CI0P[4]	No	Ransomware
NotPetya	2017	GRU/Russia[5]	Yes	This event qualifies as an offensive cyber operation by a state actor.
WannaCry	2017	Lazarus Group/North Korea[6]	Yes	Although one could call the motive financial, it was believed to be minimally effective in generating income.[7] It is not unusual for North Korean state actors to engage in activity that generates revenue for the government.
CryptoLocker	2013	CryptoLocker was crated by a criminal organization led by Evgeniy Bogachev.[8]	No	This was motivated by profit.
Conficker	2008	A group of Ukrainian actors (and one Swede) were identified as being behind Conficker.[9]	No	The motivation was presumably financial, given that Conficker propagated "scareware."
StormWorm	2007	The author is unknown but is believed to have commercial motives.[10]	No	The author is believed to have likely been in Russia. Further, the actors are likely to be loosely affiliated rather than an organized crime operation.[11]
Zeus	2007	The author is unnamed but known to be a criminal actor. [12]	No	
MyDoom	2004	It is believed to have been created by a spammer (similar to Minmail but likely unrelated).[13]	No	
Sasser	2003	Sven Jaschan created this and other worms.[14]	No	The creator was prosecuted.
SoBig	2003	It was believed to have been written by spammers.[15]	Unlikely	

Source: Author. See Appendix for references.

Table 2: Drivers/Causes of Major Cyber Catastrophe Events (continued)

Event Name	Year	Actor/Cause	State Actor	Notes
Yaha	2003	Indian hackers in support of the Indian government, although any further relationship would be speculative.[16]	Maybe	The attack against Pakistan did come during a period of conflict, although whether this could be attributed to a state actor or the direction of non-state actors by a state actor remains speculative at best. The virus was launched in 2002 but had broader effects unrelated to its initial use through 2003.[17]
Swen	2003	Actor/creator information is not available.	Unknown	It is believed to come from an author of other malware.[18]
Minmail	2003	Actor/creator information is not available.	Unknown	
SQL Slammer	2003	Created by David Litchfield, but deployed by an unknown bad actor.[19]	Unlikely	The code was reportedly taken from a public demo and deployed.
Klez	2001	Actor/creator information is not available.	Unknown	All that is known is that it originated "possibly in China or Hong Kong."[20]
CodeRed	2001	Actor/creator information is not available.	Unknown	
Nimda	2001	Actor/creator information is not available.	Unknown	Per The Register: "Actor/creator information is not available."[21]
SirCam	2001	Actor/creator information is not available.	Unknown	FBI likely did not investigate.[22]
ILOVEYOU	2000	Onel de Guzman[23]	No	The individual was not prosecuted, and his motivation remains unclear.
Melissa	1999	David Lee Smith[24]	No	The individual actor was convicted and sentenced to a 20-month sentence.
Chernobyl	1998	Chen Ing Hau (university student)[25]	No	The individual actor was never convicted of a crime.

Source: Author. See Appendix for references.

CASE STUDY 1: YAHA

Little information is available on the Yaha cyber catastrophe, having occurred in 2003[77] and involving operations initially outside the U.S. and Western Europe. Yaha featured in cyber engagements between India and Pakistan in 2002 and 2003, although the spread of the worm reached beyond their respective borders as it would use "innocent" computers to launch denial of service attacks.[78] The use of Yaha as part of a broader conflict has been characterized as "political protest"[79] and "cyber revenge."[80] Whether the attacks were cyberwar or directed by state actors is difficult to determine, but they were used for political purposes during a period of hostility.[81] The political motivation is sufficient to consider Yaha as state-related, even if it may not be as direct a connection as WannaCry or NotPetya.

The effects of Yaha on states and victims unrelated to the tension between India and Pakistan clearly represent an instance of cyber conflict spilling over beyond the intended targets. After several months of being limited to the combatant states and then to victims in the Middle East, the virus began to spread more aggressively at the end of 2002[82] and into the beginning of 2003.[83] The damage was limited to "nuisance activity,"[84] which can be characterized as impeding business activity and requiring the diversion of resources for remediation. While the potential impact may not seem cataclysmic when conveyed in that manner, Yaha was the fifth most impactful cyber catastrophe since 1998, in economic terms according to the data in Table 1. It's estimated damage of $11.1 billion in 2003 translates to approximately $21.7 billion today—or roughly 50 percent greater than that of NotPetya (similarly adjusted for inflation).

What stands out about Yaha is the size of its worldwide economic impact relative to the source and origins of the attack. It began as part of a regional conflict between India and Pakistan, and most of its rather significant economic impact landed elsewhere—a trend evident in WannaCry and NotPetya as well. In this manner, Yaha fits with the Morris Worm tradition regarding unintended consequences, and more importantly, it does so within the context of weaponization by a state

actor. Yaha represents an instance of severe spillover outside the conflict or campaign in which it was used. The spread of impact and proportion of it that could be characterized as off target speaks to fears of cyberattacks being uncontrollable, not to mention the prospect of errant impact creating the risk of diplomatic or military consequences. The unintended harm caused by Yaha could be construed as either a cyberattack or the saliently inappropriate and irresponsible use of a cyber weapon. In either instance, reprisals could be perceived as appropriate, which could then come during the preexisting tension associated with an ongoing conflict. Essentially, a state likely does not want to contend with diplomatic pressure from other states (particularly those that may be more influential) while it is actively engaged in hostilities. Of course, that risk did not materialize. Despite the significant spillover from the Yaha virus, there is no documented historical indication of state activity or response. Even when Yaha became "the most common viral menace of the Internet"[85] in July 2003, it did not appear to rise to a state-level concern outside the combatants—unlike NotPetya,[86] Colonial Pipeline,[87] Kaseya,[88] and others much later.

While consistent with the spillover risk that has helped make offensive cyber operations somewhat taboo, Yaha's legacy is

Fear of "spillover" risk—unintended victims outside the original target—has long served as a taboo that prevents military leadership from utilizing cyber as a de-escalatory form of irregular warfare. Historical case studies like Yaha demonstrate that even when a state-sponsored attack is almost entirely off-target, it rarely crosses the threshold of economic relevance or triggers a diplomatic or kinetic response. (AI-generated Adobe Stock image by miss irine)

far smaller than its relative economic impact. This may seem counterintuitive, but Yaha came during the busiest year for cyber catastrophes, with five events (the most for a single year since at least 1998) resulting in aggregate economic damage of $130.6 billion, adjusted for inflation (also the most for a single year since at least 1998)—according to the data in Table 1. So, this event is easily absorbed by the wider impact of cyber catastrophes that year. Additionally, the damage was not sufficient to create a legacy or learning opportunity, and it came early enough in the cyber domain's history that further maturation naturally made its lessons less relevant.

If Yaha is an example of the risk of cyber impact from a conflict spilling over into unintended victims and regions, then it is also an example of how high the threshold is for such spillover to be relevant. Yaha was largely off-target and, in comparison to other cyber catastrophes, quite impactful. Adjusted for inflation, it was larger than WannaCry and NotPetya combined (per the data in Table 1). Spillover risk occurred, and the taboo was tested. Although the absolute severity of the spillover paled in comparison to its relative severity, the lessons of Yaha have been forgotten. This is despite the fact that the event represents more than half the economic damage caused by state actor-induced cyber catastrophe and still failed to become memorable, suggesting that the spillover risk of offensive cyber operations is perhaps overstated.

