INSTITUTE FOR HOMELAND SECURITY

IF Insight Forward

Sam Houston State University

Collaboration Not Convergence:

Exploring Cyber-Physical Security Convergence to Prevent or Mitigate Techno-Kinetic Attacks

Institute for Homeland Security

Sam Houston State University

Collaboration Not Convergence: Exploring Cyber-Physical Security Convergence to Prevent or Mitigate Techno-Kinetic Attacks

IF Insight Forward

INSTITUTE FOR HOMELAND SECURITY

Contents

Collaboration Not Convergence: Exploring Cyber-Physical Security Convergence to Prevent or Mitigate Techno-Kinetic Attacks

Introduction

The integration of technology into people's everyday lives has led to the ubiquitous concept of cyber-physical convergence within security, meaning that an organization's cybersecurity and physical security teams should collaborate or even become unified. This discussion is particularly critical for companies managing essential services such as power grids, water treatment facilities, telecommunications networks, and transportation infrastructure, which are increasingly vulnerable to both cyber and physical threats, making collaboration between security teams not just a recommendation but a necessity. There are even regular conferences on this subject, such as the annual "Physical Cyber Convergence Forum" hosted by CTG Intelligence. Due to the nature of the problem, the majority of researchers and practitioners seem to agree that the cyber-physical integration in security is vitally important. However, there are fundamental conceptual problems combined with a lack of data. Despite the regular discussions within and between security organizations on the cyber-physical convergence and how different teams can work together to improve defense, there are no studies that demonstrate the actual costs of such attacks. Another essential problem has to do with definitions that researchers and practitioners use.

Typically, convergence is discussed within the concept of a cyber-physical attack, which is an attack on a cyber-physical system. The US Department of Commerce's National Institute of Standards and Technology (NIST) defines a cyber-physical system (CPS): "CPS comprises interacting digital, analog, physical, and human components engineered for function through integrated physics and logic."[1] This involves the Internet of Things, Industrial Internet, and more. A paper published by the Institute of Electrical and Electronics Engineers defines CPS as "a complex system that integrates sensing, computation, control and networking into physical processes and objects over Internet."[2]

[1] Edward R. Griffor, Christopher Greer, David A. Wollman, and Martin J. Burns, "Framework for Cyber-Physical Systems: Volume 1, Overview," Special Publication (NIST SP), National Institute of Standards and Technology (2017): https://doi.org/10.6028/NIST.SP.1500-201.

[2] Wenli Duo, MMengChu Zhou, and Abdullah Abusorrah, "A Survey of Cyber Attacks on Cyber Physical Systems: Recent Advances and Challenges," *IEEE/CAA Journal of Automatica Sinica*. 9, no. 5 (2022): 784-800, doi: 10.1109/JAS.2022.105548.

Therefore, cyber-physical attacks are those that target cyber-physical systems and lead to physical damage, such as the 2008 attack in Poland that derailed tram trains,[3] the 2015 attack in Ukraine on the power grid,[4] the 2021 attack on the Colonial Pipeline,[5] or the 2021 attack in Florida on a water treatment plant.[6] With that definition in mind, the concept of the cyber-physical convergence in security becomes less potent. There are few areas to incorporate physical security groups into the defense of these networks as they are still primarily, if not exclusively, cyberattacks. The attacks just have a physical *effect*. Perhaps this means including emergency response in operational planning, but it does not create a justification for the unification of cybersecurity and physical security teams. There are also the alternatives, where purely physical attacks cause damage to technology, such as the attempted bombing of the AWS data center in Virginia[7] or a disgruntled Microsoft security employee bringing a gun to the Microsoft data center in Cheyenne, Wyoming.[8] Yet these were physical attacks that did not include a cyber component.

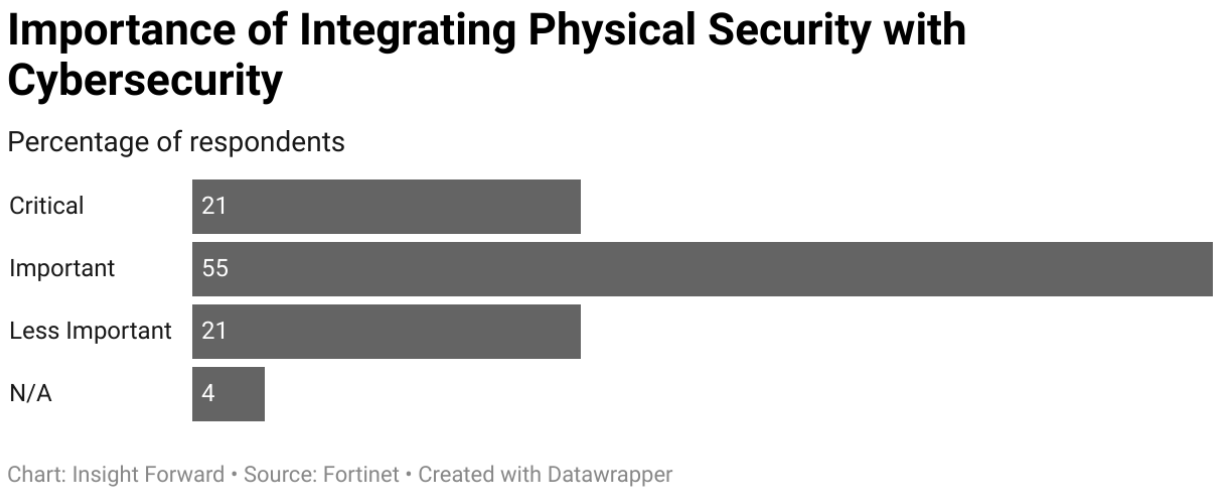
To shift this concept to an appropriate mechanism of justification for unifying the teams means a new term is needed to describe attacks that incorporate both physical and cyber aspects. For the purposes of this white paper, a **techno-kinetic attack** is either a cyber-enabled physical attack or a physically enabled cyberattack, i.e., the tactics, techniques, and procedures (TTPs) utilized by threat actors include both cyber and physical components. Techno-kinetic attacks are the types of threats that require expertise and responses from both cybersecurity and physical security teams, especially within critical infrastructure sectors, which manage systems vital to national security and daily life. Understanding the possible threats from these kinds of attacks and their costs is what would (or would not) justify convergence. As such, this white paper will look at the broad concepts and literature of cyber-physical attacks and techno-kinetic attacks to understand whether the cyber-physical convergence is justified for critical infrastructure organizations and corporations as the stakes for national and corporate security are high.

