Known Unknowns: The Inevitability of Cyber Attacks

Virginia A. Greiman
Boston University, Boston, MA, USA
ggreiman@bu.edu

Abstract: As described by Former U.S. Secretary of Defense, Donald Rumsfeld in his 2011 book, Known and Unknown, "there are many things of which we are completely unaware—in fact, there are things of which we are so unaware, we don't even know we are unaware of them." Throughout history the world has faced numerous catastrophic events that were not foreseen but in hindsight were discoverable including the devastating effects of Pearl Harbor, and the September 11 terrorist attacks. More recently, the potential for catastrophic loss has been magnified in the 2020 Solar Winds and 2021 Colonial Pipeline cyber-attacks. We may not know when or how these events will occur or how much damage or destruction will occur, but we do know that these events are possible. The literature differentiates between events that occur totally by surprise, and outcomes or events that actors have identified as possibly existing but do not know whether they will take place or not. The aim of this paper is to provide insight, based on an empirical review of selected attacks both within and outside the cyber space literature to uncover the underlying risk, uncertainty, and complexity that may have been known but not seriously considered by those who had the knowledge and capability to investigate the warning signs. Based on the case study analysis, this paper will present the reasons for inaction and how we can learn from these experiences. The following two theories – institutionalization and rationalization have been found to provide some reasons for the occurrence of behaviors which increase the possibility of unobserved risks. In this paper we explore these theories through case study analysis and propose a framework consisting of four concepts for increasing awareness of these situations.

Keywords: Known Unknown, Cyber Attacks, Cyber Security Risk, Unobserved Cyber Risk, Risk Perception

1. Introduction

Notably, according to the Center for Strategic and International Studies, since 2006 there have been more than 900 major global cyber incidents that had potential for serious catastrophic loss (CSIS, 2023). In the United States, many Members of Congress have raised concerns over the frequency, types, and impacts of cyber incidents during hearings, speeches, and in legislation (Jaikaran, 2021). Cyber incidents affect nearly every national entity, from federal and state government agencies to non-profits, private companies and individuals.

The Director of National Intelligence is required annually to deliver to Congress an assessment from the intelligence community on worldwide threats. Recent assessments have highlighted cyberspace as an area of strategic concern, with Russia, China, Iran, and North Korea as the leading threat actors. Attacks from these countries include spying on government agencies by accessing agency computers, stealing sensitive information from public and private sector entities in the United States, and destroying or potentially destroying computer equipment (Jaikaran 2021).

In March 2022, The U.S. Justice Department unsealed charges accusing four Russian officials of carrying out a series of cyberattacks targeting critical infrastructure in the United States, including a nuclear power plant in Kansas, and evidently compromising a petrochemical facility in Saudi Arabia. The announcement covered hackings from 2012 to 2018, but served as yet another warning from the Biden administration of Russia's ability to conduct such operations (DOJ 2022).

The frequency, type, and impact of cyber incidents against and in the United States continues to grow (Statista 2021). In an effort to address this challenge, policymakers are considering a variety of solutions, such as denying opportunities for successful attacks by improving defenses and deterring adversaries from engaging in disruptive activities in cyberspace. In this research we introduce another solution: finding better ways to identify and respond to the unknowns.

To guide this research four cases studies were selected involving significant attacks both within and outside the cyber-attack literature and were investigated through a review of congressional hearings and witness statements to determine the specific context of an event and the response from the perspectives of the participants (Mills, Durepos and Wiebe 2010). The small number of cases selected reflects a desire to take a deeper look at each case rather than a quantitative analysis of a large number of cases.

1.1 Exploring the Unknown

Based on some of the most significant events of our time including the horrific attack on Pearl Harbor, the September 11 terrorist attack on the United States and the recent unprovoked attacks in Ukraine it is critical to

reduce uncertainty in our complex and unknown world if we are going to prevent repeating the catastrophic losses of the past. According to the Congressional Report on Pearl Harbor, early warning signs were neglected by the United States hours before the attack (U.S. Senate 1946). Because of the surprise factor, the potential that a weaker nation might use such an attack to target a stronger one and other potential similarities, these attacks have been commonly referred to as cyber Pearl Harbor attacks (Straub 2021).

