HOW REVERSIBILITY DIFFERENTIATES CYBER FROM KINETIC WARFARE: A CASE STUDY IN THE ENERGY SECTOR

Tom Johansmeyer

Institute of Cyber Security for Society, University of Kent, Canterbury,
and PCS, a Verisk business, United Kingdom

ABSTRACT

A pair of attacks on energy sector assets offers a unique opportunity to better understand the differences in impact from cyber and kinetic warfare. A review of the 2021 cyber attack on Colonial Pipeline and the missile strike on the Syvash wind farm demonstrates the principle of reversibility in action, particularly in regard to the short-lived nature of cyber attacks. Within the context of security and strategy, particularly at the cyber/energy security nexus, this means that traditional state security thinking needs to evolve to address threats in the cyber domain rather than try to retrofit dated strategies. The two cases compared offer lessons that can be applied more broadly in the formation of state-level cyber and energy strategic thinking, ultimately improving resilience and the appropriateness of protection.

KEYWORDS

Cyber, security, strategy, energy, international relations

1. INTRODUCTION

Cyber security at the state level has been the subject of intense focus and tireless discussion for decades, with a lingering concern of the potential for apocalyptic impact and a sense that the aggressors are always a step ahead. Further, the threat environment appears to evolve constantly, effectively ensuring that a solution is never quite within reach. The domain is packed with uncertainty, which is compounded by the geopolitical volatility currently present – and rising – around the world. While it is easy to point to the conflict in Ukraine or the ransomware epidemic as symptoms of the broader risk, the threat environment features complex and compound risks that are neither easily isolated nor remedied. Concerns of nexus arise, as the points of overlapping threats require multidimensional solutions.

Along with the threats present (and growing) in the cyber domain, concerns about energy security continue to increase. In addition to the energy security implications of the conflict in Ukraine, instability in the Middle East, the proximity of the January 2022 Almaty riots to Kazakh energy assets, and China's energy relationship with Africa are salient indicators of the challenges a state faces when its access to energy is impeded. The cyber/energy nexus, therefore, is of particular concern, involving the threats directed at energy assets via the cyber domain. The U.S. General Accountability Office has indicated that a cyber attack on offshore energy platforms in the Gulf of Mexico could be as impactful as the 2010 Deepwater Horizon event [1], and that was one of the costliest such events the United States has experienced.

Unfortunately, security strategy has yet to evolve to match the unique conditions of the digital age. The prospect of state actors or their proxies causing profound and widespread harm via the

DOI: 10.5121/ijsptm.2023.12101

cyber domain of operations has led to the development of national cyber security strategies that now sit alongside national security strategies, national nuclear strategies, and other public statements of readiness and preparation. The content of those statements though, appears to miss the mark. A heavy reliance on deterrence results in a fundamental mismatch between the threats of the cyber domain (and their impacts) relative to state action. Instead of relying on Cold War strategies that required existential threats to humanity, the cyber/energy security nexus requires new thinking.

What differentiates cyber attacks from physical attacks – be they low-intensity conflicts or existential nuclear engagements – is reversibility. Simply, it is easier to undo the damage caused by a cyber attack than it is to undo the damage caused by a missile strike, bombing, or nuclear attack. The fact that cyber attacks are more reversible suggests a balanced approach to strategy that contemplates both the front-end (prevention and deterrence) as well as the back-end (resilience and recovery). Without a foundation in experience, however, this can be a difficult argument to advance. Conjecture and speculation can help the imagination run wild, resulting in hypothetical cyber conflict scenarios that belong in Hollywood more than in any risk management assessment or security strategy.

Recent experience offers the opportunity for a focused comparison of cyber and kinetic attacks on similar assets, which makes it much easier to see how cyber is more easily reversed. Two recent energy asset attacks (critical national infrastructure) show the differences clearly. In the United States, Colonial Pipeline suffered a cyber attack in 2021, and the Syvash wind farm in Ukraine was struck by a missile in 2022. The former was functioning again within five days, and the latter is not nine months after the attack, and when it will return to service remains unknown. This paper will compare the characteristics of the cyber attack on Colonial Pipeline and the kinetic attack on Syvash to show the importance of reversibility in cyber, and how that should shape security strategy.

2. DETERRENCE VERSUS REVERSIBILITY: A NEW STRATEGY FOR A NEW THREAT ENVIRONMENT

The intersection of cyber and energy security strategy comes following an evolution in security and strategy that began with a focus on military security and existential threats. Today, however, security has broken from that orthodoxy, with a few that non-military threats can have significant security implications and require thoughtful and disciplined strategy. However, that evolution has not always been smooth, and there's a tendency to prepare for the last war rather than future threats [2]. As a result, strategy focused on the cyber/energy security nexus has focused on dated approaches like deterrence, which are not a fit for the cyber domain. After reviewing the evolution of security and strategy, this section will examine the shortcomings of deterrence as a strategy, as well as the role of reversibility in undermining the effectiveness of deterrence. Finally, the differences in reversibility in cyber attacks versus kinetic attacks will be shown, providing context for the comparison of the Colonial Pipeline and Syvash events.

2.1. Security and Strategy in the Cyber Domain

To start, it helps to understand the basic principles of security and strategy, as well as how they intersect in the cyber domain. At a high level, Nye settles on "the absence of a threat to survival," with the important point that "survival is only rarely at stake"[3] Threats are therefore scarce, sitting at the far end of a spectrum of degrees of uncertainty, and most threats have much less significant potential consequences Further, security is not binary; rather, there is a continuum to security, with truly existential threats at one extreme and at the other minor hindrances or

annoyances that ultimately have little impact. There are varying degrees of uncertainty encountered in all interactions, some of which may vex, while others could be transformational (or even fatal).