---

[3] Chuck Squatrigla, "Polish Teen Hacks His City's Trams, Chaos Ensues," *Wired*, January 11, 2008, https://www.wired.com/2008/01/polish-teen-hac/.
[4] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," *Wired*, March 3, 2016, https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.
[5] Sean Michael Kerner, "Colonial Pipeline hack explained: Everything you need to know," *TechTarget*, April 26, 2022, https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know.
[6] Alex Marquardt, Eric Levenson, and Amir Tal, "Florida water treatment facility hack used a dormant remote access software, sheriff says," February 10, 2021, https://www.cnn.com/2021/02/10/us/florida-water-poison-cyber/index.html.
[7] Phil Helsel, "Texas man who wanted to blow up Amazon data center sentenced to 10 years," *NBC News*, October 1, 2021, https://www.nbcnews.com/news/us-news/texas-man-who-wanted-blow-amazon-data-center-sentenced-10-n1280615.
[8] Ellen Gerst, "Man arrested after entering Cheyenne data center with gun," *Casper Star Tribune*, May 4, 2021, https://trib.com/news/state-regional/crime-and-courts/man-arrested-after-entering-cheyenne-data-center-with-gun/article_ef1e8d25-46eb-571c-817b-d0b6f01d8fcb.html.

Literature: Cyber-Physical Systems, Attacks, and Security

There is a dearth of literature on techno-kinetic attacks as such instances are exceptionally difficult to document because most corporations do not publicly disclose the TTPs used by threat actors in physical security incidents. Many technology companies will disclose such information for cyberattacks, **which demonstrates a disconnect in the availability of necessary data to improve security**. Yet the majority of companies still believe in cyber-physical convergence for their security groups. Fortinet conducted a survey in 2018 showing that cyber-physical security integration ranked as a "critical or important topic" for three quarters of healthcare IT leaders. However, 75% of organizations surveyed did not analyze or correlate data from physical access controls with network security.[9] The Fortinet report included important takeaways for integrating physical and cybersecurity, such as leveraging an integrated network security architecture, integrating physical security workflows and threat intelligence, and gaining complete device visibility and management with network access control.[10]



Despite their survey and recommendations, the report did not establish a real justification for convergence, only that IT leaders believe it to be important.

Within the security of critical infrastructure, this gap also exists. In August 2024, the National Counterintelligence and Security Center (NCSC) highlighted the importance of protecting critical infrastructure in their 2024 *National Counterintelligence Strategy*. According to the NCSC, "We must work collaboratively across public and private sectors to share information, identify threats, and enable action by critical infrastructure owners and operators to reduce

[9] Fortinet, "State of Physical Security and Its Convergence with Cybersecurity in Healthcare" (2018), https://www.fortinet.com/content/dam/fortinet/assets/brochures/brochure-healthcare-chimes-survey.pdf, p. 2.
[10] Fortinet, p. 7.

vulnerabilities and counter threats."[11] However, the strategy failed to mention the need for cyber-physical convergence. When discussing cyber activities, the report focused on relationships between different levels of government and the private sector, but not the integration of cybersecurity and physical security.

The academic literature on cyber-physical systems and attacks contains many similar lacunae as researchers focus on attack and risk management models for cyber-physical systems that only discuss cyberattacks or general methods of integration. Nasser et al. establish a taxonomy to assess threats to CPSs, but "types of attacks" and "incident categories" are exclusively in the cyber domain, even if the focus of the paper is CPSs.[12] Gazzarata et al. did conceive of a cyber-physical data model for security of financial critical infrastructures, and they looked at how structured threat information expression (STIX) should incorporate physical systems.[13] Even though their improved model for STIX included sources like CCTV cameras and help with cyber threat intelligence sharing, it still falls short of demonstrating how techno-kinetic attacks could be circumvented with this approach. Nonetheless, all improvements to intelligence sharing should be lauded. Mantzana et al. examine risk management within cyber-physical systems, but once again, they describe a process for integrating intelligence and analysis without demonstrating the specific threats from techno-kinetic attacks.[14] Rather, they focus on how attacks on and disruptions to critical infrastructure from cyberattacks lead to negative social and economic impacts, and their risk management approach emphasizes how critical infrastructure companies and organizations can collaborate.