In its report on the terrorist attacks of Sept. 11, 2001, the 9/11 Commission noted that the intelligence community, assailed by "an overwhelming number of priorities, flat budgets, an outmoded structure, and bureaucratic rivalries," had failed to pin down the big-picture threat posed by "transnational terrorism" throughout the 1990s and up to 9/11. In response to the 9/11 Commission's recommendations, Congress created a national intelligence director and the National Counterterrorism Center to pool intelligence.

Intelligence failures are commonly understood as the failures to anticipate important information and events, such as terrorist attacks. However, intelligence can fail for many reasons, often despite the best work of intelligence professionals (Dahl 2013). Explanations for intelligence failure generally include one of more of the following causal factors: organizational obstacles, psychological and analytical challenges, problems with warning information, and failures of political leadership (Copeland 2017).

Understanding the decision making behaviors that produce successful outcomes in the recognition and identification of known/unknown risk factors is essential to preventing and reducing the risk of catastrophic cyber-attacks. The serious problem of cyber-attack and cybersecurity means finding the "unknown unknowns" (MIT 2021). Former U.S. Secretary of Defense, Donald Rumsfeld, distinguishes between categories of risk (Rumsfeld 2011). These categories described below are recognized in the defense industry, risk management, and the cyber security literature among other disciplines though not always described in the same way.

1.2 Known Knowns

The first category is identified as "known knowns" describing the things we know we know. Examples could be an organization's location, the individuals that are impacted, and other realities. Known knowns are assumptions that have been validated and are verifiable. However, it is important to recognize that known knowns need to be continually evaluated for change. For example, on the 12th of February 2002, Donald Rumsfeld, used a little known framework to help him in making the case for the invasion of Iraq. The known and unknown framework may tell us that a country has no weapons of mass destruction on a particular day, but a week later that may change.

1.3 Known Unknowns

The second category is defined as "known unknowns" describing the things we know can happen but we are uncertain of the results. Much scientific research is based on investigating known unknowns. In other words, scientists develop a hypothesis to be tested, and then in an ideal situation experiments are best designed to test the null hypothesis (Logan 2009, p. 712). Known unknowns are usually listed in an organization's risk register and mitigated to the extent possible. For instance, we may be aware of certain possible events such as the existence of hurricanes and weather change in certain locations and at certain times of the year, but we don't know what the impact might be and when and where the damage may occur. As humans, we know we are mortal but we don't know how long we will live. Or, we know we may have economic downturns in the future, but we don't know when and for how long they may occur.

1.4 Unknown Unknowns

The third category is defined as the "unknown unknowns". This category describes uncertainties that we could not have known in advance and let alone foresee their consequences, e.g., natural cataclysms. Unknown unknowns can arise from lack of awareness, insufficient information or knowledge, and from organizational, psychological, political, or cultural blindness. These risks often cannot be identified precisely due to multiplicity, but whose total negative impact appears certain. These include an act of terrorism, criminal acts, a depression or revenue risk. We may not know when or how these events will occur or how much damage or destruction will result from the event (unknown), but we do know that all of these events are possible.

1.5 Unknown Knowns

As described by Donald Rumsfeld, these are things we know, but don't know we know. Often, they are uncovered after the fact. For example, we may know that every major cybersecurity incident is a wake-up call for the nation, (known) however, no decisions were made on this knowledge as the immediate memories of the incident fade. We know that in the cyber world supply chain attacks can occur (known) but we may not have investigated our own supply chain to know how serious the problem may be (unknown). Unknown knowns have been found to be commonplace in organizations because we can know things, but not realize how important they are or how they fit together. The Solar Winds attack is a great example of an unknown known.

1.6 Theories of Unobserved Risk

The literature reflects the following theories – institutionalization and rationalization to provide some reasons for the occurrence of behaviors which increase the possibility of unobserved risks. We explore these theories to provide a deeper understanding of how these may impact the ability to uncover the unknown.