CASE STUDY 2: WANNACRY

It is easy to dismiss Yaha as from a different era. That cyber catastrophe occurred more than 20 years ago, and growth of the internet and how it is used have both expanded significantly. Yaha occurred closer in time to the Morris Worm than present day (2025), and in fact, it is nearly equidistant temporally between the Morris Worm and WannaCry (and NotPetya). Although the lessons of Yaha are relevant to the discussion of spillover risk, cyber operation taboos, and the tangible limits on their consequences, more recent examples better reflect the cyber operational environment today—not to mention the nature of the consequences of spillover risk: that leaves

WannaCry and NotPetya, back-to-back state actor-induced cyber catastrophes in 2017.

WannaCry by North Korea's Lazarus group was not an act of war or even economic coercion but rather a likely attempt to generate income for the regime. Using code from the leaked EternalBlue capabilities developed by the U.S. National Security Agency,[89] WannaCry failed in its original purpose, yielding only £108,953[90] ($144,054[91]). However, it vastly overshot its original target and ultimately caused an estimated $4 billion in economic harm worldwide. While it caused a considerable amount of economic harm relative to its initial intent, the primary issue with WannaCry is that the operators lost control of the tool.[92] According to analysis by Eugene Kaspersky, more than 70 percent of the impact of WannaCry was borne by victims in Russia, which would have been an odd choice of target for North Korea, given the occasionally close relationship between the two states.[93] The U.S., United Kingdom, and other western powers did not feature among the top twenty victims. This outcome speaks to the likelihood of a spillover effect from an uncontrolled cyber weapon, engaging the same taboo as Yaha 14 years earlier. The spillover from WannaCry thus fed the narrative that cyber capabilities can be difficult to harness, direct, and manage, which can make them unwieldy and risky to use—even though it was only the second such attempt at weaponization to lead to widespread spillover consequences.

While WannaCry's impact remained relatively small worldwide, the real impact of WannaCry with regard to the spillover taboo comes from fear of how much worse it could have been if guided by the intention to cause harm.[94] Again, this refers to the power of imagination, as discussed by Lewis, with regard to cyber catastrophe risk.[95] WannaCry could have been worse if it had involved a zero-day vulnerability,[96] one could claim, or if it had not had a kill switch.[97] If it had propagated into the U.S. and United Kingdom instead of Russia, the economic impact presumably could have been greater. It is important to remember that such alternative outcomes remain the domain of the imagination, though. To imagine what WannaCry would have accomplished with zero-day vulnerabilities invokes a meaningful

chain of prerequisites that cannot be taken for granted. The same is true of where it propagated and what the tangible benefit of the kill switch was. Ultimately, the factors that led to the malware's "[a]ccidental death"[98] must be taken at face value, and while some amount of counterfactual analysis is both acceptable and prudent, it must be grounded in the basic facts of the case, with broader deviations requiring specific justification. Even taking the counterfactual scenarios at face value and assuming that WannaCry would have been three, five, or even 10 times more severe than it actually was, had it involved zero-day vulnerabilities or lacked an easily accessed kill switch. This would result in an economic impact ranging from $12–40 billion in 2017 U.S. dollars—yet the economic effect still would have been small, with Yaha near the middle on an inflation-adjusted basis.

Regardless of whether WannaCry could have been worse, it was one of the most significant cyber catastrophes since 1998 in economic terms, and it clearly led to spillover effects—interestingly affecting a state largely aligned with (or at least sympathetic to) the actor. While the Yaha case raised the question of what spillover means for non-combatants, WannaCry has led one to ask what happens when spillover affects friendly (if not allied) states—and the answer is nothing. In fact, Russia's messaging after the event was designed to alleviate any perceived pressure on North Korea by shifting the focus of attribution to the U.S., which Russia claimed "officially blamed North Korea."[99] This comes despite the fact that Russia saw several major institutions affected, including "the Russian Emergencies Ministry, Interior Ministry, the Russian Railways company and one the country's biggest banks, Sberbank, as well as the Megafon and Vympelcom mobile phone operators."[100] However, not only did no such stern warning come, Russia even provided North Korea with some helpful messaging, claiming that "US authorities officially blamed North Korea."[101]

Despite being called "at the time, the worst cyberattack in history,"[102] was not even the worst of the previous decade, and it was by far the least severe of the three cases of state-affected cyber catastrophe

being analyzed here. Any concerns about spillover risk were clearly misplaced, and although the attack did cause multiple billions of dollars in economic damage, it was far from sufficient to warrant any sort of major state-level response. White House statements[103] and a criminal complaint[104] were largely the extent of the official response. Fears that spillover could elicit a direct response from a major adversary (like the U.S.) or even a stern warning from Russia failed to materialize.

Like Yaha, the WannaCry case shows that such runaway attacks are less impactful than may be feared. After all, $4 billion in worldwide economic damage is small in comparison to other cyber catastrophes, let alone to major drivers of catastrophic economic harm (like natural disasters).[105] Even an event orders of magnitude larger—an assumption made with no support required—would still have fallen far short of any realistic threshold of economic relevance. WannaCry affected North Korea's adversaries and partners, and in doing so elicited a response that can be charitably described as negligible.[106] In fact, NotPetya was orders of magnitude larger than WannaCry, led to considerable spillover, and still did not lead to the sort of response that contributes to the taboo associated with offensive cyber operations. Cyber operations conducted by the long-standing adversaries of the U.S. have captured widespread attention, in a manner similar to the era of CT, when intense national focus and public anxiety dominated discourse. Today, the political narratives surrounding Russia and North Korea, for example, command a similar degree of fascination and influence.

CASE STUDY 3: NOTPETYA

NotPetya is often considered one of the largest and most impactful events to have occurred in the cyber domain, although some of that is the result of hyperbole.[107] Perhaps because of the language used to describe the event, NotPetya's influence on the perception of cyber risk and cyber operations is difficult to dispute. The attack engineered by Russia's GRU (similar to the U.S. Defense Intelligence Agency) was intended for Ukraine in 2017, three years after the initial invasion and

attendant IW operations.[108] While it did ultimately impact up to 0.5 percent of Ukraine's GDP,[109] the effects were more impactful outside the country, where victims bore approximately 95 percent of the $10 billion in economic consequences.

The gap between on- and off-target economic effect is clearly linked to the fact that, like WannaCry, the actor lost control of the tool. Furthermore, like WannaCry, the spillover effects resulting from that loss of control over NotPetya were not significant economically, despite the many and vociferous claims to the contrary. While the attack was indeed noteworthy—particularly coming on the heels of WannaCry and its roots in EternalBlue[110] —its economic impact was utterly manageable. However, it did gain enough notoriety to drive questions about the risks associated with cyber operations by virtue of the fact that its propagation did result from a salient loss of control of the weapon.[111]

The similarities among NotPetya, WannaCry, and Yaha are clear. They represent the use of cyber weapons by state actors who ultimately lost control of the attacks and caused a significant amount of unintended and off-target damage. However, to view NotPetya as simply a larger WannaCry or western Yaha would be to miss the most important lessons available from the event. Unlike WannaCry and Yaha, the crucial difference of NotPetya is that it caused harm to the aggressor state. The fear of a cyberattack by one state affecting its own citizens and impairing its own cyber and economic security can be powerful. Policymakers, defense officials, and other security stakeholders would likely not welcome the prospect of having to explain to the communities they protect how they inadvertently became the aggressors. Although the psychological aspects of this fear are meaningful, they represent a topic for future research. Within the scope of the economic ramifications of state-affected cyber catastrophe, the tangible effects of such self-harm are evident from NotPetya—and they are not large.

