Defining the "Cyber-Pearl Harbor" - Validation of the DSLP-framework in "Offensive Cyberspace Operations Targeting Ukraine: A Cyber Pearl-Harbor"

Jonathan Lilja[1], Eleshwa Eishayea[1] and Gazmend Huskaj[1,2]
[1]Department of Computer and Systems Sciences, Kista, Sweden
[2]Geneva Centre for Security Policy, Geneva, Switzerland

jonathan.lilja@sandvik.com
eleshwa.eishayea@outlook.com
g.huskaj@gcsp.ch

Abstract: The use of cyberattacks against organizations, health care and individuals have increased along with the constant digitalisation. Nations have also fallen victim to cyberattacks, often combined with other means of war. A Cyber-Pearl Harbor (further shortened as CPH) is a term mentioned by the former United States Secretary of Defense, Mr. Leon Panetta, who described it as "combined attacks that result in human death and physical destruction and that paralyzes an entire nation". Gazmend Huskaj used Panetta's definition in order to create a framework (herein the "DSLP-framework") for classifying an event as a CPH. This study strives to see if the DSLP-framework can be validated since the term has been widely used for the last 25 years. However, a universal definition of the term seems to be missing, therefore it is not certain that the criteria presented in the framework is accurate. A qualitative case study was conducted through a literature review regarding the term CPH and semi structured interviews with three experts were done, which were later analysed through a thematic analysis. The framework was applied to three real life cases: a public health sector in Costa Rica, a TV-tower in Kyiv, Ukraine and the grocery company Coop in Sweden. The result from applying the DSLP-framework to each case was that only the case of TV-tower in Kiev, Ukraine, could be classified as a CPH. The following conclusions were drawn in this study: 1) The framework could not be validated due to lack of data, and 2) The interviewees views differed from the framework making it hard to find common ground.

Keywords: Cyber-Pearl Harbor, Cyber attacks, Cyber security, Hybrid operations, Russia-Ukraine war

1. Introduction

Attacks against computers or networks, commonly known as cyber attacks, have become increasingly prevalent in recent years (ENISA, 2022). With the advent of the Internet of Things (IoT), new and more complex forms of cyber attacks are continually emerging, particularly in warfare. Here, a blend of kinetic and cyber means is increasingly observed. The ongoing Russia-Ukraine war exemplifies this, where physical attacks using missiles and cyber attacks targeting infrastructure occur frequently. This situation raises questions about the extent of these attacks and whether they can be classified as Cyber Pearl Harbors (CPH).

Former United States Secretary of Defense, Mr. Leon Panetta, described a CPH as "an attack that would cause physical destruction and the loss of life, paralyzing and shocking the nation and creating a new, profound sense of vulnerability" (U.S. Department of Defense, 2012). He also noted that such an attack includes targeted attacks on key elements of a nation's critical infrastructure, rendering communication and military systems either unusable or severely limited (ibid.). Huskaj (2023) also refers to this definition and, through linguistic analysis, deconstructs it into components used in his framework, as depicted in **Figure 1:** 1) The attack comprises both cyber and physical elements; 2) The impact of the attack includes physical destruction and loss of human life; 3) The nation is plunged into a state of cognitive shock (cognitive effect).

Component 1 – Attack Type	Component 2 – Impact of Attack
Cyber attacks AND physical attacks	Physical destruction AND loss of life
Component 3 – Cognitive Effects	
Bring into being a deep, fresh, perceived wounding	
[PICTURE TO VISUALLY PRESENT THE PERCEIVED WOUNDING]	

Figure 1: The DSLP-framework

The purpose of this research product is to answer the research question: How can the "DSLP-Framework" in "Offensive Cyberspace Operations Targeting Ukraine: a Cyber Pearl-Harbor" (2023) be validated for the classification of cyber attacks as Cyber Pearl-Harbor?

By examining whether real-world examples that meet the DSLP requirements can be found in today's environment, a successful validation could enhance the framework's credibility. This, in turn, would facilitate its application in future cases. The validation was conducted using the following three real-life cases, all of which share the common characteristic of attacks focusing on disrupting systems and their availability: the attack on the public healthcare sector Caja Costarricense de Seguro Social in Costa Rica, the TV tower in Kyiv, Ukraine, and the grocery company Coop in Sweden.

