# CYBERATTACKS AND THE EROSION OF STATE SOVEREIGNTY

***Ana Maria COSTEA*** [*]
***Mihail CARADAICĂ*** [**]

**Abstract.** *This paper will tackle the issue of cyberattacks and the Erosion of State Sovereignty as cyberattacks have become a significant challenge to state sovereignty in the 21st century, threatening traditional concept of territorial control as well as the modern reliance on digital infrastructure. As technology evolved, cyberattacks developed the ability to bypass national borders and undermine state authority, creating a significant impact on how sovereignty is understood and protected. Considering the theoretical contribution of Carl von Clausewitz on new forms of warfare and Joseph Nye Jr.'s on cyber deterrence, the aim of this paper is to analyze examples such as WannaCry, Stuxnet, SolarWinds, and Heartbleed and to reveal the extent to which cyber operations can erode state sovereignty and challenge international norms.*

**Keywords:** *Cyberattacks, sovereignty, warfare, deterrence, cyberwar.*

## Introduction

The article addresses an important issue for international arena today, which is the impact of cyberattacks on state sovereignty. The methodology of the study will employ in theoretical and case study analysis. Using the theoretical contribution of Carl von Clausewitz on warfare and Joseph Nye Jr. on deterrence, the research builds a theoretical framework to understand the cyber threats as distinct and influential force in modern stated affairs. These theories allow us to analyse the strategic and political dimensions of cyberattacks and to investigate how these new digital threats are challenging the framework of understanding of state sovereignty without relying on traditional warfare. In addition to the theoretical background, the research focuses also on four case studies meant to illustrate the practical implications of cyber deterrence and sovereignty erosion. WannaCry, Stuxnet, SolarWinds, and Heartbleed were selected to highlight how various cyber operations disrupted critical infrastructure, exploited technological vulnerabilities, and impacted state sovereignty. These incidents are examined for their impacts as well as to highlight more general trends in cyberwarfare, like how simple it is to cross national borders online and how challenging it is to assign responsibility for attacks.

[*] Associate Professor PhD, National University of Political Studies and Public Administration (SNSPA). E-mail: anamaria.costea@dri.snspa.ro

[**] Lecturer in European Studies, National University of Political Studies and Public Administration (SNSPA), Department of International Relations and European Integration. E-mail: mihai.caradaica@dri.snspa.ro.

**Clausewitzian Approach to Cyber Warfare**

Carl von Clausewitz was a military theorist of the 19th-century who dedicated his main work to the nature of war, focusing on its strategic, political, and psychological dimensions. Nowadays, Clausewitz's concept of war as an extension of politics is still valid, but it needs to be adapted to the new realities. While traditional warfare involves the mobilization of physical force in order to achieve its political objectives, a cyber warfare is conducted in a virtual environment involving digital targets and tools.

The Clausewitzian approach and the emergence of the so-called new types of wars have divided the academic community. There are scholars who have deepened the idea of new wars, stating that the ongoing revolution of military affairs has changed the very nature of warfare (Lambeth 1997, 75). In their view, both the traditional Westphalian state-centric model and the Clausewitzian approach have faced several challenges dictated by security dynamics nowadays (Wilkinson 2003, 29): i.e. when referring to low-intensity conflicts. Also, there are scholars who consider that the Clausewitzian theory is not yet outdated. They emphasise that Clausewitz's ideas still have the lead (Gray 1999), and that even the low-intensity conflicts can be viewed and understood through the Clausewitzian lens. Besides, in their opinion, this would be the only way to view such actions (Smith 2003, 19). It all depends on how Clausewitz's words are interpreted. **In our paper, given the aforementioned arguments** (and the diverse nature of actors involved in a cyberwar: international organisations, national states, organised crime, organised and unorganised groups of individuals, and individuals), **we tend to agree with the latter definition**.

Another example in this sense could be a successful cyber-attack on the bank system or the electric grid of one major city like New York, London or Berlin, etc. This would have a huge impact upon the security of the society. Individuals would not have access to their financial goods, and consequently they would not be able to provide for fundamental needs such as food or water. This could generate riots, a flare-up of criminal acts, and thus physical destruction. In the case of an attack on the electric grid, we could deal – in the worst-case scenario – with a situation similar to the Stone Age, since nowadays society is dependent on electricity. In the academia, it is accepted consensually that we have not yet seen a fully-fledged cyberwar, but if it is going to happen, its results will be very costly, and it might even be lethal (Junio 2013). In order to frame it, the terms 'force' and 'violence' need to be deconstructed, and related to the matter of lethality (Stone 2013). Hence, cyberwar can take different forms and have multiple consequences, but it is definitely war.