1.7 Institutionalization: The 9/11 Terrorist Attacks

The very structure of business and governmental organizations, particularly those that are large and complex, makes it difficult to anticipate predictable surprises. Because companies are usually divided into organizational silos, the information leaders need to see and assess an approaching threat is often fragmented (Watkins and Bazerman 2003). Various people have various pieces of the puzzle, but no one has them all. And those at the top inevitably receive incomplete and distorted data. On September 11, 2001 various government agencies had pieces of information on terrorists' methods and plans that, had they been combined, would have pointed to the type of attack that was carried out against the World Trade Center and the Pentagon. Tragically, the information remained fragmented.

According to the 9/11 Report, "most of the intelligence community recognized in the summer of 2001 that the number and severity of threat reports were unprecedented. "Many officials told us that they knew something terrible was planned, and they were desperate to stop it. Despite their large number, the threats received contained few specifics regarding time, place, method, or target. Most suggested that attacks were planned against targets overseas; others indicated threats against unspecified 'U.S. interests.'" We cannot say for certain whether these reports as dramatic as they were, related to the 9/11 attacks (Kean and Hilton 2004, pp. 262-263).

1.8 Rationalization: The Ariane 5 Rocket Disaster

Rationalization enables system operators to convince themselves that not responding to a risk or threat is not only legitimate, but acceptable and perhaps even necessary. The justification for deviating from a standard, process or procedure includes the belief that the procedure is unnecessary or the work environment is dynamic, unstable and unpredictable.

On June 4, 1996, the massive Ariane 5 rocket, launched on its maiden voyage from the European Space Agency's center in French Guiana, exploded 39 seconds into flight, destroying four satellites on board (ESA, 1996). At an altitude of about 3700 m, the launcher veered off its flight path, broke up and exploded. According to the Inquiry Board Report: The failure of the Ariane 501 was caused by the complete loss of guidance and altitude information 37 seconds after start of the main engine ignition sequence (30 seconds after lift-off).

In a postmortem analysis, the European Space Agency (ESA) noted that the problem was due to a malfunction in the rocket's guidance system software, and it acknowledged that the system was not fully analyzed or understood, perhaps because the software had worked successfully with Ariane 4 (Ramesh and Browning 2014) and the participants rationalized it would work again. More generally, the disastrous outcome was due to an uncertainty of which the Agency was unaware prior to the launch— (an unknown unknown). Yet was this uncertainty truly unknowable, or was it potentially knowable but just escaped recognition from the project team? (Greiman 2023)

1.9 Case Studies

For purposes of this research four case studies were selected shown in Table 1 to understand the circumstances that led to two of the worse disasters in the history of mankind – The devastating attack on Pearl Harbor on

December 7, 1941 - and the terrorist attack on the World Trade Center on 9/11. The Solar Winds Attack in 2020 and the Colonial Pipeline attack in 2021 were selected to demonstrate the catastrophic potential of a cyber-attack when warnings are not heeded. Each case is analyzed based on the following five factors (1) the event or threat; (2) the warnings provided; (3) the reasons attributed to the failure to respond; (4) the impact of the event; and (5) the attribution.