In late May 2022, Costa Rica's public health sector, Caja Costarricense de Seguro Social (CCSS), suffered a ransomware attack. This incident resulted in 30 CCSS servers being infected and approximately 1,200 hospitals and clinics being shut down (Murillo, 2022; Córdoba & Sherman, 2022; Caja Costarricense de Seguro Social, 2022).

On March 1, 2022, Russia launched a malware attack ("DesertBlade") against a TV tower in the capital, Kyiv, aiming to destroy and silence TV media and channels in Ukraine. On the same day, two Russian missiles reportedly hit the TV tower, killing five people and injuring five others (Microsoft, 2022; Harding, 2022; Koch-Emmery & Wikén, 2022).

Beyond politics and warfare, large companies have also been targets of major cyberattacks. In Sweden, the grocery chain Coop experienced a cyber attack that crashed their cash register system due to the software company Kaseya being subjected to a ransomware attack (Toresson, 2021).

The remainder of the article is organized as follows: Section 2 describes the methods and materials; Section 3 presents the results of the study; Section 4 discusses these results; and Section 5 concludes with the conclusions and directions for future research.

2. Methods and Materials

Case studies aim to study and examine a phenomenon in depth and within its contemporary context (Johannesson & Perjons, 2014). This research strategy provides a detailed description of the research, providing a holistic perspective of the phenomenon, its processes, and its potential relationships within its context (Denscombe, 2014). Since this study seeks to investigate and validate whether a framework developed for Cyber Pearl Harbor (CPH) can be applied to three additional cases, a case study approach was deemed the most suitable research strategy. Furthermore, the flexible nature of this strategy not only facilitates the creation of new theories and/or the validation of existing frameworks but also allows for the integration of other research strategies (Denscombe, 2014). These characteristics are particularly relevant in this study, where a validation of an existing framework, published by Huskaj (2023), is undertaken. Thus, case studies are the appropriate strategy for this study.

Semi-structured interviews were conducted with the aim of collecting further data from experts, all of whom possess well-founded knowledge in the field of cybersecurity. A total of three interviews were carried out, either on-site or via Zoom. All interviewees have a background in defence, with two possessing substantial knowledge in technical means and hybrid attacks, while the third interviewee had deeper expertise in influence operations. One of the interviews was conducted in English and was intentionally not translated to retain the context that might otherwise have been lost.

To analyse the collected data and identify potential themes and patterns, the method of thematic analysis was employed. The flexibility of this method allows a researcher to identify, analyse, and report on the key themes and patterns emerging from the data (Braun & Clarke, 2006). The thematic analysis was conducted on the data collected from the literature review and the semi-structured interviews (see **Figure 2**). The review and conceptualization of the scientific research on "Cyber Pearl Harbor" are presented in **Table 1**.

Table 1: Conceptualisation derived from the literature review

Concept	Definition	References
Cyber-Pearl Harbor	A combined attack consisting of cyber and physical operations leading to loss of human life and cognitive impact on a society.	(Huskaj 2023)
Definition of the term	Researchers disagree on definitions. More research is needed to come up with a universal definition.	(Lawson & Middleton 2019; U.S. Department of Defense 2012; Smith 1998; Straub 2021; Huskaj 2023)
Probability of occurrence	There are differences of opinion on the likelihood that a Cyber Pearl Harbor would occur/has already occurred.	(Smith 1998; Straub 2021; Goldman & Warner 2017; Libicki

Concept	Definition	References
		2009; Wirtz 2018; U.S. Department of Defense 2012; Clark & Knake 2010)
Relevance of the term	Researchers disagree whether the term is still relevant.	(Kallberg 2021; Vavra 2021; Wirtz 2017)
Grey-zone	Characterised by an area between cyber warfare and political warfare that plays on a line between war and peace.	(Wither 2022; Dziwisz 2022)
Cyber disinformation	Dissemination of disinformation in the form of deep fakes, propaganda and misinformation with the aim of causing damage at a cognitive level.	(ENISA 2022; Microsoft 2022b; Whyte & Mazanec 2019)
DDoS attacks	Abbreviation for "Distributed Denial of Service". A type of cyber attack where multiple vulnerable computers are used to overload a victim's system, network or server with a large amount of traffic and make it inaccessible to users.	(ENISA 2022)
Ransomware attacks	A type of malware that encrypts a victim's files. Ransom is then used to restore access to the encrypted files. It often results in significant disruption and financial loss to victims.	(ENISA 2022)
National level	Cyber-attacks occur on a national level.	(ENISA 2022; Microsoft 2022a; Microsoft 2022b; Wither 2022; Dziwisz 2022)
Organisational level	Cyber-attacks also target businesses and the public sector, such as the healthcare sector.	(ENISA 2022; Riggi 2020; Microsoft 2022b)