Secondly, as Clausewitz mentioned, war represents a paradoxical trinity. From this perspective, Thomas Rid (2012) considers that a cyber offensive act may be deemed an act of war, if it is "*violent, instrumental and political*" (Rid 2012, 2). According to him, no single cyberattack has yet met all the three criteria. In this sense, he gives the examples of the 1982 blow up of the Siberian Pipeline, the 2007 Estonian attacks, the Russian cyberattacks during the war with Georgia, etc. (Rid 2012, 10–15).

Thus, in our research, we shall consider that a cyberattacks becomes possible especially due to the impact of globalisation on the weapon systems, impact that generated deep transformation in technological areas, such as sensors, communications or computers. Thereby, the depth of the transformation encompasses the war's arena (space and cyberspace), and the way war is waged (speed and weaponry) (Larsdotter 2004, 135). From this perspective, time and distance are tremendously reduced, while critical digital infrastructure (such as large amounts of data, servers or telecommunication

networks) becomes one of the main targets of a probable – in our view – future war. Yet, the rationale behind such actions remains the same: the continuation of politics with other means.

**Types of Deterrence in Cyberspace: Joseph Nye Jr.'s Framework**

Another theoretical approach used to better frame the cyberattacks and their impact on state sovereignty is called deterrence in cyberspace and it has been introduced by Joseph Nye Jr. According to him, in the physical world, deterrence often relies on the threat of retaliation or punishment, while in the cyberspace the lack of clear attribution, the velocity of attacks, and the involvement of non-state actors make deterrence more complex. In this regard, Nye outlines several types of deterrence in cyberspace (Nye Jr. 2017):

- **The threat of punishment**. This is the classical type of deterrence in which the enemy chooses not to attack you for fear of your retaliation (Nye Jr. 2017, 55). Thus, the cost of war is too large for him/her to consider the attack, if he/she is to be rational in terms of costs and benefits.
- **Denial by defence**. This strategy refers to one's capacity to defend, recover and respond, and thus underscores the resilience of the country under attack (Nye Jr. 2017, 56–57). In simple terms, the walls are so high, that the enemies consider an attack to be futile, because they will not succeed in penetrating them.
- **The entanglement**. This type of deterrence refers to the high level of inter-dependence created by the globalisation phenomenon for the majority of entities (organisations or states). From this angle, although there is no fear of retaliation and/or of defence against the attack, the attacker may consider that the status quo is more beneficial, and therefore he will choose not to attack (Nye Jr. 2017, 58).
- **The normative taboos**. This fourth type of deterrence is rather similar to the previous one, except that here norms are the main element that discourages an actor from launching an attack for fear of losing his status or part of his soft power projection. An example in this sense could be the possibility of using a nuclear weapon in a low-level conflict (Nye Jr. 2017, 60). Another example adapted to cyberspace would be an attack conducted by the US against France's or Germany's critical infrastructure. Such an action would damage the Image of the US as a reliable partner, thus affecting its position at the international level.

Therefore, it is rather difficult to believe that deterrence really works in the cyberspace, due to various reasons, such as: the issue of attribution, the multiple types of actors involved and their numerous rational/irrational strategies and motives, the absence of a standard and the inability to use the same weapon twice with the same effect.

At the same time, the concept of cybersecurity involves some specific challenges with regard to the application of deterrence strategies (one of the main elements of Article 5). Joseph Nye proposes four layers of deterrence. However, the direct applicability of this conceptual framework is not without difficulties. Deterrence through the threat of punishing or of a retaliatory cyberattack is not as simple or as conventional as nuclear deterrence. Firstly because "cyber-weapons" cannot be standardized by calibre, firepower, range, TNT kilotons, or the power of a nuclear warhead. Secondly, cyber-tools are by definition stealthy, concealed: they cannot be displayed or presented as potent punishment weapons to deter the adversary.