Like security, strategy can be difficult to define, which makes the digest of definitions that Baylis and Wirtz offer particularly useful. Of the nine definitions curated, five reference some variation of war, military, force, or "armed coercion," with the remainder far more flexible, to the point that they even reflect Nye's notion of soft power, which consists of "attraction and persuasion"[4,5]. Foster's thoughts about "effectively exercising power" are open to interpretation beyond use of force, and Wylie's view is wider still, discussing the use of a plan to accomplish something in particular, which in turn resonates with Osgood's thoughts on planning and Murray's and Grimslay's on "process"[6]. Freedman states that strategy is "about getting more out of a situation than the starting balance of power would suggest" [7]. Strategy clearly involves the accumulation and use of some amount of power, which Lake says "is the ability of one state to get another to do something it would not otherwise do"[8]. Gompert and Binnendijk explain that power "spans a spectrum, from offensive military force at one end to routine diplomacy at the other" [9].

Security and strategy are slippery terms to define, and the effort is complicated further when cyber is integrated into the discussion. The cyber domain is not confined by physical space, is new, and is rapidly changing. However, cyber does share many characteristics with traditional, orthodox views of security and strategy, from the role of a potential aggressor (usually a state or state-affiliated entity) to ambitions that can include securing a geopolitical advantage or impeding the sovereignty or security of an adversary. Yet, while the aspirations associated with cyber operations and other attacks can be high, the impacts have tended to be limited as a result of rapid recovery times, dulling the impact of such events. Gartzke, for example, observes, "To the degree that damage can be quickly and easily repaired, there is not much leverage in raising" threats of force [10].

Nonetheless, concerns about the potential implications of a "Pearl Harbor moment for cybersecurity" persist [11], even if such risks are remote and have little in the way of precedent. Rid straightforwardly asserts, "Cyber war has never happened in the past. Cyber war does not take place in the present. And it is highly unlikely that cyber war will occur in the future" [12]. In fact, Lorenzo Franchesci-Biccherai claims to be reluctant to use the term "cyber war" at all because it is often "used in the wrong situations [and] led to hyperbole" [13].

Unfortunately, the likes of Franchesci-Biccherai and Rid appear to have lost the fight over strategy, as evidenced by the contents of national security strategies and national cyber security strategies among the world's cyber powers. Reliance on deterrence as a security strategy for the cyber domain demonstrates the concern that cyber war is a key state-level consideration. In the United States, for example, the commitment to overmatch strength as a mechanism for deterrence appears to be the only real play across both administrations, which is surprising given the history of cyber attacks the United States claims to have endured in the strategies offered by both administrations. Further, the Department of Defense, Air Force, and Cyber Command have "released strategies and thought pieces around cyber deterrence" [14], although in fairness at least one U.S. Air Force piece positions cyber deterrence as possible but not with the current strategy [15]. NATO has published pieces in support of widening cyber deterrence, as well [16].

The Russian Federation's use of deterrence in its national cyber security apparatus may appear to be more sparing, but it really manifests with nuance. In the 2016 Doctrine of Information Security of the Russian Federation, the Russian Federation identifies "strategic deterrence" as an element of "ensuring national security in the field of national defence" [17]. While that may be

brief, it links to another brief mention of deterrence, this one in the 2021 Strategy of national security of the Russian Federation, in which "strategic deterrence and the prevention of military conflicts" is specifically identified [18]. However, a deeper review of the Russian national security strategy apparatus and attendant commentary suggests that strategic deterrence is very much in play in the Russian national cyber security strategy [19].

The United Kingdom, surprisingly, is quite different from the United States (and the Russian Federation) on the issue of deterrence. While there is some reference to it [20], the United Kingdom instead focuses on resilience defined as "the ability of an organization to maintain the delivery of its key functions and services and ensure the protection of its data, despite adverse cyber security events" [21]. Key themes include responsibility, leadership, partnership, and overarching values, such as the maintenance of a "free, open, peaceful and secure cyberspace" [22]. Cybersecurity in defense of "open societies and open economies" becomes an investment in growth and prosperity rather than spend on defense [23].

If deterrence implies the continued escalation of armament (physical or virtual) until one is able to convince adversaries to accept being deterred [24], resilience does quite the opposite. Rather than invest in the prevention of attacks, resilience operates from the acceptance that some attacks will occur – with punches that land – and commits investment into the ability to recover. Conceptually, this links to the concept of reversibility discussed above. With high levels of reversibility from some types of threat (in this case, cyber), focusing on minimizing the impact of an attack and recovering quickly makes far more sense than overinvesting in prevention via deterrence, a process that can ultimately lead to escalation rather than a reduction in risk.

Of course, there is a need for both pre-attack (e.g., deterrence and engagement) and post-attack (e.g., resilience, recoverability) strategies, and they need to be balanced. Aside from the United Kingdom's position, though, greater emphasis has been placed on deterrence, and that appears unlikely to change anytime soon. The problem is that deterrence is familiar, and as a result it offers a high degree of comfort. That takes on outsized meaning in a new and as yet ill-understood domain like cyber. The broad reliance on deterrence hearkens back to the Cold War-era treatment of the nuclear threat, in which there truly was no alternative to deterrence.