Table 1: Case Studies on Responses to Known and Unknown Events

Event/Threat	Warnings	Failure to respond	Impact	Attribution
Pearl Harbor December 7, 1941	Japanese submarine sunk in the harbor; Japanese patrol planes spotted on radar but disregarded. The Japanese Armada of attack planes were mistakenly identified as a fleet of U.S. bombers (U.S. Senate 1946).	Gross incompetence or outright dereliction of duty on the part of the officers and officials in charge (U.S. Senate 1946); Background of noise, extraneous or misleading information that can obfuscate emerging events (Wohlstetter 1962)	The attack on Pearl Harbor took the lives of more than 2,400 Americans and sunk or damaged 21 ships in the U.S. Pacific fleet (U.S. Senate 1946).	"The ultimate responsibility for the attack and its results rests upon Japan," the final congressional committee report concluded, and "the diplomatic policies and actions of the United States provided no justifiable provocation whatever for the attack by Japan on this Nation" (U.S. Senate 1946)
September 11 Terrorist Attacks	The system was blinking red (Kean and Hamilton 2004, n. 30, p. 517). Various government agencies had pieces of information on terrorists' methods and plans that, had they been combined, would have pointed to the type of attack that was carried out against the World Trade Center and the Pentagon. Tragically, the information remained fragmented (Kean and Hamilton 2004).	"The September 11 attacks fell into the void between the foreign and domestic threats. The foreign intelligence agencies were watching for foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the U.S. No one was looking for a foreign threat to domestic targets. The threat that was coming was not from sleeper cells. It was foreign-but had come from foreigners who had infiltrated into the United States" (Kean and Hamilton 2004, p. 63).	September 11 took the lives of 2,977 innocent people. The United States' response to the 9/11 attack, namely the invasion of Afghanistan, had a deeply destabilizing impact on the Middle East and North Africa region. In addition to the death of tens of thousands of Afghanis and others from the region, as well as the emergence of new terrorist groups.	Invasion of Iraq and Afghanistan; however, the threat of Taliban retaliations still exist today.
2021 Colonial Pipeline Ransomware	Attacks on critical infrastructure was entirely predictable when Stuxnet was discovered in 2010. Refusal to participate in physical and cyber pipeline security TAS assessments showed complacency and over confidence (Congress 2021).	Response plan did not include ransomware – even though ransomware attackers had been targeting critical infrastructure since 2015 (Congress 2021)	The attack on May 7 resulted in a week-long shutdown of 5,500 miles of petroleum pipeline on the East Coast that clearly represents a significant cyber-attack on critical transportation infrastructure	The lack of a global agreement on legal attributions of criminal responsibility portends a continuation of cyber-attacks until an agreement is reached.
2020 Solar Wind Hack Espionage-based assault	Prior to and throughout the long period of attack there were allegations of missed opportunities, hints of problems that were ignored, lax security and the failure of U.S. intelligence officials to connect the dots of the supply chain attack and the insertion of the	As one expert expressed, there was not enough detail to report the problem to SolarWinds or the U.S. government. "We thought we didn't have enough evidence to reach out," (Temple-Raston 2021). Critics said they should have seen the hackers	Broad attack on confidential information of U.S. Government including Homeland Security and the Pentagon and the tech tools used by companies to protect them. SolarWinds estimates that 18,000 of its over 300,000 customers are vulnerable to this malware. The U.S.	Alleged Russian Hacker Group. In April 2021 President Biden ordered a new round of economic sanctions on Russia — a response in part to a Kremlin-linked computer breach that penetrated numerous U.S. government networks.

Event/Threat	Warnings	Failure to respond	Impact	Attribution
	malicious code (Temple-Raston 2021).	from the Russian intelligence service, the SVR, preparing this attack (U.S. Senate 2021).	government estimates that as many as 250 government agencies and companies may have been affected (U.S. Senate 2021).	

1.10 Reducing the Uncertainty Surrounding Cyber Events

Due to the page limitation of this paper, we cannot fully explore the reasons behind the failure of individuals to respond to warnings of potential cyber threats or the theories behind these failures, and will reserve this analysis for future research with a larger number of case examples. Instead, in the balance of this paper we will focus on solutions to reducing the potential for unknowns by creating greater awareness of the threat environment. Thus, reducing the likelihood that institutionalization of rationalization will interfere with the opportunity to recognize the potential for a cyber-attack. The theory being that by reducing uncertainty, the potential victims will be better prepared to respond to the unknown, especially when cyber-attacks cannot be fully prevented or predicted. The framework and concepts below are intended to explore the various ways in which organizations can address uncertainty and limit the likelihood that warning signs will be ignored. through discovery-driven planning or by systemically probing for knowledge gaps

1.11 Framework and Concepts for Responding to the Unknown

The following four concepts were derived from the literature on dealing with the unknown in complex, intractable and sometimes impossible situations: (1) Accountability at the international level; (2) Reducing uncertainty; (3) Mindful organizing and (4) Sensemaking.