2.1 Limitations of the Study

This study is subject to several limitations. Firstly, time was a significant constraint due to the project's duration of six months on a half-time basis (equivalent to 3 months full-time). This temporal limitation significantly impacted the research, as it restricted the authors to conducting only three semi-structured interviews. Consequently, this leads to the second limitation: restricted access to empirical data. A larger number of respondents would have likely yielded more empirical data, thereby potentially providing a clearer insight into how respondents perceive and interpret the concept of a “Cyber Pearl Harbor.” Finally, a limitation concerning the study's conclusions must be acknowledged: the limited scope and depth of the research preclude the drawing of comprehensive conclusions.

3. Results

In this section the results of the thematic analysis and case study are presented.

3.1 Thematic Analysis

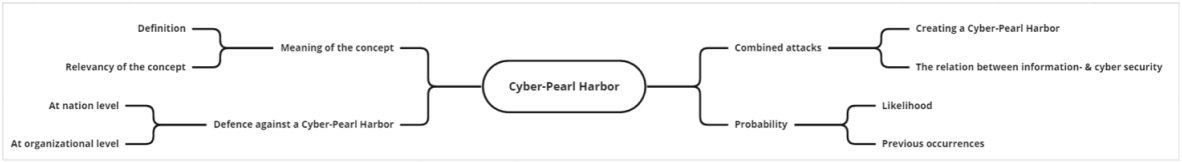

Figure 2: The thematic analysis resulted in four main themes and eight categories

3.1.1 Meaning of the concept

Meaning of concepts encompasses two categories: *Definition* and *Relevancy of the concept*. The first category addresses the disagreement over the definition of “Cyber Pearl Harbor,” highlighting the need for both a universal standard and a redefinition of the concept. In efforts to define the concept, the element of surprise is frequently mentioned, with an emphasis on the critical effects such attacks can have on society. The scope of the concept was also explored, including the aspect of utilising a combination of tools in executing a Cyber Pearl Harbor. To classify an attack as a Cyber Pearl Harbor, the involvement of multiple sectors of society or an entire country is necessary, achievable through the combination of tools and other means, as previously mentioned. The potential effects of a Cyber Pearl Harbor were also discussed, raising questions about the possibility of loss of life and examining the criteria described in Huskaj's (2023) DSLP-framework. The importance of involving relevant entities in defining the term was also underscored.

The second category involves discussions regarding the relevancy of the Cyber Pearl Harbor concept. The concept was described as outdated, needing to evolve in line with contemporary usage of the term and ongoing digitalization. The manner in which the term has changed over the years was a topic that elicited divided opinions.

3.1.2 Defence against a Cyber-Pearl Harbor

The theme of *Defence against a Cyber-Pearl Harbor* encompasses strategies at both the *national* and *organisational* levels. At the national level, the discussion focused on the implementation of an "emergency plan" that every country should follow in the event of a Cyber Pearl Harbor. The concept of cyber resilience was also mentioned in the context of building up national defence.

At the organisational level, the emphasis was placed on establishing routines and the importance of cooperation within and between different businesses. Such cooperation would contribute to the knowledge pool within an organization and serve as an opportunity to learn from and with other entities. In the event of a Cyber Pearl Harbor, these entities could assist each other, or the emergency plan mentioned previously could also function as an effective measure.