It is difficult to determine what portion of the economic impact was borne by Russia itself, but some indicators are available. It is known

that several Russian companies were indeed affected by NotPetya, including Rosneft and Sberbank, although the damage was not meaningful.[112] In fact, Russia even used the damage it sustained itself to claim victimhood and support its innocence.[113] It is of course believed that Russia was the actor,[114] but the damage to itself was problematic for the cyber operations community worldwide. A loss of control that swings back to the attacker takes the problems associated with unintended consequences and makes them a domestic matter.

The first question associated with potential self-harm risk in cyber operations, specifically with regard to NotPetya, is the extent to which the harm was meaningful, even when the attacker lost control of the weapon. Approximately half the worldwide economic damage from NotPetya can be attributed to specific companies: Merck[115] ($2 billion), St. Gobain[116] ($1 billion), FedEx/TNT[117] ($1 billion), and Maersk[118] ($300 million) alone get to $3.3 billion—with another $560 million caused to Ukraine. A series of smaller victims, including Mondelez, St Gobain, DLA Piper, and Reckitt Benkeiser, likely brings the total closer to $5 billion.[119] This means that the impact to Russia was below $5 billion—and likely much further below that level, given that the companies affected in Russia are not believed to have sustained significant impact.[120] Further, the total economic harm sustained by Russia in 2017 is estimated to have been $1.85 billion,[121] a total that spans WannaCry, NotPetya, BadRabbit, and other attacks. With Russia affected heavily by both WannaCry and BadRabbit,[122] there is a natural limit on the amount of harm that could be attributed to NotPetya. Overall, it is easy to conclude that the economic effects from its own experience with NotPetya victimhood were not significant.

The second question arising from this situation concerns the extent to which the effects could have been worse. Interestingly, the situation in Russia in 2017 is directly relevant. It was a tough year for the country, with the $1.85 billion in economic harm referenced indicative of a high rate of cyberattack frequency and severity.[123] Although the aggregate economic harm visited upon Russia in 2017 was small within the context of cyber catastrophe losses in general—not to mention other forms of loss, like natural disasters—it was focused in one year and

concentrated on one country. One could construe this as meaningful. Within that context, the effects were still not cataclysmic. In the end, this suggests that even a much worse outcome still would not have been material economically.

What is clear is that the taboo associated with accidental self-harm from the use of cyber weapons appears to be overstated. First, the risk appears to be quite rare, at least for events with any meaningful scale. Table 1 offers no clear instances of self-harm from the loss of control of a cyber weapon aside from NotPetya. Further, as demonstrated, the likely economic damage to Russia was minimal—and would have remained minimal even in a worst-case outcome.

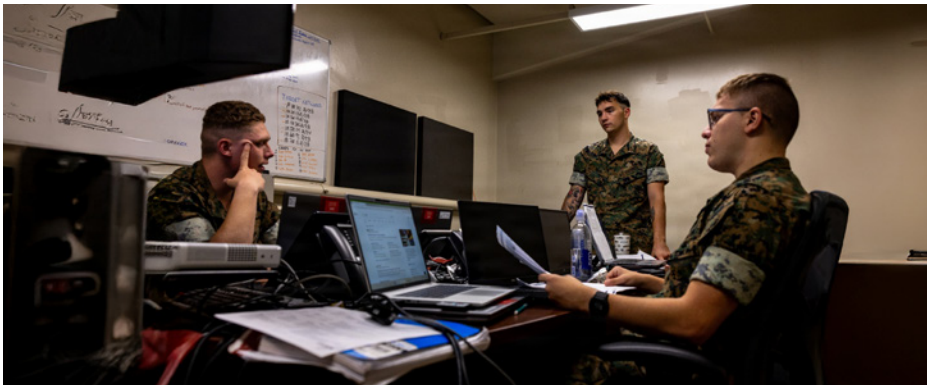
The risk of spillover from uncontrollable cyber weapons—whether to adversaries, the attacking state, or unrelated parties—is historically rare and minimal. Since 1998, it has only happened three times, and even the worst such events (Yaha) were limited in the damage they caused. The question that results, then, is not about the potential harm that can come from errant cyberattacks but whether the taboo should be sunset, restrictions on the use of cyber weapons loosened, and commanders empowered to turn to the cyber domain more readily.

The Case for Expanded Use of Cyber Operations

The limits associated with the offensive cyber toolkit are defined by a perception of the domain that has been demonstrated to be inaccurate. The depth and maturity of the research that supports the need to remove the offensive cyber stigma has only grown over the economic effects of cyber catastrophe[124] as a mechanism for contextualizing offensive cyber operations such as WannaCry and NotPetya. In fact, constraints on the circumstances in which commanders can turn to offensive cyber operations necessarily results in alternatives that may not be suited to certain circumstances, to include the potential use of kinetic warfare (even on a limited basis) where cyber operations could be used more effectively and without the permanence associated with traditional weapons.

Part of the challenge is that, although cyber operations fall under the same authorities as traditional military engagement, they are often not leveraged optimally regarding adversaries and adversary activity in the cyber domain. The challenges associated with understanding second-order effects when assessing operations from a legal perspective have been an impediment—although now addressed through the quantification of past state-actor cyberattacks with proportionately significant spillover. The result has been a tendency toward intelligence collection and other forms of cyber espionage, which have been identified by some as a better use of cyber capabilities, given that "many cyber weapons can only be used once."[125]

Furthermore, traditional (kinetic) alternatives may be simply easier to engage. Utilizing the cyber toolkit against adversary nations likely falls under special authorities, such as those relating to unconventional warfare or covert action—requiring significant approvals at the executive or congressional level. While this may be consistent with other unconventional or irregular capabilities, it still represents a divergence from known operational capabilities and lived experience.



U.S. Marine Corps Pfc. Tobby Langston, left, a native of Colorado, and Pfc. Trevor Uken, a native of Kansas, and Lance Cpl. Benjamin Olson, a native of Virginia, all cyberspace warfare operators with 3d Cyber Warfare Company, III Marine Expeditionary Force Information Group, discuss strategies during the Marine Corps Cyber Red Zone 26-1 event at Camp Courtney, Okinawa, Japan, Oct. 29, 2025. (U.S. Marine Corps photo by Lance Cpl. John-Paul Haubeil)

Rethinking legislative authorities to more regularly leverage cyber operations in a tactical sense at a lower level could fill an important gap to attain a particular result.

As a result of the familiarity with kinetic alternatives and the accepted uncertainty in regard to the use of cyber operations, the unwarranted fear of potential cyber operations impacts could lead to the use of more dangerous alternatives—if for no other reason than that they are more familiar. As a result, cyber operations concerns that have led to their limited use have actually contributed to a more dangerous world. Leaning into conservatism in the face of the seemingly unknown does not, in this case, yield a better-safe-than-sorry result. It does the contrary.

Historically, the absence of hard data reflecting economic damage associated with offensive cyber operations and the deployment of cyber weapons has made it easier to take a conservative approach. Few operations by state actors have had material economic consequences, and those consequences can only be seen as significant within the context of cyber catastrophes, which in general have had relatively little economic impact. In fact, the general ineffectiveness

of cyber weapons, which "are unlikely to have any impact in a few years'—or even less—time"[126] as well as the reversibility of those weapons,[127] speaks to an impermanence of impact without regard to whether their victims were reached intentionally or otherwise. The result is a lower level of risk associated with the use of such weapons, to include when their use goes awry.