Concluding, Nye emphasizes the importance of normative deterrence, while international norms and agreements create a collective understanding of unacceptable

behaviour in cyberspace. However, the effectiveness of these norms is often challenged by the difficulty of attributing cyberattacks to specific state actors and, also, by the lack of enforcement mechanisms. As this paper will show, the SolarWinds attack raised critical questions about the limits of cyber deterrence. Initially, it was attributed to Russia, but the complexity of responding to such a widespread espionage operation without escalating tensions, emphasised the limitations of both deterrence by denial and punishment in cyberspace.

**Case studies of Cyberattacks**

This chapter focuses on a comparative analysis of four major cyberattacks – WannaCry, Stuxnet, SolarWinds, and Heartbleed – that are emphasizing the evolving nature of a cyber warfare and its deep profound socio-political and economic impact. While these attacks vary in origins, targets and objectives, they still share similarities like he ability to exploit technological vulnerabilities and disrupt critical infrastructure through ransomware (WannaCry), espionage (SolarWinds), or security flaws (Heartbleed).

**WannaCry**, the first case study, is probably one of the most relevant examples of cyberattacks with wide-ranging and complex consequences and lessons learned. Launched on Friday, May the 12th, 2017, this virus was targeting Microsoft Windows systems and affected more than 230,000 computers in 150 countries (Ehrenfeld 2017). The WannaCry ransomware explored a vulnerability of un-patched, not updated Microsoft Windows OS and, disrupted the operation of some public institutions and private companies such as Deutsche Bahn, FedEx, the Russian Central Bank, Telefónica, Megafon, or Russia's Interior Ministry (Mattei 2017). The first reaction of governments (Egloff and Smeets 2023) and private companies was to blame the USA, Microsoft or users who did not implement security upgrades (Huss 2017). However, after investigations, many accused North Korea because the first affected devices were the POS terminals of businesses in South Korea (Volz 2017). In the United Kingdom, the WannaCry attack particularly affected the NHS, even if it was not a specific target. In England, it affected at least 80 out of the 236 trusts, 603 primary care and other NHS organisations (Morse 2017). The total financial impact for NHS was £92 million, but its worldwide damage was around $4 billion (Kaspersky 2023). From a national/ regional security perspective, WannaCry is considered one of the most dangerous attacks. This rose the question whether it could potentially enter under NATO's Article 5 application area, since it affected also the critical infrastructure of state institutions such as hospitals (the medical staff could not even access the patients' files).

**Stuxnet** is another example of malware that was considered a game changer due to its sophisticated design and its ability to show that potent cyber weapons are not just simple science fiction story, but real political tools. It was discovered in June 2010 and classified as a cyber weapon designed to sabotage the Iranian nuclear programme (Collins and McCombie 2012, 80). Since its initial spread, Stuxnet has infected over 60,000 computers, more than half of them in Iran, and other states like: India, China, Indonesia, South Korea, Azerbaijan, Malaysia, USA, the United Kingdom (UK), Australia, Finland or Germany (Farwell and Rohozinski 2011, 23). This attack was a perfect example of state action designed to influence another state's behaviour by generating actual physical damage (i.e., damage to the Iranian nuclear power plants, by programming the centrifuges to rotate to such a high speed that they melted). According to David Fidler, the Stuxnet attack is a clear example of how cyber technologies can directly impact the realpolitik

(Fidler 2011, 56). This attack is of great importance for our research since it clearly had a political and security rationale behind it (to stop the Iranian nuclear program or at least to postpone it). According to public reports, it was supposedly developed by the USA and Israel with the aim of compromising Iran's nuclear programme. It is estimated that the attack has sent Iran 10 years back, since it affected the enrichment capacity of the nuclear fuel due to the physical destruction of the centrifuges. Here again, the question is whether the level of destruction could have been compared with that of an armed attack (*the physical damage, caused by this cyberattack upon a critical point from a military perspective, had large negative effects on the nuclear development programme which is of strategic importance in this field*), thus generating the possibility of a self-defence response under article 51 of the UN Charter (UN, n.d.). If that had been the case, Iran could have responded in a similar way, thus engaging in a cyberwar?