Some of the literature remains too theoretical, complicated, or esoteric to establish a justification for convergence in security. Haibo He and Jun Yan present a model for monitoring possible cyber-physical attacks, but it remains focused on the cyberattack aspects and computational problems.[15] Rao et al. attempt to use game-theoretic models to assess the defense of cyber infrastructures against cyber-physical attacks, but such academic research does not yield useful applications for security organizations.[16] Though more practical, the research by Piotr Lis and Jacob Mendel discusses the economic implications of cyberattacks

---

[11] National Counterintelligence and Security Center, 2024 *National Counterintelligence Strategy* (August 2024), https://www.dni.gov/files/NCSC/documents/features/NCSC_CI_Strategy-pages-20240730.pdf, p. 16.

[12] Mohammed Nasser Al-Mhiqani, Rabiah Ahmad, Warusia Yassin, Aslinda Hassan, Zaheera Zainal Abidin, Nabeel Salih Ali, and Karrar Hameed Abdulkareem, "Cyber-Security Incidents: A Review Cases in Cyber-Physical Systems," *International Journal of Advanced Computer Science and Applications* 9, no. 1 (2018): 499-508.

[13] Giorgia Gazzarata, Ernesto Troiano, Luca Verderame, Maurizio Aiello, Ivan Vaccari, Enrico Cambiaso, and Alessio Merlo, "FINSTIX: A Cyber-Physical Data Model for Financial Critical Infrastructures," *Cyber-Physical Security for Critical Infrastructures Protection First International Workshop* (2020): 48-76.

[14] Vasiliki Mantzana, Eftichia Georgiou, Anna Gazi, Ilias Gkotsis, Ioannis Chasiotis, and Georgios Eftychidis, "Towards a Global CIs' Cyber-Physical Security Management and Joint Coordination Approach," *Cyber-Physical Security for Critical Infrastructures Protection First International Workshop* (2020): 155-170.

[15] Haibo He and Jun Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory and Application* 1, no. 1 (2016): 13-27.

[16] Nageswara S. V. Rao, Stephen W. Poole, Chris Y. T. Ma, Fei He, Jun Zhuang, and David K. Y. Yau, "Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models," *Risk Analysis* 36, no. 4 (2016): 694-710.

on critical infrastructure, which provides a useful framework for understanding why CPSs are important but not why convergence in security should take place.[17]

The most applicable research comes from Papadopoulos et al. in which the researchers apply the "PRAETORIAN approach" to protect critical infrastructure from combined cyber and physical threats.[18] The PRAETORIAN framework combines monitoring and analysis at multiple levels through four interconnected components: Physical Situation Awareness, Cyber Situation Awareness, Hybrid Situation Awareness, and a Coordinated Response System. Essentially, it is an intelligence monitoring approach that combines everything from CCTV to drone detection and SIEM tools, allowing operators to produce better insights. In their research, the authors use the PRAETORIAN framework to test a red teaming scenario involving Zagreb airport in Croatia and a medical laboratory at the Graz Hospital in Austria. As they document in their research, "focusing on a combined cyber–physical attack, several sensors (temperature, presence, sound), cameras, and a C-UAV system were deployed to detect the attack at different stages and improve the situation awareness. Integration of AI-based video analytics and drone detection were two of the innovations demonstrated. Information about cascading effects and possible consequences towards other CIs, together with possible mitigation actions were presented to CI operators."[19]

Yet this research still has a problem. This was a red-teaming scenario with a framework demonstration, not an actual security event. Their scenarios were also wildly fantastical, usually the kind found in security simulations but not in typical security events. That is the fundamental problem with the current literature and conceptualization of cyber-physical convergence. Using imaginative scenarios, security organizations have consistently argued that some form of convergence is beneficial or necessary, but they have not utilized cost-benefit analysis, return on investment (ROI) analysis, real-world use cases, or determined the impact of techno-kinetic attacks. Furthermore, both the examples typically used and the academic literature assume convergence is beneficial because attacks on cyber-physical systems have negative social and economic impacts on communities and countries. However, they do not demonstrate that both cyber and physical TTPs are involved in such attacks. Given these many gaps in the literature, this white paper aims to provide a better mechanism of analysis and justification for a possible cyber-physical convergence in security.

---

[17] Piotr Lis and Jacob Mendel, "Cyberattacks on critical infrastructure: An economic perspective," *Economics and Business Review* 5, no. 19 (2019): 24-47.

[18] Lazaros Papadopoulos, Konstantinos Demestichas, Eva Muñoz-Navarro, Juan José Hernández-Montesinos, Stephane Paul, Nicolas Museux, Sandra König, Stefan Schauer, Alfonso Climente Alarcón, Israel Perez Llopis, Tim Stelkens-Kobsch, Tamara Hadjina, and Jelena Levak, "Protection of critical infrastructures from advanced combined cyber and physical threats: The PRAETORIAN approach," *International Journal of Critical Infrastructure Protection* 44 (2024), https://doi.org/10.1016/j.ijcip.2023.100657.