These concepts have emerged from research and actual experience from both failed and successful outcomes from unexpected attacks both within and outside the cyber-attack literature particularly when faced with significant or emergent events with an element of surprise. Though not all of these concepts will be beneficial in all circumstances, the goal is to encourage reflection and stimulate ideas for approaching the unknown and uncertainty that lies in today's complex global domain of cyberspace.

These concepts are summarized in the framework shown in Figure 1.

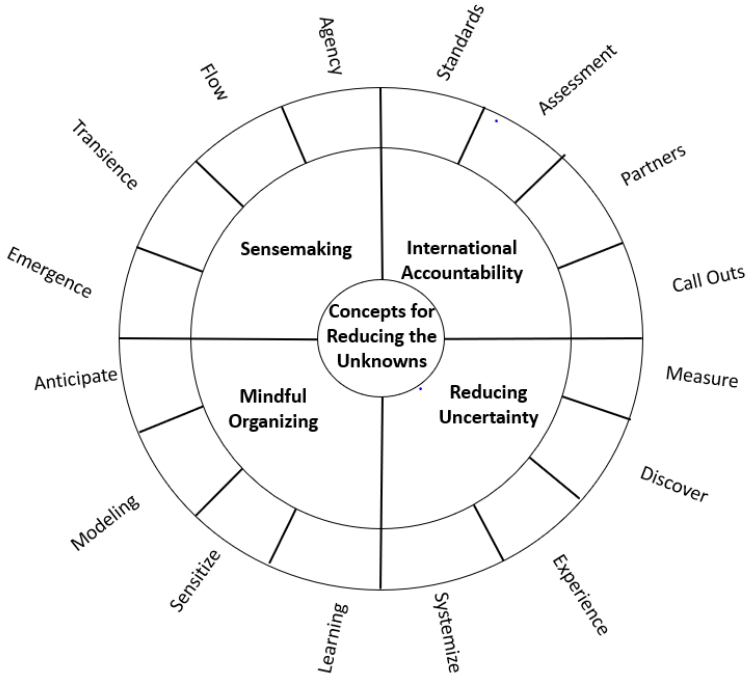

Figure 1: Concepts for Reducing the Unknown

2. International Accountability

National government and intergovernmental organizations as well as legal scholars have noted the need for accountability at the international level when one country is wrongfully attacked by another (Kuntz 2013; CEEAA 2014). Scholars recognize that States must develop accountable attribution mechanisms for international law to have practical value in the cyber sphere (Banks 2019).

An effective way of enhancing international accountability may be the establishment of standards or norms as proposed by NATO, the OECD, and other transnational organizations. “This requires a calling out of wrongful acts conducted by other states, through a harmonized attribution process, something that victimized states have been reluctant to do” (Hathaway 2017, p. 5). Moreover, because states are unable to affect the risk calculus of other states through conventional deterrence mechanisms, the next best thing is to foster an environment in which states consistently interact to provide information to one another (Brantly 2021).

Several non-state-driven norms-making initiatives have sought to fill the void, including Microsoft's (2016) cyber norms proposals, the Tallinn Manual project (Tallinn 2017), and the Global Commission on the Stability of Cyber Space (GCSC) (Eggenschwiler 2020). Scholars have contended that this emerging body of non-binding norms presents states with a critical window of opportunity to reclaim a central law-making position, similar to historical precedents including the development of legal regimes for Antarctica and nuclear safety (Mačák 2017).

Researchers have proposed a due diligence framework or minimal standards for attribution of cyber-attacks (Chircop 2018). Though due diligence is not clearly defined in the law it was reflected by the International Court of Justice (ICJ) in its Corfu Channel Judgment: “It is every State’s obligation not to allow knowingly its territory to be used for acts contrary to the rights of other states” (Corfu 1949) and has been set forth as an obligation of States in the pronouncements of the International Law Association (ILA 2014).