One of the most recent major cyberattacks took place in early 2020, and it was called "**SolarWinds**" – the name of a large-scale USA information technology company. In this case, hackers broke into the SolarWinds systems, and added a malicious code into the internal software called "Orion". The company reported that 18,000 of its 33,000 customers have installed updates that made customers vulnerable to hackers (Canales and Jibilian 2021). USA federal investigators and other cybersecurity experts stated that "*Russia's Foreign Intelligence Service, known as the SVR, was probably responsible for the attack. Russian intelligence was also credited with breaking into the email servers of the White House, the State Department, and the Joint Chiefs of Staff in 2014 and 2015. Later, the same group attacked the Democratic National Committee and members of the Hilary Clinton presidential campaign*" (Canales and Jibilian 2021). Russia has denied its involvement in this attack. Nonetheless, the Biden administration considered enacting sanctions against it, demonstrating that there can be actual political and economic consequences in the case of a high-impact cyberattack. Therefore, the sanctions were mainly applied to Russian technology companies, and they restricted the procurement of ICTS from the Russian Federation (Soliman et al. 2021).

Regarding personal data and how vulnerable the users are in front of cyberattacks, the **Heartbleed** cyber-virus is a perfect case study. It was discovered on April, the 7th, 2014 by both Google Security and a Finnish cybersecurity company. According to some media reports, it affected about half a million of Internet's secure web servers by exposing personal and financial data held by online operators (Banks 2015, 1–2). Heartbleed was in fact a flow in a software called Secure Sockets Layer (SSL), used for electronic transactions, and has permitted hackers to steal passwords from unsuspecting users (Lewis 2014, 294). The 'Heartbleed' bug in OpenSSL was viewed in particular as a case study, given the fact that it had an impact over both communities of influence and stakeholders (Jeske et al. 2017, 174). This attack shows that even secured transactions had a high risk of being exposed, highlighting the limits of sovereign states in the area of cybersecurity.

**Discussion: Cyberattacks and the Erosion of Sovereignty**

Since the Treaty of Westphalia in 1648 the concept of state Westphalia in 1648 was central for the theories that tries to explain international relations, emphasizing a state's exclusive control over its territory, political system, and people. In theory, there are two key elements to define sovereignty: internal sovereignty, that refers to the control of the state within its borders, and external sovereignty, where a state is recognized as an independent actor on international arena (Jensen 2012). Even more, realist theory argue

that sovereignty enables states to defend against threats, both internal and external, through military and economic means (Sassen 1999). However, global interconnectivity and the technological development have introduced complexities to this traditional model, challenging the efficacy of state sovereignty in the digital age.

As we already showed, because they may target vital infrastructure and cross-national borders without a military invasion, cyberattacks threaten state sovereignty. Traditional methods of defence and retaliation are becoming less and less successful because these attacks are frequently clandestine, untraceable, and can originate from both state and non-state actors. High-profile events like the WannaCry ransomware attack and the SolarWinds hack, which compromised national security in several nations, demonstrate this erosion of sovereignty (Lotriont e 2012). The difficulty of attribution is such kind of conflict, complicates the enforcement of international law as attackers remain unidentified, creating the conditions for violating another state's sovereignty (Egloff and Smeets 2023). For instance, U.S. and Israeli agencies claimed that Stuxnet, an unprecedented cross-border cyberattack, targeted Iran's nuclear facilities and disabled its centrifuges without a single soldier ever crossing the border (Egloff and Shires 2022). Therefore, in the next paragraphs we will consider the erosion of the state sovereignty from a legal perspective, regarding the role of attribution, the context of global governance and from the national policy making process.

From a legal point of view, international law has been slow to adapt to the challenges posed by cyberattacks. Although using force against a state's political independence or territorial integrity is forbidden by the UN Charter, it is uncertain if cyberattacks are included by this clause. One effort to address these concerns is NATO's Tallinn Manual on the International Law Applicable to Cyber Warfare. It is still a non-binding document, though, and it raises a number of issues, especially with regard to the standards for determining state accountability for cyberattacks (Egloff and Shires 2022). For this case, cyberattacks like Stuxnet and SolarWinds have pushed scholars in the legal field to rethink boundaries of state sovereignty and the rules governing state behaviour in cyberspace. The idea that sovereignty is linked to physical land is called into question by these attacks, which also make one wonder how international law might change to shield states against cyberattacks that do not employ conventional force. In the context of cyberattacks, the idea of non-intervention—which forbids forcefully engagement in another state's domestic affairs—has drawn special criticism. The application of this principle in the digital sphere is made more difficult by the clandestine character of cyber operations and the challenge of attribution (Nershi and Grossman 2023).