Deterrence has been effective in the nuclear sphere because of the severity of the consequences of a failure of deterrence: "Whoever shoots first dies second" [25]. After all, the prospect of a third strike – after a first strike and a response – is unlikely [26, 27] (, and even if it does happen, the future is pretty certain anyway. Fundamental to nuclear deterrence is the belief that, with nuclear aggressor-responder pairs assured of reaching a conclusion in which nobody wins, there is no incentive for aggression. The stakes involved conceal another important element of deterrence – agreement to be deterred [28]. Deterrence only works when the targeted party changes their behavior in a manner consistent with having been deterred. The problem for the cyber domain is that the agreement to be deterred – the crucial point in Gray's views on the effectiveness of deterrence as a strategy – has not been achieved, and it seems as though it will not be. Holcomb says as much: "Hostile actors such as Russia and China have not been deterred by Western policy responses" [29].

Cyber does not work this way. In fact, the application of the Russian Federation's philosophy of "information confrontation" – which brings together both cyber and information warfare [30] – demonstrates that the stakes tend to be low enough that "mutually assured destruction" is not a likely outcome. In fact, some have argued, such as Valeriano, Maness, and Jensen, that cyber attacks and other engagement in cyber warfare have been (and are unlikely) to result in escalation [31], which is effectively the polar opposite of deterrence. Unfortunately, deterrence is a difficult addiction for governments to give up, which is perhaps why Smeets refers to it as the "most

frequently referred-to strategy"[32], even if Gray believes it was one of the best ideas of the 1950s[33].

Cyber weapons are not nuclear weapons, though, and they need their own strategy. Fundamental to achieving this is to identify and evaluate the key differences between the effects of cyber and nuclear arms. Principal among them is the concept of reversibility, specifically that "cyberweapons … have a short-lived or temporary ability to effectively cause harm"[34]. Cyber attacks simply do not last as long as kinetic attacks, and returning to normal simply faster and less expensive. This stands in stark contrast to nuclear attacks. As a result, deterrence makes less sense for the cyber domain.

2.2. The Difference in Permanence from Cyber to Kinetic Warfare

Kinetic warfare falls between cyber and nuclear engagement in terms of impact and reversibility, and of course, it has its own spectrum bounded by that running from cyber to nuclear engagement. Kinetic warfare can be localized, low-intensity, and relatively contained, or it can span powers and entail a lengthy, broad, and devastating scope. For the purposes of understanding the role of reversibility in cyber relative to kinetic attacks in regard to energy security, what is important to note is that cyber warfare, generally, lacks the enduring effect of kinetic engagement. Damage from cyber attacks is easier to reverse. This has become evident throughout the conflict in Ukraine in 2022, although it requires some comparison to attacks outside the conflict. Kinetic warfare in Ukraine can be compared to cyber attacks outside the country – both on energy targets – to enable a clear analysis of the effectiveness of each.

Kinetic warfare is easy to see and thus to understand. Damaged buildings and vehicles hint at the human toll, which of course runs much deeper than property. Moreover, the time that such damage persists reinforces the notion that kinetic attacks can be relatively difficult to reverse. A walk through Sarajevo or Mostar, in Bosnia-Hercegovina, puts one face to face with war ruins that are three decades old and still yet to be repaired. While the conflict in Ukraine is still new and ongoing, efforts to quantify the damage reveals the scale of the problem. The ongoing conflict in Ukraine has led to extensive damage to businesses and communities. At least "60% of industrial enterprises have been destroyed or shut down," according to Vitaliy Daviy, CEO of cleantech company IB Centre Inc.[35].In the renewable energy sector, 60% of installed capacity near or in areas of active fighting, and 30-40% of that capacity presumed damaged by energy data firm Kosatka [36]. The Kiev School of Economics estimates the cost of physical damage from the conflict at more than $127 billion [37].This is three times the largest cyber attack, as measured by economic impact, as seen in Table 1.

Table 1: Economic losses from historical cyber attacks

Event	Year	Economic Loss[1]
MyDoom	2004	$38 billion
SoBig	2003	$37 billion[2]
Klez	2001	$19.8 billion
ILOVEYOU	2000	$15 billion[3]
Petya/NotPetya	2017	$10 billion
StormWorm	2007	$10 billion
Conficker	2007	$9.1 billion
WannaCry	2017	$4 billion
Zeus	2007	$3 billion
Code Red	2001	$2.4 billion[4]
Nimda	2001	$1.5 billion
Melissa	1999	$1.1-1.5 billion
SirCam	2001	$1.15-1.25 billion
SQL Slammer	2003	$1.2 billion[5]
CryptoLocker	2013	$665 million
Sasser	2004	$500 million

Sources: [38,39,40,41,42]

Nonetheless, chatter about the severe risks of cyber warfare, the prospect of a cyber "Pearl Harbor" or even a "cyber [Hurricane] Andrew," and the need for a nuclear-caliber strategy (i.e., deterrence) has not only persisted but escalated [43]. The treatment of cyber security threats appears to be dislocated from historical precedent and nearly all available evidence. Even the notion of a knock-on effect from a cyber attack – like "crashing the grid" –is not only remote but less likely and less impactful than a kinetic attack on energy and power assets[44]. The conflict in Ukraine and 2021 wave of ransomware attacks in the United States yielded an opportunity at like-for-like comparison. Kinetic attacks on energy assets in Ukraine in 2022 and cyber attacks on energy assets in the United States in 2021 may not offer a perfect basis for comparison, but the parallels are sufficiently close to allow for an important case study review in the differences in impact between cyber and kinetic attacks, as well as what the comparison says about reversibility, which can be applied to future security and strategy exercises.