According to the Defense Science Board (DSB 2017) as offensive cyber capabilities continue to grow, and are likely to outpace cyber defense, there are likely to be growing risks of misperception that could lead to rapid cyber escalation – and the potential for rapid escalation to armed conflict requiring the necessity of working closely with the private sector.

3. Reducing Uncertainty

Lenfle and Loch (2017) in their studies of megaproject failure found that the first of the three major causes of failure is: “Underestimation of or refusal to acknowledge uncertainty.” Thus, an increase in complexity often means that it is more difficult to comprehend the effect of influencing one element; hence there is increased uncertainty. Put differently, uncertainty refers to the components, relationships, and interactions we do not fully comprehend or of which we may not even be aware. Complexity and uncertainty are thus strongly related (Salet 2021).

Finding ways to reduce the unknown is a central focus of this research. Thus, reducing uncertainty will contribute to the goal of reducing surprise and preventing potential cyber disasters. Experience has found that uncertainty that is unforeseen can be diagnosed through discovery-driven planning or by systemically probing for knowledge gaps (McGrath and McMillan 2000). Uncertainty refers to the possibility of emergent indeterminate events. Traditionally, organizations particularly in cyber security have focused on what economists call risk and have not tended to deal explicitly with uncertain, emergent, and unforeseen events (Miller and Hobbs 2005).

4. Mindful Organizing

The wisdom of learning from failure is incontrovertible. Yet organizations that do it well are extraordinarily rare. High-reliability-organizations (HROs) are an example of organizations that have developed practices to help prevent catastrophic failures in complex systems like nuclear power plants aircraft carriers through early detection. According to Weick & Sutcliffe (2015) HROs demonstrate particular characteristics in the way they operate: anticipating problems (being aware of what is happening in the work system; being alert to ways in which an incident could occur; looking beyond simplistic explanations for incidents; and containing problems using relevant expertise regardless of where it is situated within the organizational hierarchy). They identified five principles they define as “mindful organizing” that include preoccupation with failure, a reluctance to simplify, a sensitivity to operations, a commitment to resilience and a deference to expertise as a shared set of values that foster resilience through constant communication and recalibration in the face of unknowable risks (Weick & Sutcliffe 2015). High reliability theory should be explored in the cyber field because of the high potential

for catastrophic outcomes from a cyber incidence. For instance, a cyber-attack on a nuclear plant could have long lasting and deadly consequences.

5. Sensemaking

Sensemaking, a term introduced by Karl Weick, refers to how we structure the unknown so as to be able to act on it and has been defined as a key leadership capability for the complex and dynamic world we live in today (Ancona 2011). Sensemaking involves producing a plausible understanding—a map—of a shifting world; testing this map with others through data collection, action, and conversation; and then refining, or abandoning, the map depending on its credibility.

As described by Weick, Sutcliff and Obtsfeld (2005) to focus on sensemaking is to portray organizing as the experience of being thrown into an ongoing, unknowable, unpredictable streaming of experience in search of answers to the question, "what's the story?" (Weick et al 2005). Plausible stories animate and gain their validity from subsequent activity. The language of sensemaking captures the realities of agency, flow, equivocality, transience, re-accomplishment, unfolding, and emergence, realities that are often obscured by the language of variables, quantities, and structures (Weick et al 2005). Students of sensemaking understand that the order in organizational life comes just as much from the subtle, the small, the relational, the oral, the particular, and the momentary as it does from the conspicuous, the large, the substantive, the written, the general, and the sustained (Weick et al 2005). The concept of sensemaking fills important gaps in organizational theory.

5.1 Future Approaches to Counter Cyber Attacks

The approach taken by most organizations to counter cyber-attacks is defensive and reactionary. Threats are only removed and analyzed once they are detected; at which point, the harm is done—the network has already been breached and valuable information compromised.