The role of attribution is also a pressing issue in the process of responding to cyberattacks. Unlike traditional warfare, where the identification of the aggressor is easier, cyberattacks are frequently organised by anonymous actors who can hide their identities using different techniques. An excellent illustration of this was Stuxnet, where the role of state actors was only revealed after an in-depth investigation. In a similar vein, it took months to attribute the SolarWinds attack to Russia, and this claim is still debatable in some circles (Trautman and Ormerod 2018). Without clear attributions, it is very difficult for a victim to justify a reaction or to pursue diplomatic solutions. Because of this ambiguity, states can more easily conduct cyber operations without worrying about a response, undermining the effectiveness of international rules. Due to this, cyberattacks such as SolarWinds and Stuxnet have created a situation in which governments can infringe on the sovereignty of other people with a high degree of impunity (Scaife, Traynor, and Butler 2017).

Another sign of state sovereignty erosion are the efforts made by the international community to develop a framework and to govern the state behaviour in cyberspace. At the UN level was established a working group with the purpose to set up new norms in order to shape state behaviour in cyberspace, including the principle that they should not knowingly allow on their territory any cyberattacks against other nations. However, these norms remain voluntary and non-binding, limiting their effectiveness in the mitigation process of cyber threats (Ghafur et al. 2019). This is also because many states view cyberspace as a new domain for asserting power and influence, making them more sceptical to reduce cyber capabilities. Cyber governance has consequently become fragmented, with several nations using various approaches to deal with the issue. As a result, the idea of sovereignty in the digital age is further undermined by a fragmented and frequently ineffectual international response to cyberattacks (Egloff and Shires 2022).

The national answers to cyber threats didn't take long to appear. Many countries have established national cybersecurity agencies and implemented laws designed to protect critical infrastructure from cyber threats. A good example here is the U.S. Cybersecurity and Infrastructure Security Agency (CISA) that hat a leading role in defending against cyberattacks and coordinating responses to incidents like SolarWinds (Beaman et al. 2021). However, these efforts are often slowed down by the global nature of cyberspace. Since attacks can come from anywhere in the world, no state can completely control or defend its digital borders. Because cyberspace is permeable, nations are depending more and more on private enterprises, non-state actors, and international cooperation to safeguard their networks, resulting in a growing sharing of sovereignty. The traditional idea of sovereignty, according to which governments are exclusively in charge of their own security, is called into question by this interconnectedness (Trautman and Ormerod 2018).

**Conclusions**

This article explores how cyberattacks are increasingly and constantly challenging the concept of the state sovereignty. In cyberspace, where strategic goals are pursued by digital tools rather than physical force, Clausewitz's theory that warfare is an extension of politics is modified. Unlike conventional combat, cyberwarfare takes place in a virtual environment and interferes with systems that governments rely on to maintain their sovereignty, such electrical grids and financial institutions. Because cyberattacks generate weaknesses that governments find difficult to solve through traditional combat or political means, the classical idea of state sovereignty needs to be revised.

Joseph Nye Jr.'s theory, on the other hand, is also very important for this analysis. According to Nye, deterrence in cyberspace is fundamentally different from deterrence in the real world because of things like the speed at which attacks occur and the difficulties in identifying specific criminals. His approach describes several deterrent tactics, including entanglement, punishment, denial by defence, and normative taboos. These ideas illustrate the difficulties a government encounters when is trying to preserve sovereignty through digital defences. Comparing with Cold War deterrence model, when nuclear capabilities were quite visible and enemies quite clear, cyber deterrence is more ambiguous, often leading to limited responses to attacks and, ultimately, an erosion of sovereign authority in cyberspace.