3. A STUDY IN CONTRASTS: COLONIAL PIPELINE AND SYVASH

Vulnerabilities in the energy sector have been of considerable concern in a world where energy security can be compromised by a wide range of factors, from armed conflict to economic actions (e.g., sanctions) to supply chain disruption. The conflict in Ukraine has had salient energy security concerns for many countries in the region, such as Germany and Moldova [45,46], and around the world. Simultaneously, concerns about cyber security and energy have arisen. A study by the U.S. Government Accountability Office (GAO), for example, has found that an attack on the country's network of 1,600 offshore facilities could lead to effects resembling those of the 2010 Deepwater Horizon loss[47]. As a reference point, the industry-wide loss to the insurance industry alone from that event was more than $3 billion, according to data from PCS, a Verisk business [48]. Clearly, threats to energy infrastructure bring involve significant economic

[1] Where there are multiple sources with different estimates, the highest is presented.
[2] Gerencer has it at only $30 billion.
[3] Leman is the outlier at $10 billion.
[4] Cyware Hacker News has it at only $2 billion.
[5] Cyware Hacker News has it at only $750 million, but Gerencer and Leman are at $1.2 billion.

vulnerability, along with secondary risks, such as civil unrest resulting from energy insecurity, as seen during the summer and autumn of 2022 in Moldova [49].

The vulnerability at the cyber/energy security nexus manifested in 2021 and 2022, with significant cyber and kinetic attacks having come to bear. The United States was home to the high-profile cyber attack on Colonial Pipeline, in May 2021, and in 2022, the kinetic conflict in Ukraine has led to widespread energy infrastructure damage, including renewable energy, utilities, and nuclear plants [50,51]. This has led to a rare opportunity to test the concept of reversibility at a granular level, as it relates to energy security in the cyber domain and physical world – and see how it manifests in the face of real-world cyber and kinetic attacks. Although there are complicating factors in the comparison, what is clear is that cyber attacks, under difficult circumstances extrapolated from what was seen in the Colonial Pipeline event, still appear to be much more easily reversed than those from kinetic warfare.

3.1. United States: Colonial Pipeline

Ransomware gang DarkSide shut down Colonial Pipeline on May 7, 2021[52], which took five days to bring back up[53,54,55]. During that period, fuel shortages led to panic buying up and down the east coast of the United States [56]. However, it was brief. The impact from the attack itself turned out to be minimal. Within a few days, at least on the surface, everything seemed to be back to normal, with the understanding that there is always a lag period where operational workarounds revert back to standard operations and other underlying issues, which may not be visible to the public, are addressed. The insured loss from the event is estimated at approximately $10 million, with little indication of further economic loss[57]. Compared to other cyber attacks – again, refer to Table 1 – Colonial Pipeline did not have a significant economic effect. Even the 2017 Equifax breach's $1 billion economic impact, which did not affect critical national infrastructure, puts the cost of the Colonial Pipeline event in perspective [58].

While the attack on Colonial Pipeline may not have had a significant direct impact, it did affect perspective. It offered a frightening glimpse of how easily an important energy asset could be lost, and what that asset would mean for the broader supply chain – and society as a whole. Further, the cyber attack was sufficient to fuel escalating hypotheticals, ranging from the implications of an increase in the duration of the outage to a mass simultaneous attack on cyber energy and other critical national infrastructure assets. What if the pipeline had been shut off longer? What if we lost two at the same time? What other energy targets are vulnerable? It is easy to get lost in that sort of speculation.

Further, post-event speculation includes meaningful mitigation factors from the way the event unfolded. For example, the attack was easy to reverse in part because a ransom was requested – and that ransom (initially $5 million) was seemingly manageable for the victim [59]. Ransomware gangs, which are financially motivated, facilitate the reversal of damage upon payment, and in fact, many are eager to do so, fearing the reprisals that can come when an operation is high-profile [60]. State actors may not be so easily bought, and when money is not the motivation, attacks need to be reversed without the help of the attacker, as was the case with the WannaCry and NotPetya attacks. However, even then, the ability to operate largely returned within weeks.

As a result, the main lesson from the Colonial Pipeline attack is that reversibility certainly constrains the amount of possible damage, and reversibility can be improved when the attacker has financial motivations. However, even without the ability to pay for relief, cyber attacks can still be unwound relatively easily (although with some aggravating factors). The "doomsday scenario" may be so remote as to be of little immediate concern, even for those in the security

space, and the most realistic severe threats can be managed post-attack if they can't be handled pre-attack. This is not a suggestion that defenses can be removed or deprioritized. Prevention remains crucial. However, planning for recovery in the event of an attack can make more sense than the prevent-at-all-costs posture implied by a reliance on strategies like deterrence. To understand why the potential for cyber damage remains relatively low, it helps to look at what kinetic attacks can do, as evidenced by the missile strike on the Syvash wind farm in Ukraine.

3.2. Ukraine: Syvash Wind Farm

A missile struck the Syvash wind farm was March 3, 2022, and it caused considerable physical damage [61]. Subsequently, the wind farm was shut down and the staff evacuated, with the facility ultimately occupied by the attacking force. No reports of any resumption of operations have been released since the attack, implying that the Syvash wind farm remains unproductive, with reports of damage coming as recently as September 4, 2022[62]. Further, the Syvash wind farm is in territory still occupied, as shown on a map offered by the Institute for the Study of War viewed on December 14, 2022[63], which suggests it is unlikely to return to operation in the near future. When repairs can begin – an eventuality impossible to predict – the process could be slowed by parts and equipment shortages, as suggested by key manufacturer Vestas[64]. Quite simply, the Syvash wind farm has been down for nine months and is likely to be down for many more as a result of the kinetic attack.