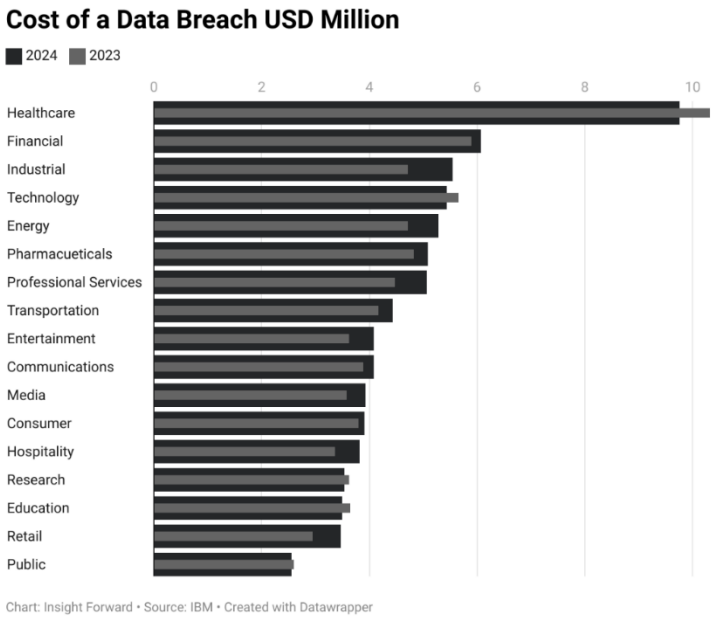
[19] Ibid, p. 11.

Cost of Cyberattacks and Physical Attacks

Cyberattacks and physical attacks separately cost organizations millions of dollars, and the potential for disruption is even greater for critical infrastructure companies such as those in energy (e.g., power grids), water treatment, transportation (e.g., airports, rail systems), and telecommunications. When attacks combine the TTPs of both cyber and physical domains, companies in these sectors are likely to face even greater costs. Currently, no studies demonstrate the costs of a techno-kinetic attack. However, various assessments of the overall costs of cyberattacks exist, and there is currently one major study on the costs of physical attacks. Although these studies do not provide a precise measurement of the impacts of techno-kinetic attacks, they will help establish a broad understanding of the potential costs.

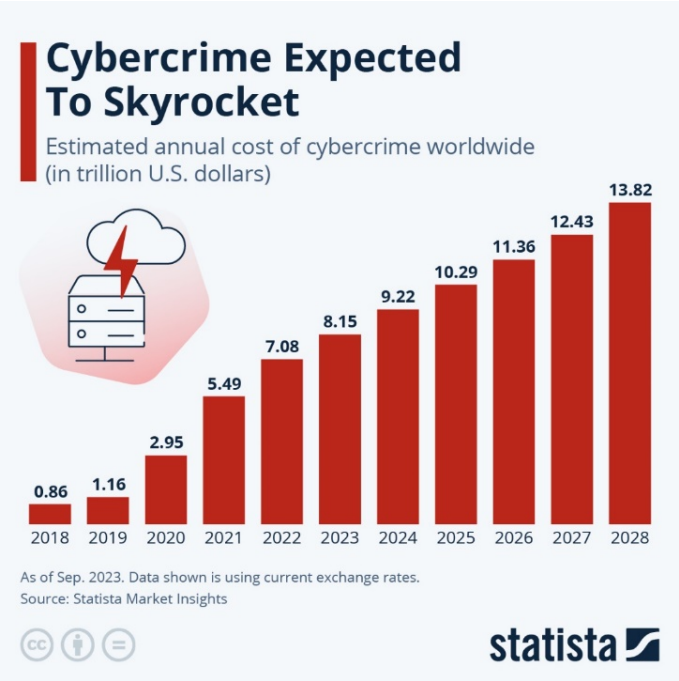
Cost of Cyberattacks

Corporations release numerous reports annually that delineate the costs of various types of attacks, and these are usually the industry standard for determining the impacts and therefore requisite resources. For example, IBM annually publishes a report that focuses specifically on data breaches within companies. The 2024 report found that the average cost of a data breach reached $4.88 million; interestingly, it also found that the use of AI in prevention led to an average reduction of $2.2 million per breach.[20] In addition, IBM assessed that a "malicious insider attack" was even more costly with an average of $4.99 million, indicating a crossover with physical security and investigations. Focusing on one type of attack, Chainalysis, a blockchain data platform, determined that ransomware gangs had extracted $1.1 billion in cryptocurrency payments through ransom extortion, the highest amount ever recorded to that point.[21] Of course, payments alone do not account for ransomware costs, as MGM likely incurred damages of $100 million without paying the ransom when it was attacked.



[20] IBM, *Cost of a Data Breach Report 2024*, https://www.ibm.com/reports/data-breach, p. 2.
[21] "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," Chainanalysis, February 7, 2024, https://www.chainalysis.com/blog/ransomware-2024/.