The misunderstanding of what could go wrong has become an impediment to optimizing coercive capabilities and using them in a targeted, incisive, and non-escalatory manner. As the five case studies mentioned demonstrate, there is plenty that can go wrong in cyber operations—but nothing that rises to the point where cyber operations should be constrained.

The fact that cyber capabilities are "not likely to serve as the final arbiter of conflict in an anarchic world,"[128] suggests a broader prospective use for them, and to this end, a niche for offensive cyber operations within the IW toolkit has clearly begun to emerge. There is an opportunity to use offensive cyber operations more frequently as a tool to make room for diplomacy—rather than as a "continuation of political intercourse with an admixture of other means."[129] The use of offensive cyber operations can serve as a precursor to diplomacy, a way to buy time for further negotiation, or as a coercive capability engagement intended to demonstrate a superiority in the cyber domain that simply makes it advantageous for the target state to reconsider negotiation.

The fact that cyber operations may be a third option does not preclude them from becoming an early consideration for SOF use or broader applications, particularly with suggested models for further integration between SOF and cyber units.[130] An improved understanding of how cyber operations can help advance strategic objectives is useful, but to remove the taboo associated with them is more important in the near term. The misunderstanding of what could go wrong has become an impediment to optimizing coercive

capabilities and using them in a targeted, incisive, and non-escalatory manner. As the five case studies mentioned demonstrate, there is plenty that can go wrong in cyber operations—but nothing that rises to the point where cyber operations should be constrained.

Conclusion

Cyber operations are not only here to stay—they should become more common. Historically believed to be unwieldy and uncontrollable, the evolution of cyber weapons, their use, and impact demonstrate not only the contrary but that the effects of their use tend to be limited and even de-escalatory. When cyber weapons do veer off target—to co-opt the language of traditional weapons—the collateral damage is far less severe than feared. Moreover, it is certainly less severe damage caused by errant bombs. Rather than fearing an unknown scale of unintended consequences, it is instead time to evaluate potential offensive cyber operations based on what weapons, operators, and domain do well. There are clear cases for cyber operations, and the best capability for each mission and domain should be used.

Rather than fearing an unknown scale of unintended consequences, it is instead time to evaluate potential offensive cyber operations based on what weapons, operators, and domain do well. There are clear cases for cyber operations, and the best capability for each mission and domain should be used.

To start, this means that cyber operations stakeholders and their commanders need to start to believe what they see. There is no shortage of empirical evidence as to the limited effectiveness of cyber weapons and cyber warfare. The worst mistakes neither caused carnage nor triggered escalatory behavior (let alone retaliation), as WannaCry and NotPetya both show. Cyber operations can work well, and they can fail manageably.

To overcome the stigma associated with cyber operations, understanding and experience is crucial. The former makes it easier to

deploy cyber capabilities in third-option scenarios, and the latter demonstrates that the legacy fears associated with the cyber domain are unfounded. There is no substitute, frankly, for letting the operators operate. In doing so, the potential for a virtuous cycle emerges, in which experience validates knowledge—which feeds future experience. Several iterations of this virtuous cycle would thus result in the ready adoption and improved use of the most important IW resource that is not being used enough. 

Appendix

Table 2: Drivers/Causes of Major Cyber Catastrophe Events

Event Name	Year	Actor/Cause	State Actor	Notes
Crowdstrike	2024	System failure	No	This event was the result of internal error.[1]
CDK	2024	BlackSuit[2]	No	Ransomware
Change Healthcare	2024	BlackCat/ALPHV[3]	No	Ransomware
MOVEit	2023	Cl0P[4]	No	Ransomware
NotPetya	2017	GRU/Russia[5]	Yes	This event qualifies as an offensive cyber operation by a state actor.
WannaCry	2017	Lazarus Group/North Korea[6]	Yes	Although one could call the motive financial, it was believed to be minimally effective in generating income.[7] It is not unusual for North Korean state actors to engage in activity that generates revenue for the government.
CryptoLocker	2013	CryptoLocker was crated by a criminal organization led by Evgeniy Bogachev.[8]	No	This was motivated by profit.
Conficker	2008	A group of Ukrainian actors (and one Swede) were identified as being behind Conficker.[9]	No	The motivation was presumably financial, given that Conficker propagated "scareware."
StormWorm	2007	The author is unknown but is believed to have commercial motives.[10]	No	The author is believed to have likely been in Russia. Further, the actors are likely to be loosely affiliated rather than an organized crime operation.[11]
Zeus	2007	The author is unnamed but known to be a criminal actor. [12]	No	
MyDoom	2004	It is believed to have been created by a spammer (similar to Minmail but likely unrelated).[13]	No	
Sasser	2003	Sven Jaschan created this and other worms.[14]	No	The creator was prosecuted.

Source: Author

Table 2: Drivers/Causes of Major Cyber Catastrophe Events (continued)

Event Name	Year	Actor/Cause	State Actor	Notes
SoBig	2003	It was believed to have been written by spammers.[15]	Unlikely	
Yaha	2003	Indian hackers in support of the Indian government, although any further relationship would be speculative.[16]	Maybe	The attack against Pakistan did come during a period of conflict, although whether this could be attributed to a state actor or the direction of non-state actors by a state actor remains speculative at best. The virus was launched in 2002 but had broader effects unrelated to its initial use through 2003.[17]
Swen	2003	Actor/creator information is not available.	Unknown	It is believed to come from an author of other malware.[18]
Minmail	2003	Actor/creator information is not available.	Unknown	
SQL Slammer	2003	Created by David Litchfield, but deployed by an unknown bad actor.[19]	Unlikely	The code was reportedly taken from a public demo and deployed.
Klez	2001	Actor/creator information is not available.	Unknown	All that is known is that it originated "possibly in China or Hong Kong."[20]
CodeRed	2001	Actor/creator information is not available.	Unknown	
Nimda	2001	Actor/creator information is not available.	Unknown	Per The Register: "Actor/creator information is not available."[21]
SirCam	2001	Actor/creator information is not available.	Unknown	FBI likely did not investigate.[22]
ILOVEYOU	2000	Onel de Guzman[23]	No	The individual was not prosecuted, and his motivation remains unclear.
Melissa	1999	David Lee Smith[24]	No	The individual actor was convicted and sentenced to a 20-month sentence.
Chernobyl	1998	Chen Ing Hau (university student)[25]	No	The individual actor was never convicted of a crime.

Source: Author

1 "CrowdStrike Outage: Lessons for Operational Resilience," *Financial Conduct Authority*, October 31, 2104, https://www.fca.org.uk/firms/operational-resilience/crowdstrike-outage-lessons-operational-resilience.

2 "Explainer: The 'BlackSuit' Hacker Behind the CDK Global Attack Hitting US Car Dealers," *Reuters*, June 27, 2024, https://www.reuters.com/technology/cybersecurity/blacksuit-hacker-behind-cdk-global-attack-hitting-us-car-dealers-2024-06-27/.

3 Daneil Croft, "Change Healthcare Reveals Data Stolen in ALPHV/RansomHub Cyber Attack," *CyberDaily*, June 24, 2024, https://www.cyberdaily.au/security/10733-change-healthcare-reveals-data-stolen-in-alphv-ransomhub-cyber-attack.

4 "#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability," Cybersecurity and Infrastructure Security Agency, June 7, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

5 Ellen Nakashima, "Russian Military Was Behind 'NotPetya' Cyberattack in Ukraine, CIA Concludes," *Washington Post*, January 12, 2018, https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html.