3.1.3 Combined attacks

Combined attacks were a central theme in all interviews. Interviewees shared the view that cyber-attacks, on their own, do not yet possess the scale required to create effects as described in the DSLP-framework. The importance of employing multiple means of action simultaneously was emphasised, particularly in understanding what could constitute a Cyber Pearl Harbor (CPH) in practice. This includes not only the execution of CPH but also how cyber-attacks are intertwined with influence operations and should be considered from a defence perspective, linking information and cyber security. There were also multiple mentions of the strategy of launching attacks in different locations simultaneously to achieve maximum effect. Such a strategy can confuse the adversary and create a sense of desperation, especially when the attacks target resources essential to the functioning of society.

The interviewees unanimously agreed that discussions on cybersecurity cannot exclude information security. From an offensive standpoint, this linkage is often manifested through the simultaneous use of physical and cyber-attacks.

3.1.4 Probability

In the context of the Russia-Ukraine War, discussions arose regarding the probability of a Cyber Pearl Harbor and the factors necessary to facilitate it. To estimate this probability, it is essential to consider *previous incidents*. All interviewees concurred that a Cyber Pearl Harbor has not yet occurred. This consensus is attributed to several factors, such as the insufficiency of single cyber attacks in achieving the crippling effect required by the DSLP definition without the support of combined means of action. Additionally, cyber attacks have not been extensive enough to impact an entire society. This might be due to foreign military powers allocating more resources to conventional means than to cyber, and the challenge in identifying clear instances where cyber means alone have resulted in human fatalities. It is also evident that countries frequently targeted by cyber attacks have developed cyber resilience as a defence, and adversaries have not been prepared to encounter such resistance in the cyber domain.

Opinions varied regarding the likelihood of a Cyber Pearl Harbor in the future. Interviewee 1 suggested that the probability of a nationwide attack is high, but it is improbable to paralyse a country for an extended period. Interviewee 2 questioned whether society is sufficiently uniform and integrated to be wholly impacted by a potential Cyber Pearl Harbor. Conversely, Interviewee 3 focused more on when a Cyber Pearl Harbor will occur rather than if it will occur, citing the advancement of AI and similar digital technologies as potential significant threats.

However, all interviewees emphasized that it is currently impossible to predict with certainty when a Cyber Pearl Harbor will occur. This uncertainty is partly due to the element of surprise encompassed in the DSLP-framework's definition, which can also be applied to previous war incidents that have shocked the world.

3.2 Validation of the DSLP-Framework

The validation shows that only one out of three cases could be classified as a Cyber-Pearl Harbor (*TV-tower in Kiev, Ukraine*), which is presented in the table below.

Table 2: Cases versus the DSLP-framework

Case	Criteria	
Public healthcare sector, Caja Costarricense de Seguro Social in Costa Rica	Cyber attacks	Kinetic attacks
	Physical destruction	Loss of life
	Cognitive effects	
Tv-tower in Kiev, Ukraine	Cyber attacks	Kinetic attacks
	Physical destruction	Loss of life
	Cognitive effects	
Grocery company Coop in Sweden	Cyber attacks	Kinetic attacks
	Physical destruction	Loss of life
	Cognitive effects	

3.2.1 Public healthcare sector Caja Costarricense de Seguro Social in Costa Rica

The cyber-attack against the CCSS in Costa Rica was a ransomware attack in which approximately 30 servers were directly infected by the virus (Córdoba 2022). No physical attacks were reported in connection with this cyber-attack. However, a significant consequence of the cyber-attack was the closure of around 1,200 hospitals and clinics (Murillo 2022). Several patients were affected by the cyber-attack and its repercussions, but fortunately, no human deaths were reported. One of the cognitive effects of the cyber-attack included the disruption in reporting and accounting for COVID-19 related data (Córdoba 2022). Additionally, patients were informed that they could not receive treatment during this period, and there were reports of surgeries being delayed (Caja Costarricense de Seguro Social 2022).

In summary, the cyber-attack against the CCSS healthcare sector in Costa Rica does not qualify as a Cyber Pearl Harbor under the DSLP-framework. Despite targeting a sensitive sector where human casualties could easily occur, the attack did not coincide with any kinetic attack, nor were there any reported loss of life.