While the Colonial Pipeline attack fueled speculation about how much worse the attack could have been, such an exercise is not necessary for the kinetic attack in Ukraine. The Syvash wind farm is one of at least four to have been damaged, along with at least three solar facilities and numerous other energy assets [65]. The wind farm damage alone could cost the global insurance industry as much as $800 million [66], with other economic impact from the widespread effects on energy assets across the country. The attack on Syvash alone could cost several hundred million dollars (as part of the $800 million, above), which makes it far more directly impactful than the cyber attack on Colonial pipeline. The open question that remains is what the ultimate economic and societal cost of the Syvash attack will be, as well as the damage to peer facilities. For now, the future is uncertain: It's impossible to tell when Ukraine's renewable energy capabilities will be restored, but the process is likely to take years.

Unlike a cyber attack, which may have some physical damage implications but is largely a virtual endeavor, kinetic activity requires that parts be sourced and shipped and local repairs made– all of which starts with physical access to the damage site. That alone could take months, depending on how long the conflict persists. And supply chain challenges could frustrate the problem further. In fact, Vestas has indicated that current supply chain woes are more significant than the effects of the cyber attack they experienced in 2021[67]. The long time expected for repair, shortage of materials, and inability to start until the conflict cools off illustrate the difference in magnitude between cyber and kinetic attacks. Even the financial consequences could be more severe. While bankruptcy is often cited as a risk from cyber attacks [68], Kosatka indicates that it could become an issue for several Ukrainian renewable energy companies [69].

A true side-by-side comparison remains impossible, for now, because the impacts to Syvash are ongoing, given that the conflict has not yet been concluded. In addition to the potential for further physical damage to the Syvash facility, speculation as to how much worse the situation could get will continue to be fed by the accumulation of damage from further kinetic activity, with the assumption that imagination can always add to the scale experienced in developing a hypothetical worst-case scenario. However, despite the lack of rigor resulting from the fact that one point of comparison is still in progress, it is possible to develop some key observations that can be put to immediate use in security and strategy at the cyber/energy security nexus.

3.3. Reversibility Makes a Noticeable Difference

The direct comparison of Colonial Pipeline and Syvash makes clear the claims of analysts and scholars over the past decade. The potency of cyber attacks is constrained by their ability to be reversed. In fact, the role of reversibility in the different outcomes in the two attacks is impossible to ignore, particularly given the speed and ease with which Colonial Pipeline recovered from the cyber attack. It was up and running again within a week. Syvash, on the other hand, will take months or even years to become active again.

It is easy to focus on the mechanics of reversibility as the reason why cyber attacks are less permanent than kinetic attacks, and there is some merit to the view. The cyber recovery process is at least in part virtual. Even if there is a physical damage component, it has tended to be both rare and limited in comparison to lack of access to systems or the destruction of data. Although a perfect recovery is difficult (or even impossible, in some cases) to achieve, being able to function in a manner short of full restoration is nonetheless possible. A partial recovery buys more time to finish the process while minimizing the impact of the attack.

The characteristics of the Colonial Pipeline attack did lend themselves to reversibility in a way that the characteristics of other cyber attacks do not, as mentioned above, and this is meaningful to the comparison with Syvash. Because DarkSide's motivation was financial, the group was able to put a price on reversibility, and upon receiving payment indeed did its part to reverse the damage, although there were steps to be taken after by Colonial Pipeline. When the attack involves motives other than finance – and when the attacker is either a state or a non-state party advancing either a sponsoring state's agenda or other ideological purpose – the process of recovery may be more difficult. The actor would be less likely to serve as a "partner" in reversing the attack, likely elongating the period to recover. Yet, even with a truly adversarial attacker (rather than a collaborative attacker that wants to get paid, as in the case of most ransomware events), the cyber attacks appear to be more reversible than kinetic attacks.

Although measures such as duration of down time are blunt instruments, they do provide an easy reference point for comparison. Colonial Pipeline's five days versus the nine months (so far) experienced by Syvash demonstrates immediately a profound difference in scale, as does the insured loss associated with each. Using insured loss as a proxy for economic impact, Syvash is twenty times more severe than Colonial Pipeline. Although there is plenty of room for debate around whether that difference should be narrowed (or even broadened), the scale alone is enough to render bickering over the delta unnecessary. Moreover, Syvash is still down, and it likely will be for quite a while.

One thing is clear, though: Cyber is reversible, while kinetic attacks are less so. Although the cases are not mirror images, the differences between the impacts of the cyber attack on Colonial Pipeline and the missile strike on Syvash are indicative of a difference in scale and reversibility. The vulnerability of critical national infrastructure, such as energy assets, requires a modern take on security and strategy, rather than a fallback to deterrence that inflates the nature of cyber risk. There are many lessons one can take from the Colonial Pipeline/Syvash comparison, and among the most important is the need to tailor strategy to the nature of the threat.

4. CONCLUSION

Subtlety and nuance make everything more difficult, and that holds true for security and strategy. Moreover, the cyber/energy security nexus is packed with subtlety and nuance, as one would expect from a risk environment sensitive to geopolitical volatility and a domain that is both new and evolving. Understanding security and strategy at the cyber/energy security nexus is a lot like trying to shoot a moving target from a moving car – where the target and the car move unpredictably. That said, the threat environment can be tamed through careful analysis, a review of the cases that are available as new events arise, and the development of thinking and models that are directly relevant to the risk environment. So far, that has not happened, as evidenced by the continued reliance of major cyber powers on deterrence. Thankfully, though, change is on the horizon.