6 Foreign and Commonwealth Office, "Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks," Gov.UK, December 19, 2017, https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks.

7 Ellen Nakashima, "The NSA Has Linked the WannaCry Computer Worm to North Korea," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html.

8 Joshua Cannell, "Cryptolocker Ransomware: What You Need to Know," Malwarebytes Labs, October, 8, 2013, https://www.malwarebytes.com/blog/news/2013/10/cryptolocker-ransomware-what-you-need-to-know.

9 Mark Bowden, "The Worm That Nearly Ate the Internet," *New York Times*, June 29, 2019, https://www.nytimes.com/2019/06/29/opinion/sunday/conficker-worm-ukraine.html.

10 "Storm Worm: Five Things to Know About Powerful, Adaptive Malware," HYPR, https://www.hypr.com/security-encyclopedia/storm-worm.

11 John Leyden, "Storm Worm Turns One: Many Unhappy Returns," *The Register*, January, 18, 2008, https://www.theregister.com/2008/01/18/storm_worm_botnet/.

12 Diane Bartz, "Top Hacker 'Retires'; Experts Brace for His Return," *Reuters*, October 29, 2010, https://www.reuters.com/article/idUSTRE69S54Q20101029/.

13 Helen, "[Review] MyDoom Virus: The Most Destructive & Fastest Email Worm," MiniTool, https://www.minitool.com/backup-tips/mydoom-virus.html?amp#who-created-mydoom%3F-10726.

14 Duncan Macrae, "Everything You Need to Know About the Sasser Worm," *Tech Monitor*, April 11, 2014, https://www.techmonitor.ai/technology/cybersecurity/everything-you-need-to-know-about-the-sasser-worm-4213147?cf-view.

15 "Sobig Worm Recruits PCs for Profit," *Al Jazeera*, August 21, 2003, https://www.aljazeera.com/news/2003/8/21/sobig-worm-recruits-pcs-for-profit.

16 "Worm Launches Attack on Pakistan Govt Website," Help Net Security, July 1, 2002, https://www.helpnetsecurity.com/2002/07/01/worm-launches-attack-on-pakistan-govt-website/.

17 Michelle Delio, "Yaha Virus Uses Netizens as Pawns," *Wired*, March 13, 2003, https://www.wired.com/2003/03/yaha-virus-uses-netizens-as-pawns/.

18 "Worm:W32/Swen," F-Secure, https://www.f-secure.com/v-descs/swen.shtml.

19 David Litchfield, "The Inside Story of SQL Slammer," ThreatPost, October 20, 1010, https://threatpost.com/inside-story-sql-slammer-102010/74589/.

20 "Worm:W32/Klez," F-Secure, https://www.f-secure.com/v-descs/klez.shtml.

21 John Leyden, "Ten Years on from Nimda: Worm Author Still at Large," *The Register*, September 17, 2011, https://www.theregister.com/2011/09/17/nimda_anniversary/.

22 David Becker, "FAQ: What You Need to Know About SirCam," CNet, July 24, 2001, https://www.cnet.com/tech/tech-industry/faq-what-you-need-to-know-about-sircam/.

23 Mark Landler, "A Filipino Linked to 'Love Bug' Talks About His License to Hack," *New York Times*, October 21, 2000, https://www.nytimes.com/2000/10/21/business/a-filipino-linked-to-love-bug-talks-about-his-license-to-hack.html.

24 "The Melissa Virus: An $80 Million Cyber Crime in 1999 Foreshadowed Modern Threats," FBI.gov, March 25, 2019, https://www.fbi.gov/news/stories/melissa-virus-20th-anniversary-032519.

25 Paul Ducklin, "20 Years Ago Today! What We Can Learn from the CIH Virus...," *Sophos*, April 26, 2018, https://www.sophos.com/en-us/blog/20-years-ago-today-what-we-can-learn-from-the-cih-virus.

Acronyms

CFR	Council on Foreign Relations
CT	counterterrorism
GDP	gross domestic product
GRU	Main Directorate of the General Staff of the Armed Forces of the Russian Federation (Russian Defense Intelligence Agency)
IW	irregular warfare
JSOU	Joint Special Operations University
NATO	North Atlantic Treaty Organization
OCO	offensive cyber operations
SOF	special operations forces

Notes

1 Stephanie Pendino et al., "U.S. Cyber Deterrence: Bringing Offensive Capabilities Into the Light", *Campaigning: The Journal of the Joint Forces Staff College, (2022): 6,* https://jfsc.ndu.edu/Media/Campaigning-Journals/Academic-Journals-View/Article/3149856/us-cyber-deterrence-bringing-offensive-capabilities-into-the-light/.

2 Darren Pain, *Cyber Risk Accumulation: Fully Tackling the Insurability Challenge,* The Geneva Association, (November 2023): 6, https://www.genevaassociation.org/sites/default/files/2023-11/cyber_accumulation_report_91123.pdf.

3 Tom Johansmeyer et al., "Cyber Strategy in Practice: The Evolution of US, Russian and Ukrainian National Cyber Security Strategies Through the Experience of War," *RUSI Journal* 169, no. 3 (2024): 42, https://doi.org/10.1080/03071847.2024.2377544.

4 Pendino et al., "U.S. Cyber Deterrence," 6.

5 Howden Group, *Cyber Insurance: A Hard Reset 2.0*, (2022): 17 https://www.howdengroup.com/sites/corporate.howdenprod.com/files/2022-06/howden-cyber-insurance-a-hard-reset-2.0-single-page-final.pdf.

6 Emil Larsson, "Collateral Damage from Offensive Cyber Operations—A Systematic Literature Review," *Journal of Cybersecurity and Privacy* 5, no. 35 (2025): 1, https://doi.org/10.3390/jcp5020035.

7 Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2011): 5-32, https://doi.org/10.1080/01402390.2011.608939.

8 Johansmeyer et al., "Cyber Strategy in Practice," 42.

9 "Unexpectedly, the Cost of Big Cyber-Attacks Is Falling," *The Economist,* May 17, 2024, https://www.economist.com/graphic-detail/2024/05/17/unexpectedly-the-cost-of-big-cyber-attacks-is-falling.

10 The focus on economic harm does omit discussions of non-economic harm, such as the impacts of espionage on an adversary. This article focuses on the weaponization of cyber capabilities rather than other military and diplomatic uses, which leaves such topics as espionage outside its scope.

11 Kelly R. M. Ihme, Patrick O'Brien Boling, Michael Zimmerman, and Timothy G. McCormick, "Who Is in Charge of Cyber Incidence Response in the Homeland?" *U.S. Army War College Publications,* September 16, 2025, https://publications.armywarcollege.edu/News/Display/Article/4305189/who-is-in-charge-of-cyber-incidence-response-in-the-homeland/.

12 Tom Johansmeyer, "Rewriting History: Understanding Historical Catastrophic Cyber Economic Losses," *Journal of Strategic Competition,* 2, no. 1 (2026), https://strategiccompetition.org/index.php/josc/article/view/22/3; The general hyperbolization of the economic effects of cyber catastrophe can be found in 'Rewriting History;' Tom Johansmeyer, "NotPetya, Ukraine, and the Limits of Economic Impact from Cyber Attacks," *The Loop: ECPR's Political Science Blog*, August 18, 2025, https://theloop.ecpr.eu/notpetya-ukraine-and-the-limits-of-economic-impact-from-cyber-attacks/; A specific view of how this manifested with regard to the effects of NotPetya in Ukraine is offered in 'NotPetya, Ukraine, and the Limits of Economic Impact.'