A lot of solutions have been offered to prevent or reduce cyber-attack impacts, including mandatory reporting requirements, wider use of multi-factor authentication, requiring a software bill of goods, and significantly improving threat information sharing between the government and the private sector. However, these solutions will not be sufficient in light of the lack of understanding of the large number of unknown unknowns prevalent in the domain of cyber space.

Predictive analytics will have a prominent role in the future of cybersecurity given its use of historical data and statistical algorithms to predict future threats. The most promising aspect of predictive analytics is that with the meteoric rise in machine learning through Artificial Intelligence (AI), it will be possible to teach machines how to do it; through which human error can be eliminated. This will introduce a very high level of efficiency to detecting threats very early on while giving cybersecurity a chance to be proactive instead of reactive.

6. Conclusion:

Cyber security risk in the U.S. and around the world is a major national security threat impacting all nations. Analyzing the underlying causes for failure to respond to these threats can make these surprise attacks less likely. Cyber security failures will no longer be inevitable if we find ways to identify and take appropriate action on the unknowns so that policymakers may gain a greater understanding of the cyber risks that the nation and the world faces. Knowledge of known adversaries, the types of activities they conduct online, and how they are identified by national governments will inform the debate Until we have a greater understanding of the reasons behind the failure to respond to the warning signs of potential cyber-attacks the inevitability of countering cyber-attacks before they occur will remain.

Acknowledgements

I would like to thank my graduate research assistant, Renee Macasaet for the extensive and valuable research she contributed to this paper.

References

Ancona, D. (2011) Sensemaking: Framing and Acting in the Unknown. In: S. Snook, N. Nohria, & R. Khurana, (eds.) (2011). *The Handbook for Teaching Leadership: Knowing, Doing, and Being*. Thousand Oaks, CA: Sage Publications.