The differences between the effects of cyber and kinetic attacks as demonstrated in the comparison of Colonial Pipeline and the Syvash wind farm reveal not just how cyber warfare is different from kinetic warfare but also that cyber warfare is different from the expectations of the security community, with those expectations expressed in national security strategies and similar domain-specific statements. Cyber threats are certainly meaningful, escalating, and evolving, but they manifest differently from kinetic threats. The impact of cyber attacks is not enduring because the damage is more easily reversed. This does not mean that cyber is not an important threat environment. In fact, it is sufficiently important to warrant a specific and relevant approach to strategy.

So far, cyber has been stuck with deterrence, much like every other major state-level security threat. Given that cyber is more reversible than other threats, though, deterrence does not make sense. Deterrence aligns with a permanence of impact. Cyber, on the other hand, benefits from rapid recovery capabilities. The lessons from Colonial Pipeline demonstrate this. Even when removing favorable risk dimensions, such as the willingness of ransomware actors to collaborate on a resolution (which of course involves payment), cyber remains more reversible than kinetic attacks. Applying some characteristics from the Equifax breach or NotPetya attack to the Colonial Pipeline case may make the duration and extent of the attack, on a hypothetical basis, more severe, but that still would not rise to the extent witnessed with Syvash and its peers.

The details of the Colonial Pipeline/Syvash comparison can be extrapolated back up to state-level challenges at the cyber/energy security nexus. States have invested in both cyber and energy security strategies, as well as overarching security strategies. A better understanding of the differences between the Colonial Pipeline and Syvash attacks should inform those plans and perspectives, enabling states to implement security strategies that are directly relevant to the threats they face, rather than trying to retrofit decades-old thinking (i.e., deterrence) into the modern age. Two specific attacks in the energy may not be enough to reshape strategy, but they certainly offer an input into the process, not to mention a starting point for the exercise.

5. AUTHOR CONFLICT STATEMENT

The author is head of PCS at data/analytics firm Verisk (www.verisk.com/pcs). The views expressed herein are those of the author, based on research conducted by the author, and may not necessarily represent the views of others, unless otherwise noted. PCS, a Verisk business, generally provides data and analytics to the global re/insurance and ILS markets. PCS captures reported loss information on certain events, which encompasses, on average, approximately 70% of the market. Any reference to industry-wide is based on this research and the author's view of trends in the industry and does not necessarily represent the view(s) of others in the industry.

REFERENCES

[1] United States Government Accountability Office (GAO), (2022)Offshore Oil and Gas: Strategy Urgently Needed to Address Cybersecurity Risks to Infrastructure,October. [https://www.gao.gov/assets/gao-23-105789.pdf]

[2] Smoler, Fredric, (2001)"Fighting the Last War – and The Next,"American Heritage,52(8), https://www.americanheritage.com/fighting-last-war-and-next [Accessed 14 December 2022].

[3] Nye, J.S. (1974)"Collective Economic Security,"International Affairs, 50(4), pp. 585.

[4] Baylis, John &James J. Wirtz, (2016),"Introduction: Strategy in the Contemporary World,"Strategy in the Contemporary World, Oxford University Press. 5th Edition, p. 4.

[5] Nye, Joseph Jr. (2017),"Soft power: the origins and political progress of a concept,"Palgrave Communications, 3(17008), 21 February,https://www.nature.com/articles/palcomms20178 [Accessed 20 November 2021].

[6] Baylis & Wirtz, p. 4.

[7] Ibid.

[8] Lake, David. A. (2007) "Escape from the State of Nature: Authority and Hierarchy in World Politics,"International Security,32(1), p.51.

[9] Gompert, David C. & Hans Binnendijk (2016)The Power to Coerce: Countering Adversaries Without Going to War, RAND Corporation, Santa Monica, California, p. 2.

[10] Gartzke, Erik (2013)"The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,"International Security,38(2), p. 56.

[11] Reeder, Joe R. &Tommy Hall (2021)"Cybersecurity's Pearl Harbor Moment,"The Cyber Defense Review,6(3), p. 15.

[12] Rid, Thomas (2012), "Cyber War Will Not Take Place,"Journal of Strategic Studies,35(1), p. 6.

[13] Galt, Matthew (2022)"Ukraine's Decentralized Cyber Army,"CYBER,19 July.

[14] Hammer, Ann E.; Trisha H. Miller; & Eva C. Uribe (2020)Resilient Energy Systems and Cyber Deterrence and Resilience Strategic Initiative: Cyber Resilience as a Deterrence Strategy, September. Albuquerque: Sandia National Laboratories, p. 16.

[15] McKenzie, Timothy M. (2017)"Perspectives on Cyber Power: Is Cyber Defense Possible?"Air Force Research Institute Papers,January, p. 13.

[16] Burton, Joe. 2018. Cyber Deterrence: A Comprehensive Approach? The NATO Cooperative Cyber Defence Centre of Excellence. January, p. 27.

[17] Russian Federation (2016)Doctrine of Information Security for the Russian Federation. 5 December, p. 7.

[18] Russian Federation (2021)National Security Strategy, https://acrobat.adobe.com/link/review?uri=urn:aaid:scds:US:438ab784-5cb3-409f-b6bc-920eee9a30bb#pageNum=1 [Accessed 18 July 2022], p. 12.

[19] Hakala, Janne & Jazlyn Melnychuk (2021)Russia's Strategy in Cyberspace, Riga: NATO Cooperative Cyber Defence Centre of Excellence, p. 10.