13 Josh Golding, "Byte, With, and Through: How Special Operations and Cyber Command Can Support Each Other," *War on the Rocks,* November 11, 2022, https://warontherocks.com/2022/11/byte-with-and-through-how-special-operations-and-cyber-command-can-support-each-other/.

14 Josh Golding, "Byte, With, and Through."

15 Chaveso "Chevy" Cook et al., "Going Above and Beyond the Battlefield: Elevating Civil Affairs and Psychological Operations in the SOF-Space-Cyber Triad," *Special Warfare,* August 7, 2025, https://www.swcs.mil/Special-Warfare-Journal/Article/4268817/going-above-and-beyond-the-battlefield-elevating-civil-affairs-and-psychologica/.

16 Arquilla and Ronfeldt do sustain a fair amount of criticism in this article—and in a sense unfairly. It is worth remembering that they sought to address a new, unknown, and untested potential threat environment with virtually no context from which to draw. What they proposed was revolutionary at the time and helped get the scholarship get to where it is today. The security and strategy community owes these gentlemen more thanks than they likely receive.

17 John Arquilla and David Ronfeldt, "Cyberwar Is Coming!" *Comparative Strategy* 12, no. 2 (1993): 144, https://doi.org/10.1080/01495939308402915.

18 Arquilla and Ronfeldt, "Cyberwar Is Coming," 147.

19 Arquilla and Ronfeldt, "Cyberwar Is Coming," 144.

20 Arquilla and Ronfeldt, "Cyberwar Is Coming," 142.

21 Tom Johansmeyer, "Cyber Attacks in Perspective: Cutting Through the Hyperbole," *Irregular Warfare Initiative,* June 25, 2024, https://irregularwarfare.org/articles/cyber-attacks-in-perspective-cutting-through-the-hyperbole/.

22 Cameran Ashraf, "Defining Cyberwar: Towards a Definitional Framework," *Defense and Security Analysis* 37, no. 3, (2021): 281, https://doi.org/10.1080/14751798.2021.1959141.

23 Lindsay Lennon, "The 'Morris Worm': A Notorious Chapter of the Internet's Infancy," *Cornellians,* November 16, 2023, https://alumni.cornell.edu/cornellians/morris-worm/.

24 Lennon, "The 'Morris Worm.'"

25 Arquilla and Ronfeldt, "Cyberwar Is Coming," 147.

26 Lennon, "The 'Morris Worm.'"

27 Tom Johansmeyer, "Recent Cyber Catastrophes Show an Intensifying Trend—but They Are Manageable," *The Loop: ECPR's Political Science Blog*, September 25, 2024, https://theloop.ecpr.eu/recent-cyber-catastrophes-show-an-intensifying-trend-but-they-are-manageable/.

28 Julian Ring, "30 Years Ago, One Decision Altered the Course of Our Connected World," *All Things Considered*, NPR, April 30, 2023, https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary.

29 United States Department of Commerce, *E-Stats*, March 19, 2003, https://www.census.gov/content/dam/Census/library/publications/2001/econ/1999estatstext.pdf.

30 Charles Krauthammer, "The Unipolar Moment," *Foreign Affairs*, January, 1, 1990, https://www.foreignaffairs.com/articles/1990-01-01/unipolar-moment?check_logged_in=1.

31 Damien McGuinness, "How a Cyber Attack Transformed Estonia," *BBC News*, April 27, 2017, https://www.bbc.com/news/39655415.

32 James Pamment et al., *Hybrid Threats: 2007 Cyber Attacks on Estonia*, NATO Strategic Communications Centre of Excellence, June 6, 2019, 66, https://stratcomcoe.org/pdfjs/?file=/publications/download/cyber_attacks_estonia.pdf?zoom=page-fit.

33 Pamment et al., *Hybrid Threats,* 67.

34 Johansmeyer et al., "Cyber Strategy in Practice," 42.

35 Jon Bateman et al., "What the Russian Invasion Reveals About the Future of Cyber Warfare," Carnegie Endowment for International Peace, December 19, 2022, https://carnegieendowment.org/posts/2022/12/what-the-russian-invasion-reveals-about-the-future-of-cyber-warfare?lang=en.

36 Jon Bateman, "Russia's Wartime Operations in Ukraine: Military Impacts, Influences, and Implications," Carnegie Endowment for International Peace, December 16, 2022, 32–3, https://carnegie-production-assets.s3.amazonaws.com/static/files/Bateman_Cyber-FINAL21.pdf.

37 Thomas Rid, 2012, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (2011): 7 https://doi.org/10.1080/01402390.2011.608939.

38 Francis Miyata, "The Grand Strategy of Carl von Clausewitz," *War Room: Online Journal,* March 26, 2021, https://warroom.armywarcollege.edu/articles/grand-strategy-clausewitz/.

39 Hugh Smith, "Clausewitz's Definition of War and its Limits," *Military Strategy Magazine,* December (2020), https://doi.org/10.64148/msm.article.943.

40 Rid, "Cyber War Will Not Take Place," 11.

41 Hannah Mitchell, "Cyberattack on Alabama Hospital Linked to 1st Alleged Ransomware Death," *Becker's Health IT*, September 30, 2021. Several cyberattacks have caused limited physical damage, including LockerGoga and NotPetya, with the former impacting NorskHydro and the latter Merck. https://www.beckershospitalreview.com/healthcare-information-technology/cybersecurity/cyberattack-on-alabama-hospital-linked-to-1st-alleged-ransomware-death/; Becky Bracken "Court Rules 'War or Hostile Acts' Exclusion Does Not Apply to the Pharma Giant's 2017 Cyberattack," *ThreatPost*, January, 21, 2022, https://threatpost.com/merck-insurance-payout-notpetya-attack/177872/. Please see for a source on loss of life, for the implications of LockerGoga on NorskHydro (physical damage).

42 James Andrew Lewis, "Dismissing Cyber Catastrophe," Center for Strategic and International Studies, August 17, 2020, https://www.csis.org/analysis/dismissing-cyber-catastrophe.

43 Rishi Iyengar, "'Everything, Everywhere, All At Once': U.S. Officials Warn of Increased Cyberthreats," *Foreign Policy*, April 1, 2024, https://foreignpolicy.com/2024/04/01/cybersecurity-defense-hacking-china-russia-iran-critical-infrastructure/.

44 Johansmeyer, "Recent Cyber Catastrophes."

45 Johansmeyer et al., "Cyber Strategy in Practice," 42.

46 Johansmeyer et al., "Cyber Strategy in Practice," 42.

47 Tom Johansmeyer, "Cyber Attacks in Perspective."

48 Jack Buckby, "$600 Billion: That's How Much Economic Damage the Ukraine War Has Caused," *1945*, June 1, 2022, https://www.19fortyfive.com/2022/06/600-billion-thats-how-much-economic-damage-the-ukraine-war-has-caused/.

49 Tom Johansmeyer, "Is the Fear of Cyberwar Worse Than Cyberwar Itself?" *Lawfare*, November 15, 2023, https://www.lawfaremedia.org/article/is-the-fear-of-cyberwar-worse-than-cyberwar-itself.

50 Tom Johansmeyer, "Why Natural Catastrophes Will Always Be Worse than Cyber Catastrophes," *War on the Rocks*, April 5, 2024, https://warontherocks.com/2024/04/why-natural-catastrophes-will-always-be-worse-than-cyber-catastrophes/.