Large corporations are not the only ones impacted. According to a survey by the insurance company Hiscox, the median cost of cyberattacks for a small business was $8,300 in 2023.[22] Their data came from 5,000 cybersecurity professionals responsible for a company's cyber strategy from the US, UK, France, Germany, Spain, Belgium, Republic of Ireland, and the Netherlands. Ransomware especially impacted small businesses, as they typically paid over $16,000 in ransoms in the past year; only 50% recovered all their data, while 27% faced further ransom demands. Cybercrime generally incurs many costs, beyond just ransomware. The FBI's Internet Crime Complaint Center found that there were $37.4 billion in losses from the 3.79 million complaints the organization received between 2019-2023.[23] In a broader context, Statista's Market Insights reported that "the global cost of cybercrime is expected to surge in the next four years, rising from $9.22 trillion in 2024 to $13.82 trillion by 2028."[24]



When considering the potential costs to critical infrastructure, the costs to governments specifically are just as deleterious. Sophos's *The State of Ransomware in State and Local Government 2024* found that the average cost for state and local governments to recover from a ransomware attack was $2.83 million in 2024.[25] One reason that it was so costly to recover was the number of devices infected. The report found that, on average, "56% of computers in state and local government organizations were impacted by a ransomware attack, above the cross-sector average of 49%."[26]

Cyberattacks impose far-reaching costs beyond the immediate financial impact.[27] Businesses face significant revenue losses due to operational disruptions, especially in critical sectors like finance, healthcare, and transportation. Extended outages result in lost sales, damaged

---

[22] "Cyber Attacks Cost US Small Businesses Over $8,000 Annually, Reveals Hiscox Cyber Readiness Report 2023," Hiscox, December 5, 2023, https://www.hiscox.com/articles/cyber-attacks-cost-us-small-businesses-over-8000-annually-reveals-hiscox-cyber-readiness.
[23] Internet Crime Complaint Center, *Federal Bureau of Investigation Crime Report 2023*, https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf, p. 7.
[24] Anna Fleck, "Cybercrime Expected To Skyrocket in Coming Years," Statista, February 22, 2024, https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/.
[25] Puja Mahendru, "The State of Ransomware in State and Local Government 2024," Sophos, August 14, 2024, https://news.sophos.com/en-us/2024/08/14/the-state-of-ransomware-in-state-and-local-government-2024/.
[26] Ibid.
[27] "Unmasking the True Cost of Cyberattacks: Beyond Ransom and Recovery," *The Hacker New*, April 23, 2024, https://thehackernews.com/2024/04/unmasking-true-cost-of-cyberattacks.html.

reputations, and strained relationships with customers and suppliers. The loss of customer trust can lead to long-term impacts, including a shift in business to competitors. This is difficult to quantify, but it should be incorporated into assessments of the costs of attacks (and consequently the return on investment for appropriate security measures and expenditures). In addition, businesses may face regulatory fines for non-compliance with privacy laws like GDPR and CCPA, further increasing their financial strain. Cyberattacks can also result in rising insurance premiums as companies become higher-risk targets, compounding their financial challenges.

Again, corporations are not the only ones negatively affected by such attacks. Research by the Brookings Institution found that "cyberattacks lead to roughly $1.77 billion in mark-to-market losses for municipal bond investors on the $870 billion in outstanding bonds of issuers hit by data breaches between 2010 and 2019."[28] Importantly, this estimate is likely a "lower bound" as "many bonds of issuers affected by cyberattacks may be illiquid and not trade in the 60-day window studied." Altogether, there are significant direct and indirect costs from cyberattacks in general, forming the basis for estimating the costs of techno-kinetic attacks.

Cost of Physical Attacks

The first *World Security Report*, commissioned by Allied Universal and G4S, reveals that large global companies lost $1 trillion in revenue in 2022 due to physical security incidents.[29] According to the report, companies anticipate a rise in threats such as social unrest, climate change, fraud, and theft, prompting an increase in physical security budgets. Fraud is considered to be the greatest external threat, while internal threats primarily involve the leaking of sensitive information. In addition to the threats, the report also documented that in 2022, companies spent $660 billion on physical security, approximately 3.3% of global revenue. The report surveyed 1,775 chief security officers (CSOs) and found that 25% of companies experienced a decline in corporate value following security incidents. Additionally, investors predicted an average 29% drop in stock prices following significant security breaches. Based on this research, physical attacks appear to be just as costly as cyberattacks, particularly in terms of lost revenue.

Cost of Security Incidents

The escalating impact of cyber and physical security threats has become a critical issue for organizations worldwide, with both digital and physical incidents resulting in substantial financial and operational losses. As businesses increasingly rely on digital infrastructure, they face growing risks from cybercrime, ransomware, and data breaches. Additionally, physical security breaches further complicate the landscape. In both the digital and physical realms, the cost of security incidents continues to rise, as companies face mounting challenges to

[28] Tristan Loa and David Wessel, "What cyberattacks do to municipal issuers' borrowing costs," Brookings Institution, August 7, 2024, https://www.brookings.edu/articles/what-cyberattacks-do-to-municipal-issuers-borrowing-costs/.
[29] Allied Universal and G4s, *World Security Report* (2023), https://www.worldsecurityreport.com/key-findings/.

protect their assets, data, and reputation. The combination of economic losses from cyberattacks, particularly ransomware, and the increasing threats of physical security breaches highlights the potential costs of a techno-kinetic attack.