[20] HM Government (2022)National Cyber Strategy 2022: Pioneering a cyber future with the whole of the UK, p. 13.

[21] HM Government (2022), p. 19.

[22] HM Government (2021)Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy,March, p. 41.

[23] HM Government (2021), p. 18.

[24] Gray, Colin S. (2000) "Deterrence in the 21st Century,"Comparative Strategy, 19(3), pp. 256.

[25] NuclearFiles (2022)"Mutually Assured Destruction,"NuclearFiles.org: Project of the Nuclear Age Peace Foundation,http://www.nuclearfiles.org/menu/key-issues/nuclear-weapons/history/cold-war/strategy/strategy-mutual-assured-destruction.htm [Accessed 11 December 2022].

[26] Snow, Donald M. (1979)"Current Nuclear Deterrence Thinking: An Overview and Review,"International Studies Quarterly,23(3), pp. 449.

[27] Rublee, Maria Rost (2020)"3. Nuclear Deterrence Destabilized,"Perspectives on Nuclear Deterrence in the 21st Century. Eds. Beyza Unal, Yasmin Afina, and Patricia Lewis. Chatham House: London, p. 14.

[28] Gray, p. 257.

[29] Holcomb, Franklin. [No year given] Countering Russia and Chinese Cyber-Aggression: Prospects for Transatlantic cooperation, Washington, D.C.: Center for European Policy Analysis, p. 1.

[30] Hakala and Melnychuk, p. 5.
[31] Valeriano, Brandon; Ryan C. Maness; & Benjamin Jensen (2021) "What Do We Know About Cyber War?" What Do We Know About War,eds. Sara Mclaughlin Mitchell and John A. Vasquez. Rowman & Littlefield Publishers: Lanham, p. 5.
[32] Smeets, Max (2018)"A matter of time: On the transitory nature of cyberweapons,"Journal of Strategic Studies,41(1-2), https://www.tandfonline.com/doi/full/10.1080/01402390.2017.1288107[Accessed 29 June 2022], p. 92.
[33] Gray, p. 255.
[34] Smeets, Max (2020)"Cyber Deterrence Is Dead. Long Live Cyber Deterrence!"Council on Foreign Relations,18 February,https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence [Accessed 14 July 2022].
[35] Daviy, Vitaliy (2022)"Ukraine: Is there a pessimistic solar scenario? No!"pv magazine, 2 May,https://www.pv-magazine.com/2022/05/02/ukraine-is-there-a-pessimistic-solar-scenario-no/ [Accessed 14 December 2022].
[36] Ignatiev, Stanislav (2022)"Destroyed by the war and on the verge of bankruptcy. What's the future of green energy in Ukraine?"Kosatka Media,12 April,https://kosatka.media/en/category/vozobnovlyaemaya-energia/news/zelenaya-energetika-v-ukraine-razrushena-voynoy-i-na-grani-bankrotstva-chto-dalshe [Accessed 14 December 2022].
[37] Kyiv School of Economics (KSE) (2022) "The total amount of damage caused to Ukraine's infrastructure is more than $127 billion – KSE Institute's report as of September 2022,"Kyiv School of Economics,21 October,https://kse.ua/about-the-school/news/the-total-amount-of-damage-caused-to-ukraine-s-infrastructure-is-more-than-127-billion-kse-institute-s-report-as-of-september-2022/ [Accessed 14 December 2022].
[38] Beattie, Andrew (2012)"The Most Devastating Computer Viruses,"Techopedia,6 March,https://www.techopedia.com/2/26178/security/the-most-devastating-computer-viruses [Accessed 27 August 2022].
[39] Cyware Hacker News (2016) "Most Expensive Computer Viruses of All Time,"Cyware Social,30 August,https://cyware.com/news/most-expensive-computer-viruses-of-all-time-de0d5fae [Accessed 27 August 2022].
[40] Gerencer, Tom (2020) "The Top 10 Worst Computer Viruses in History,"HP Tech Takes,4 November,https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history [Accessed 27 August 2022].
[41] Greenberg, Andy (2018)"The Untold Story of NotPetya, the Most Devastating Cyberattack in History,"Wired,. 22 August,https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ [Accessed 27 August 2022].
[42] Leman, Jennifer (2019) "11 Malware Attacks That Nearly Wrecked the Internet,"Popular Mechanics, 31 October,https://www.popularmechanics.com/technology/security/g29625471/history-of-malware-attacks/ [Accessed 27 August 2022].
[43] Girnius, Tomas & Scott Stransky (2015) "What Might a 'Cyber Andrew' Look Like?"Carrier Management,27 September,https://www.carriermanagement.com/features/2015/09/27/145732.htm [Accessed 14 December 2022].
[44] Uchill, Joe (2018) "Why 'crashing the grid' doesn't keep cyber experts awake at night,"Axios,.23 August,https://www.axios.com/2018/08/22/why-crashing-the-grid-doesnt-keep-cyber-experts-awake-at-night [Accessed 14 December 2022].
[45] Stelzenmüller, Constanze (2022) "Putin's war and European energy security: A German perspective on decoupling from Russian fossil fuels,"Brookings,7 June, https://www.brookings.edu/testimonies/putins-war-and-european-energy-security-a-german-perspective-on-decoupling-from-russian-fossil-fuels/ [Accessed 14 December 2022].
[46] Necsutu, Madalin (2022) "Russian Strikes on Ukraine Threaten Moldova's Energy Security,"BalkanInsight,16 November,https://balkaninsight.com/2022/11/16/russian-strikes-on-ukraine-threaten-moldovas-energy-security/ [Accessed 14 December 2022].
[47] GAO, p. 19.
[48] Johansmeyer, Tom & Ted Gregory (2018)PCS Global Risk Loss Report FY2017, p. 3. [https://www.verisk.com/siteassets/media/pcs/pcs-global-risk-loss-report-2017.pdf]
[49] Fati, Sabina (2022)"Moldova PM: 'Greatest threats relate to energy security,'"Deutsche Welle,1 December,https://www.dw.com/en/moldova-pm-greatest-threats-relate-to-energy-security/a-63950354 [Accessed 14 December 2022].