51 Tom Johansmeyer et al., "Invisible Lines, Visible Impact: How Territorial Security Influences Russian Cyber Security Strategy" *RUSI Journal* 170, no. 1, (2025): 20, https://www.tandfonline.com/doi/full/10.1080/03071847.2025.2458143.

52 Joshua Rovner, "Everything, Everywhere, All at Once? Cyberspace Operations and Chinese Strategy," *War on the Rocks,* March 25, 2024, https://warontherocks.com/2024/03/everything-everywhere-all-at-once-cyberspace-operations-and-chinese-strategy/.

53 Tom Johansmeyer, "Surprising Stats: The Worst Economic Losses from Cyber Catastrophes," *The Loop: ECPR's Political Science Blog,* March, 12, 2024, https://theloop.ecpr.eu/surprising-stats-the-worst-economic-losses-from-cyber-catastrophes/. This is implied by the absence of severe economic effects in the historical record.

54 Johansmeyer et al., "Invisible Lines, Visible Impact," 26.

55 Claudia Emilie Aanonsen, "Stuxnet, Revisited (Again): Producing the Strategic Relevance of Cyber Operations," *Journal of Cyber Policy* 10, no. 1 (2025): 70, 81, https://doi.org/10.1080/23738871.2025.2492570.

56 Aanonsen, "Stuxnet, Revisited (Again)," 73.

57 Lennart Maschmeyer, "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations," *International Security* 46, no. 2, (2021): 64, https://doi.org/10.1162/isec_a_00418.

58 Tom Johansmeyer, "Cyber Attacks in Perspective: Cutting Through the Hyperbole," *Irregular Warfare Initiative*, June 25, 2024, https://irregularwarfare.org/articles/cyber-attacks-in-perspective-cutting-through-the-hyperbole/.

59 Tom Johansmeyer, "NotPetya, Ukraine."

60 Tom Johansmeyer, "Debunking NotPetya's Cyber Catastrophe Myth," *Binding Hook,* April 10, 2024, https://bindinghook.com/debunking-notpetyas-cyber-catastrophe-myth/.

61 Jason Healey and Robert Jervis, "The Escalation Inversion and Other Oddities of Situational Cyber Stability," *Texas National Security Review,* (2020): 32, http://dx.doi.org/10.26153/tsw/10962.

62 Joshua Rovner and Tyler Moore, "Does the Internet Need a Hegemon?", *Journal of Global Security Studies* 2, no. 3 (2017): 188, https://doi.org/10.1093/jogss/ogx008.

63 Rovner and Moore, "Does the Internet Need a Hegemon?", 188.

64 Robert J. Bliwise, "Reckoning with America's Longest War," *Duke Mag*, November 24, 2021, https://dukemag.duke.edu/stories/reckoning-americas-longest-war.

65 Joseph E. Stiglitz and Linda J. Bilmes, "The True Cost of the Iraq War: $3 Trillion and Beyond," *Washington Post*, September 5, 2010, https://www.washingtonpost.com/wp-dyn/content/article/2010/09/03/AR2010090302200.html.

66 Maschmeyer, "The Subversive Trilemma," 82.

67 Johansmeyer, "Rewriting History," 16.

68 Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, 38, no. 2 (2013): 23, https://www.jstor.org/stable/24480929.

69 Trump White House Archives, "Statement from the Press Secretary," February, 15, 2018, https://trumpwhitehouse.archives.gov/briefings-statements/statement-press-secretary-25/.

70 WannaCry is not included as an exception because the damage it caused at the time, $4 billion, is well below the 1998–2024 average. However, as one of only 24 events to meet the cyber catastrophe criteria used for this article, one could still call it noteworthy.

71 "Cyber Operations Tracker," Council on Foreign Relations (2024), https://www.cfr.org/cyber-operations/.

72 Johansmeyer, "Rewriting History," 16.

73 "Climate Change Is Showing its Claws: The World Is Getting Hotter, Resulting in Severe Hurricanes, Thunderstorms and Floods," *Munich RE,* January 9, 2025, https://www.munichre.com/en/company/media-relations/media-information-and-corporate-news/media-information/2025/natural-disaster-figures-2024.html.

74 Johansmeyer, "Why Natural Catastrophes."

75 Johansmeyer, 2026, 16.

76 Tom Johansmeyer, "Bad Decisions Have Consequences: How Cyber Security Could Fall Victim to Climate Change," *British Actuarial Journal* 30, e15 (2025): 4, https://doi.org/10.1017/S1357321725000091.

77 Mi2g, "Mimail to Become 4th Worst."

78 "Indian Hackers Target Pakistan," *BBC News,* March 13, 2003, http://news.bbc.co.uk/2/hi/technology/2847455.stm.

79 Kenneth Geers, *Strategic Cyber Security,* NATO Cooperative Cyber Defence Centre of Excellence (CCD COE, 2011), 23, https://ccdcoe.org/uploads/2018/10/2011_Proceedings_0-1.pdf.

80 Dmitri Kramarenko, "Hackers or Cyber-Soldiers?" Computer Crime Research Center.org, September 28, 2004, https://www.crime-research.org/interviews/hacker0904.

81 "Indian, Pakistani Hackers Take War to Cyberspace," *SiliconIndia*, March 14, 2003, https://www.siliconindia.com/shownews/indian-pakistani-hackers-take-war-to-cyberspace-nid-18862-cid-2.html.

82 Dennis Fisher, "Yaha Worm Spreads Beyond Middle East," *eWeek*, December 31, 2002, https://www.eweek.com/security/yaha-worm-spreads-beyond-middle-east/.

83 John Leyden, "Unhappy New Yaha," *The Register*, January 7, 2003, https://www.theregister.com/2003/01/07/unhappy_new_yaha/.

84 Leyden, "Unhappy New Yaha."

85 John Leyden, "Yaha Usurps Klez," *The Register*, July 31, 2003, https://www.theregister.com/2003/07/31/yaha_usurps_klez/.

86 "NotPetya and WannaCry Call for a Joint Response from International Community," CCDOE, https://ccdcoe.org/news/2017/notpetya-and-wannacry-call-for-a-joint-response-from-international-community/.

87 Scott Jasper, "Assessing Russia's Role and Responsibility in the Colonial Pipeline Attack," *New Atlanticist* (blog), June 1, 2021, https://www.atlanticcouncil.org/blogs/new-atlanticist/assessing-russias-role-and-responsibility-in-the-colonial-pipeline-attack/.

88 Tom Johansmeyer, "Can Cyber Insurance Survive Without Diplomatic Support?," *Global Policy,* October 5, 2021, https://www.globalpolicyjournal.com/blog/05/10/2021/can-cyber-insurance-survive-without-diplomatic-support.

89 Dan Goodin, "An NSA-Derived Ransomware Worm Is Shutting Down Computers Worldwide," *Ars Technica,* May 12, 2017, https://arstechnica.com/information-technology/2017/05/an-nsa-derived-ransomware-worm-is-shutting-down-computers-worldwide/.

90 Samuel Gibbs, "WannaCry: Hackers Withdraw £108,000 of Bitcoin Ransom," August 3, 2017, https://www.theguardian.com/technology/2017/aug/03/wannacry-hackers-withdraw-108000-pounds-bitcoin-ransom.

91 Oanda Currency Converter, https://www.oanda.com/currency-converter/en/?from=GBP&to=USD&amount=1.
The currency conversion is based on the rate for August 3, 2017, the date of the article that cites the £108,953 amount.