3.2.2 TV-tower in Kiev, Ukraine

The attack on the TV tower in Kyiv was a combined assault employing both physical means, in the form of missiles, and cyber means, through the “DesertBlade” trojan (Microsoft, 2022). This attack resulted in the loss of five lives and damage to hardware, leading to the disruption of broadcasting on the TV company's channels (Harding, 2022). Beyond instilling fear in Kyiv, where the attack occurred, the objective was to crush the hope and resistance of the Ukrainian people and their army. However, the (former) Minister of Defence of Ukraine expressed hopeful words, asserting that victory was the only option and that Ukraine would never surrender (ibid.). This suggests that the cognitive effects Russia intended to create were not entirely successful. Nevertheless, the event had a nationwide impact, affecting the entirety of Ukraine.

The attack on the TV tower in Kyiv can be classified as a Cyber Pearl Harbor under the DSLP-framework. The assault was a combined operation with different means of action that resulted in human casualties and had clear cognitive effects on the entire country. The only discrepancy lies in the fact that the cognitive effects did not completely paralyse Ukraine, as the nation continued to defend itself and encouraged its population to maintain hope.

3.2.3 Grocery company Coop in Sweden

The attack against Coop was executed solely through cyber means, specifically using ransomware (Toresson 2022). The physical effects of the attack included financial losses for the company, the closure of the majority of its stores, and a paralysed web shop (Truesec n.d.). The event's major cognitive impact was the increased concern among other companies about similar incidents, and the state of shock experienced by Coop during the attack (Stenberg 2022). In summary, although the attack occurred on a nationwide level for the company, it did not result in a societal paralysis. This is because Coop did not hold a monopoly on food sales, allowing

society to continue functioning relatively normally, albeit with Coop customers having to shop at other stores. The attack was surprising to society, but it was not paralysing. Moreover, it was purely a cyber-attack without any kinetic component, and no human deaths resulted from it. With these factors in mind, the Coop attack cannot be classified as a Cyber Pearl Harbor under the DSLP-framework.

4. Discussion

Panetta's definition of a Cyber Pearl Harbor describes an attack aimed at causing physical destruction, loss of life, and paralysing and shocking a nation (U.S. Department of Defense, 2012). However, this definition does not align with those shared by the interviewees, highlighting the current lack of a universal standard for the concept. Discrepancies were noted either in specific aspects of the concept, such as the element of surprise or the combination of several tools, or in the overall definition itself, such as questioning whether a Cyber Pearl Harbor could lead to loss of life. Due to this inability to agree on a standard definition, the probability of a Cyber Pearl Harbor was also dismissed entirely, contradicting the conclusions drawn by Huskaj (2023) in his article. This divergence could be a result of the absence of a universal definition and uncertainty about what exactly is required for an attack to be classified as a Cyber Pearl Harbor. This ambiguity could pose significant challenges in establishing prevention strategies within nations and organisations. Without an international standard to follow, a nation or organisation may expose itself to greater vulnerability and weaknesses than if such a standard existed.

Another key point raised was the scope of the concept, emphasising the importance of a Cyber Pearl Harbor being comprehensive, i.e., involving multiple entities. This aspect aligns with Panetta's definition, where a Cyber Pearl Harbor includes attacks against national infrastructure with the objective of significantly limiting or completely eliminating it.

The theme of combined tools was a recurring topic in all interviews, along with the consensus that a Cyber Pearl Harbor cannot currently be executed using cyber means alone. The interviewees noted that for an attack to be classified as a Cyber Pearl Harbor, it must result in a major impact, a result that the combination of tools can ensure. Although the use of combined tools is not explicitly mentioned in the DSLP-framework, it is hinted at in the criterion of “Cyber attacks & Kinetic attacks.” This criterion implies that a combination is occurring, as it involves the use of both cyber and kinetic attacks. It is noteworthy that the interviewees did not recognise this subtle connection, further exemplifying the confusion surrounding the concept of Cyber Pearl Harbor and how it persists due to the lack of a universal definition. Similar to the challenges in defining the overall concept of Cyber Pearl Harbor, additional uncertainties exist regarding what exactly constitutes a cyber attack, what constitutes a kinetic attack, and what actions are necessary to achieve these.