The case studies that we have identified in this article, including Stuxnet, WannaCry, SolarWinds, and Heartbleed, showed the vulnerabilities of the sovereign states. For instance, Stuxnet disrupted Iran's nuclear ambitions by demonstrating how cyber

technologies may be used to do physical harm. The SolarWinds hack exposed how even strong states are vulnerable to these kinds of attacks by compromising the digital infrastructure of several U.S. governmental organisations. The Heartbleed cyberattack revealed flaws in vital digital infrastructures that governments depend on to safeguard private data and keep control over their internal affairs, while WannaCry ransomware attack emphasis how cyber threats can disrupt essential public services and critical infrastructure across multiple countries. Each example point the effectiveness of cyber operations in bypassing traditional state defences.

In conclusion, the theoretical frameworks and case studies reveal a significant transformation of the nature of state sovereignty. Westphalian model needs to be revised as cyberattacks are not bound by geographical of physical limitation. Clausewitz's notion of warfare and Nye's deterrence theory are reframed according to new realities and the states are required to reconsider what sovereignty means in an era where digital threats pervade borders without crossing them physically.

## BIBLIOGRAPHY

Banks, James. 2015. 'The Heartbleed Bug: Insecurity Repackaged, Rebranded and Resold'. *Crime, Media, Culture* 11 (3): 259–79. https://doi.org/10.1177/1741659015592792.

Beaman, Craig, Ashley Barkworth, Toluwalope David Akande, Saqib Hakak, and Muhammad Khurram Khan. 2021. 'Ransomware: Recent Advances, Analysis, Challenges and Future Research Directions'. *Computers & Security* 111 (December): 102490. https://doi.org/10.1016/j.cose.2021.102490.

Canales, Katie, and Isabella Jibilian. 2021. 'The US Is Readying Sanctions against Russia over the SolarWinds Cyber Attack. Here's a Simple Explanation of How the Massive Hack Happened and Why It's Such a Big Deal'. Business Insider. 2021. https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12.

Collins, Sean, and Stephen McCombie. 2012. 'Stuxnet: The Emergence of a New Cyber Weapon and Its Implications'. *Journal of Policing, Intelligence and Counter Terrorism* 7 (1): 80–91. https://doi.org/10.1080/18335330.2012.653198.

Egloff, Florian J, and James Shires. 2022. 'Offensive Cyber Capabilities and State Violence: Three Logics of Integration'. *Journal of Global Security Studies* 7 (1): ogab028. https://doi.org/10.1093/jogss/ogab028.

Egloff, Florian J., and Max Smeets. 2023. 'Publicly Attributing Cyber Attacks: A Framework'. *Journal of Strategic Studies* 46 (3): 502–33. https://doi.org/10.1080/01402390.2021.1895117.

Ehrenfeld, Jesse M. 2017. 'WannaCry, Cybersecurity and Health Information Technology: A Time to Act'. *Journal of Medical Systems* 41 (7): 104. https://doi.org/10.1007/s10916-017-0752-1.

Farwell, James P., and Rafal Rohozinski. 2011. 'Stuxnet and the Future of Cyber War'. *Survival* 53 (1): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Fidler, David P. 2011. 'Was Stuxnet an Act of War? Decoding a Cyberattack'. *IEEE Security & Privacy* 9 (04): 56–59. https://doi.org/10.1109/MSP.2011.96.

Ghafur, S., S. Kristensen, K. Honeyford, G. Martin, A. Darzi, and P. Aylin. 2019. 'A Retrospective Impact Analysis of the WannaCry Cyberattack on the NHS'. *Npj Digital Medicine* 2 (1): 1–7. https://doi.org/10.1038/s41746-019-0161-6.

Gray, Colin. 1999. 'Clausewitz Rules, OK? The Future Is the Past – with GPS'. *Review of International Studies* 25:161–82.

Huss. 2017. 'North Korea Bitten by Bitcoin Bug: Financially Motivated Campaigns Reveal New Dimension of the Lazarus Group | Proofpoint US'. Proofpoint. 19 December 2017. https://www.proofpoint.com/us/threat-insight/post/north-korea-bitten-bitcoin-bug-financially-motivated-campaigns-reveal-new.

Jensen, Eric Talbot. 2012. 'Sovereignty and Neutrality in Cyber Conflict'. *Fordham International Law Journal* 35 (3): 815–41.

Jeske, Debora, Andrew Mcneill, Lynne Coventry, and Pamela Briggs. 2017. 'Security Information Sharing via Twitter: "Heartbleed" as a Case Study'. *International Journal of Web Based Communities* 13 (November): ePub. https://doi.org/10.1504/IJWBC.2017.084384.