92 Sam Jones, "What Is WannaCry and How Can It Be Stopped?" *Financial Times,* May 12, 2017, https://www.ft.com/content/af74e3f4-373d-11e7-99bd-13beb0903fa3.

93 Oleg Yegorov, "WannaCry Hack: Why Has Russia Suffered More than Other Countries?" *Russia Beyond*, May 16, 2017, https://www.rbth.com/international/2017/05/16/wannacry-hack-why-has-russia-suffered-more-than-other-countries_763869.

94 The same issues are discussed frequently with regard to the third case study in this article, which focuses on the NotPetya cyber catastrophe event.

95 Lewis, "Dismissing Cyber Catastrophe."

96 "Implications of the WannaCry Cyber-Attack for Insurance," *Moodys*, May 17, 2017, https://www.moodys.com/web/en/us/insights/insurance/implications-of-the-wannacry-cyber-attack-for-insurance.html.

97 Nadia Khomami and Olivia Solon, "'Accidental Hero' Halts Ransomware Attack and Warns: This Is Not Over," *The Guardian,* May 13, 2017, https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack.

98 Adrian Winckles, "Here's How the Ransomware Attack Was Stopped—and Why It Could Soon Start Again," *The Conversation,* May 17, 2017, https://theconversation.com/heres-how-the-ransomware-attack-was-stopped-and-why-it-could-soon-start-again-77745.

99 "Malicious Malware: Lessons Learned and What to Expect from Cyber Crime in 2018," *TASS,* December 31, 2017, https://tass.com/economy/983704.

100 "Russian Defense Ministry Blocks WannaCry Ransomware Attack—Source," *TASS*, May 16, 2017, https://tass.com/defense/946110.

101 *TASS*, "Malicious Malware: Lessons Learned.

102 Andy Greenberg, "The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet," *Wired,* May 12, 2020, https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/.

103 Trump White House Archives, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," December 19, 2017, https://trumpwhitehouse.archives.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

104 Office of Public Affairs, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," press release, Archives: U.S. Department of Justice, September 6, 2018, https://www.justice.gov/archives/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

105 Johansmeyer, "Why Natural Catastrophes."

106 "Ransomware Cyber-Attack: Who Has Been Hardest Hit?" *BBC News*, May 15, 2017, https://www.bbc.com/news/world-39919249.

107 Johansmeyer, "Cyber Attacks in Perspective."

108 Johansmeyer et al., "Invisible Lines, Visible Impact," 25.

109 Igor Burdyga, "'Black Tuesday' of Ukraine IT: What Damage Was Caused by the Cyberattack, and Who Committed It," *Hromadske*, July 8, 2017, https://hromadske.ua/posts/naslidki-kiberataki.

110 Johansmeyer, "Cyber Attacks in Perspective."

111 Maschmeyer, "The Subversive Trilemma," 82.

112 Group-IB, "Petya Starts with Ukraine and then Goes Global," *Group-IB Blog*, June 27, 2017, https://www.group-ib.com/blog/petya/.

113 "Russia Blasts London's Groundless 'Cyberattack Against Ukraine' Allegations," *TASS*, February 21, 2018, https://tass.com/politics/991068.

114 Johansmeyer, "NotPetya, Ukraine."

115 Kevin Townsend, "Court Awards Merck $1.4B Insurance Claim Over NotPetya Cyber Attack," *SecurityWeek*, January 24, 2022, https://www.securityweek.com/court-awards-merck-14b-insurance-claim-over-notpetya-cyberattack/. The economic damage sustained by Merck is based on a $1.4 billion insurance claim from its property policy and a $275 million claim from its affirmative cyber insurance policy. Additional economic harm would have been captured by any insurance deductibles (not disclosed) and possibly led to uninsured damage, as well. This makes an approximation of total economic harm of $2 billion realistic; See "Merck & Silent Cyber Impacts Drove Petya Industry Loss: PCS," *Artemis.bm*, November 7, 2018, https://www.artemis.bm/news/merck-silent-cyber-impacts-drove-petya-industry-loss-pcs/ for information about the $275 million claim.

116 Johansmeyer, "Could NotPetya's Tail Be Growing?", 2.

117 Johansmeyer, "Could NotPetya's Tail Be Growing?", 3.

118 Jill Leovy, "Cyberattack Cost Maersk as Much as $300 Million and Disrupted Operations for 2 Weeks," *Los Angeles Times*, August 17, 2017, https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html.

119 Matteo Crosigani et al., "Pirates Without Borders: The Propagation of Cyberattacks Through Firms' Supply Chains," *Journal of Financial Economics* 147, no. 2, (2023): 442, https://doi.org/10.1016/j.jfineco.2022.12.002.

120 "Kremlin Says 'Petya' Ransomware Attack Validates Russia's Call to Fight Hackers," *TASS,* June 28, 2017, https://tass.com/politics/953672.

121 Frank Umbach, "The Rise of State-Supported Cyberattacks from Russia," *GIS Reports*, November 19, 2019, https://www.gisreportsonline.com/r/russian-cyberattacks/.

122 Maschmeyer, "The Subversive Trilemma," 83.

123 Yegorov, "Wanna Cry Hack."

124 Johansmeyer, "Recent Cyber Catastrophes."

125 Matthew R. Cook, "Nuclear Deterrence and the Space and Cyber Domains," (Naval Postgraduate School, 2022), 16, https://apps.dtic.mil/sti/trecms/pdf/AD1189488.pdf.

126 Max Smeets, "A Matter of Time: On the Transitory Nature of Cyberweapons," *Journal of Strategic Studies* 41, nos. 1-2, (2018): 7, https://doi.org/10.1080/01402390.2017.1288107.

127 Josiah Dykstra et al., "Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat," *Joint Force Quarterly* 99, (2020): 118, https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-99/jfq-99_116-123_Dykstra-Inglis-Walcott.pdf?ver=g74GeG8vGw7Qnee0ZByJIg%3D%3D.

128 Smeets, "A Matter of Time," 92.

129 Quoted in Vincent J. Esposito, "War as a Continuation of Politics," *Military Affairs* 18, no. 1 (1954): 20, https://www.jstor.org/stable/1982704.

130 Golding, "Byte, With, and Through."

Offensive cyber operations remain heavily constrained by an outdated taboo rooted in the fear of uncontrollable cyber collateral damage. In ***Small and Unthreatening: The Case for Increased Offensive Cyber Operations***, Tom Johansmeyer, PhD dismantles these hyperbolic narratives through an empirical review of the three most economically impactful state-actor cyber catastrophes in history: Yaha, WannaCry, and NotPetya. His analysis demonstrates that even when actors lost control of these tools, the actual financial and structural fallout was profoundly limited, easily absorbed, and far less severe than traditionally feared.

Ultimately, this monograph reveals that because cyber damage is inherently transitory and reversible, offensive cyber tools offer a precise, potentially de-escalatory alternative to traditional kinetic weapons. Johansmeyer makes a compelling case for military and special operations leaders to retire the legacy stigma, loosen operational restrictions, and actively embrace offensive cyber capabilities as a vital resource for modern statecraft and asymmetric engagement.

United States Special Operations Command
ATTN: JSOU Press
7701 Tampa Point Boulevard | MacDill AFB, FL 33621-5323
jsou.edu/press

JSOU PRESS
JOINT SPECIAL OPERATIONS UNIVERSITY

DIGITAL VERSION

ISBN 978-1-941715-87-1