The respondents disagreed with the framework regarding whether a Cyber Pearl Harbor (CPH) has already occurred. In Huskaj's article (2023), where the framework was introduced, he suggests that this disagreement may stem from individual perceptions of what constitutes a CPH, as well as a narrow-minded approach among some cybersecurity experts. This conclusion is also supported by the literature review and interviews conducted in this study. One reason experts claim that a CPH has not yet occurred could be due to the rapid development of technology and digital means, which may have created a distorted perception of the power of combined attacks and the significance of cyber means, including influence operations such as deep fakes and disinformation.

During the interviews, estimates of the likelihood of a CPH were also discussed. Two out of three interviewees believe that the probability of a single attack reaching the level of a CPH is low, but they emphasise the uncertainty surrounding this assessment. The third interviewee anticipates a CPH occurring in the Russia-Ukraine war, viewing it as a potential decisive tool in the conflict. This contradicts the framework, which used cases from the Russia-Ukraine war and classified the event as a CPH. Generally, however, this interviewee perceives a high probability of a CPH, suggesting that it may already exist within our systems, yet to be executed. The interviewee argues that the constant digitalisation of society, increased use of IoT, and development of AI are creating vulnerabilities in nations for cyber warfare, necessitating more resources for cyber defence. Cyber-attacks may have evolved since 2012, when Panetta highlighted the issue, to a point where kinetic attacks are no longer required to cause human death, infrastructure failure, and shock. However, this evolution has not yet been widely recognised. The framework is based on Panetta's speech, which served as a warning about the threat posed by a CPH and the importance for nations to take it seriously and build defences against it.

Although the cases presented in this study did not meet the set criteria for a CPH, there is no indication that a future occurrence is impossible. This is particularly relevant in the context of cyberattacks against healthcare, a sector that has seen an increase in all forms of cyberattacks over the years. While the sector may not yet have fallen victim to a cyberattack at the level of a CPH, considering its crucial role in society and its high sensitivity, such an attack could very well occur (or may have already occurred without being noticed).

5. Conclusions

The results suggest that the current capabilities of cyber operations are not sufficient to create an event comparable to what might be classified as a Cyber Pearl Harbor (CPH); a combination of means is required, as the framework supports. While the framework posits that a CPH has already occurred, this case study's findings do not corroborate that assertion. The DSLP-framework does not explicitly state the likelihood of a CPH occurring. However, Huskaj's (2023) article, which identifies two instances of a CPH, allows for the assumption that the probability is relatively high. This study's results are mixed, with some aspects supporting this assumption and others contradicting it, leading to the conclusion that the probability of a CPH occurring remains indeterminate.

Currently, validating the framework is not feasible due to the insufficient data available to fully substantiate it. The majority of the existing data does not support the framework. Although there may be similar perceptions of the concept among respondents, the differences are too significant to form a consensus. Therefore, it is essential to involve a broader range of participants to collect more data, contributing to the development of a universal definition of the term.

Future research should aim to include a larger and more diverse group of respondents to gain a more comprehensive understanding of the research community's views, particularly regarding whether the majority align with Huskaj's definition of a CPH. Additionally, analysing suitable defence measures for attacks of this magnitude would contribute to enhancing cyber resilience. Further in-depth research into the cognitive effects of various attacks could also be valuable, potentially aiding in the future validation of the framework, especially in the context of a major hybrid operation.

References

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Caja Costarricense de Seguro Social. (2022). #Importante El Hospital de Niños urge comunicarse con familiares de pacientes en espera de cirugía ambulatoria referidos al área de salud Tibás [...] [Facebook post]. Facebook. https://www.facebook.com/ccssdecostarica/posts/5552368771453467

Clarke, R. A., & Knake, R. (2010). *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins.

Córdoba, J. (2022). Costa Rica public health system targeted by ransomware. *Associated Press News*. https://apnews.com/article/russia-ukraine-covid-politics-technology-health-0e24e6644b09e2737af96814635fcd22

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative* (4th ed.). Pearson.

Denscombe, M. (2014). *The Good Research Guide: For Small-Scale Social Research Projects* (5th ed.). Open University Press.

Dziwisz, D. (2022). Cyber Pearl Harbor is not coming: US politics between war and peace. *Understanding Contemporary Security*, 19(4), 95-109. https://doi.org/10.12797/Politeja.19.2022.79.07

ENISA. (2022). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Goldman, E. O., & Warner, M. (2017). Why a digital Pearl Harbor makes sense ... and is possible. In G. Perkovich & A. E. Levite (Eds.), *Understanding Cyber Conflict: Fourteen* Analogies (pp. 147-157). Georgetown University Press.