Banks, W. (2019) The Bumpy Road to a Meaningful International Law of Cyber Attribution. *American Journal of International Law* Unbound, vol. 113, pp 191-196. doi:10.1017/aju.2019.32.
Brantly, A.F. (2021) Risk and uncertainty can be analyzed in cyberspace. *Journal of Cybersecurity*, 2021, 1–12.
Center for Strategic and International Studies (2022) *Significant Cyber Incidents Since 2006*, CSIS, Washington, D.C.
Chircop, L. (2018) A Due Diligence Standard of Attribution in Cyberspace. *International and Comparative Law Quarterly*, Vol. 67, no. 3, pp 643-668. doi:10.1017/S0020589318000015.
Copeland, T.E. (2017) *Intelligence Failure Theory*. International Studies Association and Oxford University Press, Oxford, England.
Corfu Channel (United Kingdom v Albania) (Judgment) [1949] ICJ Rep 4, 22 (Corfu Channel).
Dahl, E. (2013) *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond.* Georgetown University Press, Washington, D.C.
Defense Science Board (DSB) (2017) *Task Force on Cyber Deterrence*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D.C.
Eggenschwiler, J. (2020) Expert commissions and norms of responsible behaviour in cyberspace: a review of the activities of the GCSC. *Digital Policy, Regulation and Governance*, Vol. 22 No. 2, pp. 93-107. https://doi.org/10.1108/DPRG-03-2019-0019.
Greiman, V.A. (2023) *Global Megaprojects: Lessons, Case Studies and Expert Advice on International Megaproject Management*. John Wiley & Sons, Hoboken, NJ
Hathaway, M. (2017) *Getting Beyond Norms*, CIGI Papers No. 127, Centre for International Governance Innovation, Ontario, Canada.
International Law Association (ILA) (2014) ILA Study Group on Due Diligence in International Law (First Report, ILA, 7 March).
Jaikaran, C. (2021) Cybersecurity: Selected Cyberattacks, 2012-2021. Congressional Research Services (CRS), Washington, D.C.
Kean T.H., and Hamilton L.H. (2004) *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States*. Norton, New York, NY.
Kuntz, R. L. (2013) How Not to Catch A Thief: Why the Economic Espionage Act Fails to Protect American Trade Secrets, 28 *Berkeley Tech. L.J.* 901.
Lenfle, S. and Loch, C. (2017) Has Megaproject Management Lost Its Way?: Lessons from History. In B. Flyvbjerg (ed.) *The Oxford Handbook of Megaproject Management*, 21-38. Oxford University Press, Oxford, England.
Logan, D. C. (2009) Known knowns, known unknowns, unknown unknowns and the propagation of scientific enquiry. *Journal of Experimental Botany*, Vol. 60, No. 3, pp. 712–714.
Mačák, K. (2017) From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers. *Leiden Journal of International Law*, Vol. 30, No. 4, pp 877 – 899.
McGrath, R.G. and MacMillan, I.C. (2000) *The Entrepreneurial Mindset: Strategies for Continuously Creating Opportunity in an Age of Uncertainty,* The Fellows of Harvard College, Cambridge, MA.
Microsoft (2016) *From articulation to implementation: Enabling progress on cybersecurity norms*, White Paper, Microsoft, Redmond, Washington.
Mills, A. J., Durepos, G., and Wiebe, E. (Eds.) (2010) *Encyclopedia of case study research*. Sage Publications, Inc. Thousand Oaks, CA.
MIT Technology Review Insights (2021) Better cybersecurity means finding the "unknown unknowns." MIT, Cambridge, MA.
Ramesh, R.V. and Browning, T.R. (2014) A conceptual framework for tackling knowable unknown unknowns in project management. *Journal of Operations Management* Vol. 37 (4) 190-204.
Rumsfeld, D. (2011) *Known and Unknown: A Memoir*. Sentinel, Penguin Publishing Group, USA
Salet, W. (2021) Public Norms in Practices of Transitional Planning: The Case of Energy Transition in The Netherlands. *Sustainability* Vol.13, 4454. https:// doi.org/10.3390/su13084454
Statista, U.S. Companies and Cyber Crime, (2021). https://www.statista.com/study/12881/smb-and-cyber-crime-in-theunited-states-statista-dossier/.
Straub, J. (2021) Defining, evaluating, preparing for and responding to a cyber Pear Harbor. *Technology in Society*, Vol. 65, 101599.
Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017). Michael N. Schmitt (ed.) 2nd ed. Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), Cambridge University Press.
Temple-Raston, D. (2016) A Worst Nightmare' Cyberattack: The Untold Story Of The SolarWinds Hack. All Things Considered, National Public Radio (NPR). https://www.npr.org/2021/04/16/985439655/a-worst-nightmare-cyberattack-the-untold-story-of-the-solarwinds-hack.
U.S. Congress (2021) *Cyber threats in the pipeline: lessons from the federal response to the colonial pipeline ransomware attack*. 117th Congress (2021-2022).
U.S. Department of Justice (2022, Mar 24) Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide. DOJ, Office of Public Affairs, Washington, D.C. https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical.

U.S. Senate (2001) Hearing Before the Select Committee on Intelligence of the United States Senate, Hack of U.S. Networks by a Foreign Adversary. 117th Congress, First Session. Tuesday, February 23, 2001.

U.S. Senate Historical Office (1946) Report of the Joint Committee on the Investigation of the Pearl Harbor Attack. (The Pearl Harbor Committee). U.S. Senate, Washington D.C.

United States Cyber Economic Espionage Accountability Act (CEEAA) Summary: H.R.2281 — 113th Congress (2013-2014).

Watkins, M.D., and Bazerman, M.H. (2003) Predictable surprises: the disasters you should have seen coming. *Harvard Business Review*, Vol. 81, No. 3, pp. 72-80, 140.

Weick, KE, and Sutcliffe KM. (2015) *Managing the Unexpected: Sustained Performance in a Complex World* (3rd ed.) John Wiley & Sons, Hoboken, NJ.

Weick, K.E., Sutcliffe. K.M. and Obstfeld, D. (2005) Organizing and the process of sensemaking. *Organization Science* Vol. 16 (4) pp. 409-421. Institute for Operations Research and the Management Sciences.