Cyber-Physical Convergence for Techno-Kinetic Attacks

While there is a lack of comprehensive literature on techno-kinetic attacks and a misunderstanding of the possible convergence for CPSs, examples of techno-kinetic attacks would help organizations understand the theoretical justification for convergence and the impacts on companies. Crucially, understanding techno-kinetic attacks could also lead organizations to conclude that convergence is not necessary if these attacks are too rare or lack significant impact, indicating that the ROI of convergence would be insufficient. To reiterate, a **techno-kinetic attack** is either a cyber-enabled physical attack or a physically enabled cyberattack, i.e., the tactics, techniques, and procedures utilized by threat actors include both cyber and physical components. This section will examine some use cases of techno-kinetic attacks or easily conceivable ones that could credibly be executed, as opposed to fantastical scenarios that are extremely unlikely or practically impossible to occur.

Stuxnet

The best example of *both* a techno-kinetic attack *and* a cyber-physical attack is Stuxnet, the sophisticated cyberweapon that caused physical damage at Iran's Natanz nuclear facility.[30] The propagation vector for Stuxnet was a USB thumb drive (external storage device), which starts the physical aspect to the attack. According to Richard Sale, Israeli agents hired proxies (likely from the dissident Mujahedeen-e-Khalq group) to use infected USB sticks at the facility.[31] Once the USB was inserted, the computer became infected, and Stuxnet would exploit one or more zero-day vulnerabilities, allowing it to infect other external storage devices or laptops that were connected. Once Stuxnet discovered programmable logic controllers (PLCs), it would execute its function, controlling the PLCs and varying the rotation speeds of centrifuges to damage them, thereby disrupting Iran's nuclear program. This example demonstrates how techno-kinetic attacks occur (agents hired to spread infected devices that then execute a cyberattack) and how cyber-physical attacks function (cyberattack on centrifuges that led to their physical damage and destruction).

[30] There is not enough room to fully explore the Stuxnet attack, but for the full story see: Kim Zetter, *Countdown to Zero Day* (New York: Broadway Books, 2014).
[31] Janus Kopfstein, "Stuxnet virus was planted by Israeli agents using USB sticks, according to new report," *The Verge*, April 12, 2012, https://www.theverge.com/2012/4/12/2944329/stuxnet-computer-virus-planted-israeli-agent-iran.

Insider Threats

Probably the most common and salient techno-kinetic attack would be from insider threats who deliberately attempt to harm the organization from within. There are several examples of malicious insider threats stealing intellectual property or customer data after quitting or being fired. In 2022, a former Yahoo employee stole intellectual property because the employee had obtained a new job and wanted to use the information to improve their standing.[32] The employee transferred the IP to two personal laptops using an external storage device. In 2023, two former Tesla employees took 23,000 internal documents containing employees' PII, customers' financial information, and other proprietary information.[33, 34] This breach could have led to a €3.26 billion GDPR fine from insufficient protection of data, and it likely occurred because security did not revoke access permissions.

Dr. Marisa Randazzo, the former Executive Director of the Ontic Center of Excellence, noted that an internal government study in which she participated found that "insiders who sabotage or exploit information systems don't just snap. Before major incidents, they follow a pathway of planning and research. They engage in troubling behaviour that is observable – online and in person – and that alarms co-workers and friends."[35] The finding illustrated that threat indicators were present before an attack, and that physical and cyber teams working together would likely be capable of tracking those threat indicators. For the actual attack, though, this is primarily an IT issue based on access controls and compartmentalized information. Insider threat encapsulates the techno-kinetic attack where physical and cyber teams can collaborate to track problems and issues.

Social Engineering

There is a common phrase in cybersecurity that people are the weakest link in security, and social engineering exploits that weak link in techno-kinetic attacks. Research indicates that approximately 88% of data breaches are due to employee mistakes and errors, and threat actors regularly attempt to exploit those psychological vulnerabilities.[36] Social engineering attacks typically involve phishing or vishing. For small businesses, phishing remains the most common entry point for ransomware (53%), followed by unpatched servers/VPNs (38%), and credential theft (29%). Notably, in the survey, 59% of small businesses lack security awareness

---

[32] Alex Lee, "Yahoo Employee Stole 570,000 Pages of Source Code the Day He Quit to Join a Competitor," *Cyberhaven*, August 27, 2002, https://www.cyberhaven.com/blog/yahoos-lawsuit-alleged-engineer-stole-sensitive-data.

[33] Riham Alkousaa and Toby Sterling, "Dutch watchdog looking into alleged Tesla data breach," *Reuters*, May 26, 2023, https://www.reuters.com/business/autos-transportation/german-authorities-looking-into-possible-data-protection-violations-by-tesla-2023-05-25/.

[34] Chris Brook, "Tesla Data Theft Case Illustrates the Danger of the Insider Threat," Digital Guardian, August 22, 2024, https://www.digitalguardian.com/blog/tesla-data-theft-case-illustrates-danger-insider-threat.

[35] Marisa Randazzo, "Why the insider threat will motivate cyber and physical teams to collaborate more than ever in 2022," *IFSEC Insider*, January 5, 20202, https://www.ifsecglobal.com/cyber-security/why-the-insider-threat-will-motivate-cyber-and-physical-teams-to-collaborate-more/.