Harding, L. (2022). Ukraine says Russia targeting civilians as missiles hit Kyiv TV tower. *The Guardian*. https://www.theguardian.com/world/2022/mar/01/ukraine-russia-civilians-missiles-kyiv-tv-tower

Huskaj, G. (2023). Opérations offensives dans le cyberespace ciblant l'Ukraine: Un cyber Pearl Harbor? *Revue Militaire Suisse, Artikel Numéro Thématique - Ukraine - 2023*, 42-44.

Johannesson, P., & Perjons, E. (2014). *An Introduction to Design Science.* Springer International Publishing.

Kallberg, J. (2021). Bye bye, cyber Pearl Harbor. *CyberWire*. https://www.researchgate.net/publication/351980025_Bye_bye_cyber_Pearl_Harbor

Koch-Emmery, L., & Wikén, E. (2022). Attack mot tv-torn i Kiev – "Tystar medier som når ut längst". *SVT*. https://www.svt.se/nyheter/utrikes/attack-mot-tv-torn-i-kiev-tystar-medier-som-nar-ut-langst

Lawson, S., & Middleton, M. K. (2019). Cyber Pearl Harbor: Analogy, fear, and the framing of cyber security threats in the United States, 1991-2016. *First Monday, 24*(3). https://doi.org/10.5210/fm.v24i3.9623

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. RAND Corporation.

Microsoft. (2022a). Defending Ukraine: Early lessons from the cyber war. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/

Microsoft. (2022b). An overview of Russia's cyberattack activity in Ukraine. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd

Murillo, A. (2022). Latest cyberattack in Costa Rica targets hospital system. *Reuters*. https://www.reuters.com/world/americas/latest-cyberattack-costa-rica-targets-hospital-system-2022-05-31/

Riggi, J. (2020). Ransomware attacks on hospitals have changed. American Hospital Association. https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

Smith, G. (1998). An electronic Pearl Harbor? Not likely. *Issues in Science and Technology, 15*(1).

Stenberg, J. (2022). Experter: Därför är Coop-attacken bara början. *Tidningen Näringslivet*. https://www.tn.se/naringsliv/18119/experter-darfor-ar-coop-attacken-bara-borjan/

Straub, J. (2021). Defining, evaluating, preparing for, and responding to a cyber Pearl Harbor. *Technology in Society, 65*, Article 101599. https://doi.org/10.1016/j.techsoc.2021.101599

Toresson, J. (2021). It-attacken mot Coop – detta har hänt. *SVT*. https://www.svt.se/nyheter/inrikes/it-attacken-mot-coop-detta-har-hant

Truesec. (n.d.). Back in business after the largest ransomware attack of all time. https://www.truesec.com/why-truesec/cases/coop-back-in-business-after-the-largest-ransomware-attack-of-all-time

U.S. Department of Defense. (2012). Remarks by Secretary Panetta on cybersecurity to the Business Executives for National Security, New York City. https://content.govdelivery.com/accounts/USDOD/bulletins/571813

Vavra, S. (2021). What gets lost in "cyber Pearl Harbor"-style rhetoric. *CYBERSCOOP*. https://cyberscoop.com/cyber-pearl-harbor-911-cyberwar-hacking-leon-panetta-ciaran-martin/

Wirtz, J. J. (2018). The cyber Pearl Harbor redux: Helpful analogy or cyber hype? *Intelligence and National Security, 33(*5), 771-773. https://doi.org/10.1080/02684527.2018.1460087

Wirtz, J. J. (2017). The cyber Pearl Harbor. *Intelligence and National Security, 32*(6), 758–767. https://doi.org/10.1080/02684527.2017.1294379

Wither, J. K. (2022). Trends in warfare. In K. R. Lester (Ed.), *Encyclopedia of Violence, Peace, & Conflict* (3rd ed., pp. 241-253). Academic Press.

Whyte, C., & Mazanec, B. (2019). *Understanding Cyber Warfare: Politics, Policy and Strategy*. Routledge.