[50] Johansmeyer, Tom (2022) "Damage to Ukraine's renewable energy sector could surpass $1 billion,"Bulletin of the Atomic Scientists, 20 April,https://thebulletin.org/2022/04/damage-to-ukraines-renewable-energy-sector-could-surpass-1-billion/ [Accessed 11 December 2022].
[51] KSE.
[52] Bing, Christopher & Stephanie Kelly (2021) "Cyber attack shuts down U.S. fuel pipeline 'jugular,' Biden briefed," Reuters, 8 May, https://www.reuters.com/technology/colonial-pipeline-halts-all-pipeline-operations-after-cybersecurity-attack-2021-05-08/ [Accessed 14 December 2022].
[53] Lyons, Kim (2021) "Colonial Pipeline says operations back to normal following ransomware attack," TheVerge, 15 May, https://www.theverge.com/2021/5/15/22437730/colonial-pipeline-normal-ransomware-attack-fuel [Accessed 14 December 2022].
[54] Parfomak, Paul W. & Chris Jaikaran (2021)Colonial Pipeline: The DarkSide Strikes,. 11 May, Congressional Research Service, p. 1.
[55] Schwirts, Michael & Nicole Perlroth (2021) "DarkSide, Blamed for Gas Pipeline Attack, Says It Is Shutting Down, "New York Times,8 June. https://www.nytimes.com/2021/05/14/business/darkside-pipeline-hack.html [Accessed 14 December 2022].
[56] Romo, Vanessa (2021) "Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack," NPR, 11 May, https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack [Accessed 14 December 2022].
[57] Johansmeyer, Tom(b) (2022) "Insurance Instead of Deterrence: A Pivot in Cybersecurity Strategy, "The SAIS Review of International Affairs,22 June,https://saisreview.sais.jhu.edu/insurance-instead-of-deterrence-a-pivot-in-cybersecurity-strategy/ [Accessed 14 December 2022].
[58] Johansmeyer, Tom (2019)Handling Original Risk: Making Sense of Cyber Catastrophe Claims, p. 6, https://www.verisk.com/siteassets/media/pcs/handling-original-risk.pdf [Accessed 14 December 2022].
[59] Schwirtz & Perlroth.
[60] Smilyanets, Dmitry (2021) "An interview with BlackMatter: A new ransomware group that's learning from the mistakes of DarkSide and REvil,"The Record. 2 August,https://therecord.media/an-interview-with-blackmatter-a-new-ransomware-group-thats-learning-from-the-mistakes-of-darkside-and-revil/ [Accessed 14 December 2022].
[61] Filbert, Anne (2022) "Russian rocket attack against Ukrainian wind farm,"EnergyWatch,"3 March 2022,https://energywatch.com/EnergyNews/Renewables/article13792263.ece [Accessed 14 December 2022].
[62] Energy Charter Secretariat (2022). Ukrainian energy sector evaluation and damage assessment – II (as of September 24, 2022), Belgium: International Energy Charter, p. 15.
[63] Institute for the Study of War (ISW) (2022)"Interactive Map: Russia's Invasion of Ukraine,"Institute for the Study of War,"https://storymaps.arcgis.com/stories/36a7f6a6f5a9448496de641cf64bd375 [Accessed 14 December 2022].
[64] Frangoul, Anmar (2022) "Wind turbine maker warns of volatile business environment as inflation and supply chain issues bite,"CNBC,26 January,https://www.cnbc.com/2022/01/26/wind-energy-faces-tough-2022-as-supply-chain-issues-persist-vestas.html [Accessed 14 December 2022].
[65] Energy Charter Secretariat, p. 15.
[66] Johansmeyer (2022).
[67] Frangoul (2022).
[68] Johnson, Robert, III. (2019) "60 Percent of Small Companies Close Within 6 Months of Being Hacked,"Cybercrime Magazine,2 January,https://cybersecurityventures.com/60-percent-of-small-companies-close-within-6-months-of-being-hacked/ [Accessed 14 December 2022].
[69] Ignatiev (2022).

AUTHOR

Tom Johansmeyer is working on his PhD in international conflict analysis at the University of Kent, Canterbury, with a focus on the role of the cyber insurance protection gap in economic security. Additionally, he leads PCS at data/analytics firm Verisk, a group that estimates the industry-wide insured losses associated with major natural and man-made disasters. Tom's work has appeared in such publications as Harvard Business Review, Bulletin of the Atomic Scientists, Journal of Global Politics and Current Diplomacy, The Journal of Risk Management and Insurance, Small Wars Journal, and the World Economic Forum Global Agenda. Based in Bermuda, Tom is an avid cyclist, swimmer, and coffee-drinker. He has a BA in philosophy and history from Ripon College in Wisconsin, an MBA in accounting from Suffolk University in Boston, and is wrapping up an MA in global diplomacy at the University of London's School of Oriental and African Studies.