[36] "'Psychology of Human Error' Could Help Businesses Prevent Security Breaches," *CISOMAG*, September 12, 2020, https://cisomag.com/psychology-of-human-error-could-help-businesses-prevent-security-breaches/.

training, and 43% don't use network-based firewalls.[37] This indicates that a lack of security awareness and protocols are major factors in enabling such attacks on small businesses.

A real-world example of this is the SCATTERED SPIDER group, which relies heavily on identity-based tactics in its operations.[38] According to CrowdStrike, throughout 2023, they conducted advanced social engineering campaigns to compromise victim accounts. Their methods included SMS phishing (smishing), voice phishing (vishing), and making phone calls to help desks to trick staff into resetting passwords or multi-factor authentication (MFA) credentials. They also exploited previous telecom breaches to conduct SIM swaps, enabling them to intercept one-time passwords (OTPs) sent via SMS. SCATTERED SPIDER targets employees in information security and IT, seeking access to security tools and documentation that facilitate further attacks. To avoid detection, they use residential proxies that make it appear as though they are logging in from the victim's location, demonstrating a deep understanding of identity-based security measures used by organizations. SCATTERED SPIDER is a prime example of a group engaging in techno-kinetic attacks because they combine cyberattacks with physical social engineering tactics (e.g., smishing and vishing).

Drones and Cyberattacks

In 2022, a financial services company on the East Coast allegedly discovered an unusual cyberattack in which drones were used to infiltrate its network.[39] The attack was detected when security staff noticed suspicious activity on the company's internal Atlassian Confluence page, revealing the use of a duplicate MAC address. Using a Wi-Fi tester, the team tracked the source to the building's roof, where they found two drones: a modified DJI Phantom equipped with a Wi-Fi Pineapple device to hijack connections and steal credentials, and a modified DJI Matrice 600 outfitted with a Raspberry Pi, laptop, and communication devices. Quick action by the security team prevented a more serious breach, but the attackers were never caught. Additionally, the attack likely cost only about $15,000,

CC0 Public Domain

[37] "Cyber Attacks Cost US Small Businesses Over $8,000 Annually, Reveals Hiscox Cyber Readiness Report 2023," Hiscox, December 5, 2023, https://www.hiscox.com/articles/cyber-attacks-cost-us-small-businesses-over-8000-annually-reveals-hiscox-cyber-readiness.

[38] Crowdstriek, *Crowdstrike 2024 Global Threat Report* (2024), https://go.crowdstrike.com/global-threat-report-2024.html, p. 16.

[39] Mike Elgan, "Why consumer drones represent a special cybersecurity risk," *Security Intelligence,* September 7, 2023, https://securityintelligence.com/articles/why-consumer-drones-represent-a-special-cybersecurity-risk/.

representing a low barrier to entry.[40] Drones are increasingly used in cyberattacks due to their versatility. They can perform physical surveillance, capture Wi-Fi network data, and execute attacks such as network spoofing and Denial-of-Service (DoS). This tactic, first demonstrated in theoretical scenarios, has now become a reality, with drones playing a significant role in cyber warfare, notably in the Russia-Ukraine conflict, where they gather intelligence, bypass security, jam signals, and deliver malware. These capabilities make drones highly effective in potential techno-kinetic attacks.

Flipper – The Ideal Tool

Concerningly, for many both inside and outside of the security industry, the Flipper Zero device exemplifies the ideal tool for techno-kinetic attacks. The website describes the device as "a portable multi-tool for pentesters and geeks in a toy-like body. It loves hacking digital stuff, such as radio protocols, access control systems, hardware, and more. It's fully open-source and customizable, allowing you to extend it in any way you like."[41] The device was initially known primarily to red teamers and pentesters when it first launched, but TikTok has spread awareness of the device through various pranks. What matters, though, is that amateur hackers and script kiddies[42] have effectively used the device to turn off electronic menus at restaurants, open charging ports on Tesla vehicles, and change the price at gas stations.[43] Importantly, the Flipper includes hardware hacking and RFID emulation capabilities, highlighting the intersection of cybersecurity and physical security. To copy low-frequency RFID requires physical proximity to a fob, similar to infrared control. Though the device is brilliantly designed, it has physical limitations, meaning that physical security plays a role in observing and detecting intruders or being aware of threat actors getting too close to people to copy their fobs.

Maciej Łutczyk, CC BY-SA 4.0

Emerging Threat from Techno-Kinetic Attacks

Techno-kinetic attacks, which blend cyber and physical TTPs, present a growing threat that organizations must acknowledge. Real-world examples, such as Stuxnet and insider threats,

[40] Dark Reading Staff, "Airborne Drones Are Dropping Cyber-Spy Exploits in the Wild," *Dark Reading*, October 12, 2022, https://www.darkreading.com/threat-intelligence/drones-cyber-spy-exploits-in-the-wild.
[41] See https://flipperzero.one/.
[42] A person who uses existing computer scripts or codes to hack into computers, lacking the expertise to write their own.
[43] "How the rise of Flipper Zero poses a new threat to IoT cybersecurity," Trustonic, November 8, 2023, https://www.trustonic.com/opinion/how-the-rise-of-flipper-zero-poses-a-new-threat-to-iot-cybersecurity/.

demonstrate the potential damage of these convergent attacks, while emerging tools like drones and devices like Flipper Zero enable increasingly sophisticated methods. Despite their relative rarity, the potential impact of techno-kinetic attacks on both physical and cyber systems necessitates taking proactive measures. By understanding these risks, organizations can better assess the need for convergence between cybersecurity and physical security, ensuring comprehensive protection against such hybrid threats.