Junio, Timothy J. 2013. 'How Probable Is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate'. *Journal of Strategic Studies* 36 (1): 125–33. https://doi.org/10.1080/01402390.2012.739561.

Kaspersky. 2023. 'What Is WannaCry Ransomware?' Www.Kaspersky.Com. 6 July 2023. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry.

Lambeth, Benjamin S. 1997. 'The Technology Revolution in Air Warfare'. *Survival* 39 (1): 65–83. https://doi.org/10.1080/00396339708442897.

Larsdotter, Kersti. 2004. 'New Wars, Old Warfare?: Comparing US Tactics in Vietnam and Afghanistan'. In *Rethinking the Nature of War*. Routledge.

Lewis, James A. 2014. 'Heartbleed and the State of Cybersecurity'. *American Foreign Policy Interests* 36 (5): 294–99. https://doi.org/10.1080/10803920.2014.969176.

Lotriont e, Catherine. 2012. 'State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights'. *EMORY INTERNATIONAL LAW REVIEW* 26 (2): 825–919.

Mattei, Tobias. 2017. 'Privacy, Confidentiality, and Security of Health Care Information: Lessons from the Recent WannaCry Cyberattack'. *World Neurosurgery News*. https://www.academia.edu/33783546/Privacy_Confidentiality_and_Security_of_Health_Care_Information_Lessons_from_the_Recent_WannaCry_Cyberattack.

Morse, Amyas. 2017. 'Investigation: WannaCry Cyber Attack and the NHS, National Audit Office'. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf.

Nershi, Karen, and Shelby Grossman. 2023. 'Assessing the Political Motivations Behind Ransomware Attacks'. SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.4507111.

Nye Jr., Joseph Samuel. 2017. 'Deterrence and Dissuasion in Cyberspace'. *International Security* 41 (3): 44–71. https://doi.org/10.1162/ISEC_a_00266.

Rid, Thomas. 2012. 'Cyber War Will Not Take Place'. *Journal of Strategic Studies* 35 (1): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Sassen. 1999. 'The Impact of the Internet on Sovereignty: Real and Unfounded Worries | Nautilus Institute for Security and Sustainability'. 11 December 1999. https://nautilus.org/information-technology-and-tools/the-impact-of-the-internet-on-sovereignty-real-and-unfounded-worries/.

Scaife, Nolen, Patrick Traynor, and Kevin Butler. 2017. 'Making Sense of the Ransomware Mess (and Planning a Sensible Path Forward)'. *IEEE Potentials* 36 (6): 28–31. https://doi.org/10.1109/MPOT.2017.2737201.

Smith, M.L.R. 2003. 'Guerrillas in the Mist: Reassessing Strategy and Low Intensity Warfare'. *Review of International Studies* 29 (01). https://doi.org/10.1017/S0260210503000020.

Soliman, Tamer, David Simon, Rajesh De, Jason Hungerford, Yoshihide Ito, Ori Lev, and Anjani Nadadur. 2021. 'Biden Administration Announces Expansion of Sanctions Against Russia and Signals Potential Additional Restrictions Following SolarWinds Cyber-Attack | Perspectives & Events | Mayer Brown'. 2021. https://www.mayerbrown.com/en/perspectives-events/publications/2021/04/biden-administration-announces-expansion-of-sanctions-against-russia-and-signals-potential-additional-restrictions-following-solarwinds-cyber-attack.

Stone, John. 2013. 'Cyber War Will Take Place!' *Journal of Strategic Studies* 36 (1): 101–8. https://doi.org/10.1080/01402390.2012.730485.

Trautman, Lawrence J., and Peter Ormerod. 2018. 'Wannacry, Ransomware, and the Emerging Threat to Corporations'. SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3238293.

Volz, Dustin. 2017. 'U.S. Blames North Korea for "WannaCry" Cyber Attack'. *Reuters*, 19 December 2017, sec. World. https://www.reuters.com/article/idUSKBN1ED00Q/.

Wilkinson, Philip. 2003. 'The Changing Nature of War: New Wine in Old Bottles – A New Paradigm or Paradigm Shift?' *The Royal Swedish Academy of War Sciences: Proceedings and Journal* 207 (1): 25–35.