Justification for the Physical-Cyber Security Convergence

Threat Assessment of Techno-Kinetic Attacks

The first step in establishing a justification for the physical-cyber security convergence would be a threat assessment determining the likelihood and impact of known or easily conceivable techno-kinetic attacks. The attacks described above are use cases by which organizations can do threat assessments. For example, they could determine the likely number of persons or groups of interest with the resources and technical capabilities to purchase and modify drones for cyberattacks and assess whether they have the motivation or intention to act. Part of this threat assessment should include a review of their internal security controls and what it would take to bypass them, ensuring that they focus on techno-kinetic attacks that are credible, likely, and impactful.

Return on Investment Analysis

The Center for Internet Security (CIS) has developed a simple formula to determine the return on investment for security decisions, providing a practical and useful model for critical infrastructure corporations to evaluate whether they should invest the time, effort, and resources into implementing cyber-physical convergence in security.[44] The simple formula for calculating Risk-Reduction ROI is:

Risk-Reduction ROI

$$\textbf{ROI} = \frac{(\text{reduction in risk '\$'} - \text{cost of control})}{\text{Cost of control}}$$

Reduction in Risk	=	Annualized rate of occurrence	X	Expected monetary loss for a single event	X	Reduction in probability of risk occurrence with the implemented control

[44] Center for Internet Security, "The One Equation You Need to Calculate Risk-Reduction ROI," https://www.cisecurity.org/insights/blog/the-one-equation-you-need-to-calculate-risk-reduction-roi.

CIS uses a phishing attack as an example:

- If there is an annual occurrence of five phishing attacks per year with the expected monetary loss for a single event at $35,000 and a reduction of 85% probability of the risk event with the implemented control, combined with a control cost of $25,000, then the ROI is 4.95 or a saving per year of $123,750.

Calculating Risk-Reduction ROI

Reduction in Risk: $5 \times \$35{,}000 \times 0.85 = \$148{,}750$

Return on Investment: $$\frac{(\$148{,}750 - \$25{,}000)}{\$25{,}000} = 4.95$$

Savings per year: $\$25{,}000 \times 4.95 = \$123{,}750$

Similar examples could be used to justify cyber-physical convergence in security. Working with finance groups within the business, security managers can deduce the likely ROI for combining their physical and cyber security teams, or at least creating mechanisms for them to work together. However, the formula would need to include potential regulatory fines and lost revenue in the "expected monetary loss for a single event." In addition, as techno-kinetic attacks are still developing, security organizations might have to estimate the *potential* number of such attacks for the "annual occurrence" variable.

Conclusion and Future Research

This white paper examined the present literature on cyber-physical attacks and their security while delineating how a new concept is needed: techno-kinetic attacks. Cyber-physical attacks are cyberattacks that lead to physical effects, which are different from an attack that incorporates both cyber and physical tactics, techniques, and procedures. Techno-kinetic attacks involve the combination of cyber and physical elements in the attack itself, not just in the impacts. Examples include attacks like Stuxnet, insider threats, and drones used for cyberattacks. Such attacks highlight the vulnerabilities that arise when physical and cyber security are treated as separate entities, but this does not necessarily create a sufficient justification for cyber-physical security convergence. The current evidence suggests that *collaboration, not convergence,* is necessary for security of critical infrastructure. None of the use cases of techno-kinetic attacks seemed to require abrogating the current structures of security. Cybersecurity and physical security each have their own expertise, and collaboration between these teams is increasingly essential for critical infrastructure sectors to prevent or mitigate attacks. For example, an investigations team could assist in determining indicators for

insider threats while cybersecurity teams could monitor internal networks on the person of interest. In that case, the teams should work together, but these instances are most likely the exception rather than the norm. Given the limited use cases available and the lack of financial impact analysis specifically focused on techno-kinetic attacks, there is not yet a strong enough business case for convergence.

Both academic literature and industry publications lack accurate assessments of the impacts of techno-kinetic attacks, and at best, provide indirect measurements or theoretical models. Given the limited use cases, significantly more research is needed on techno-kinetic attacks before a definitive conclusion can be reached regarding the justification for cyber-physical security convergence. Additionally, the increasing potential for techno-kinetic attacks calls for further research to understand the evolving threat landscape. Although these attacks remain uncommon, their potential for significant damage is evident, especially as technologies like drones and low-cost hacking devices become more accessible.

More studies on the convergence of cyber and physical security are necessary to determine whether the return on investment for integrating these security measures is justified. Using the ROI formula provided by CIS, security organizations may determine that convergence is necessary to enhance their security measures. However, until that data is made available for other researchers and practitioners, there is limited ability to generalize.

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University