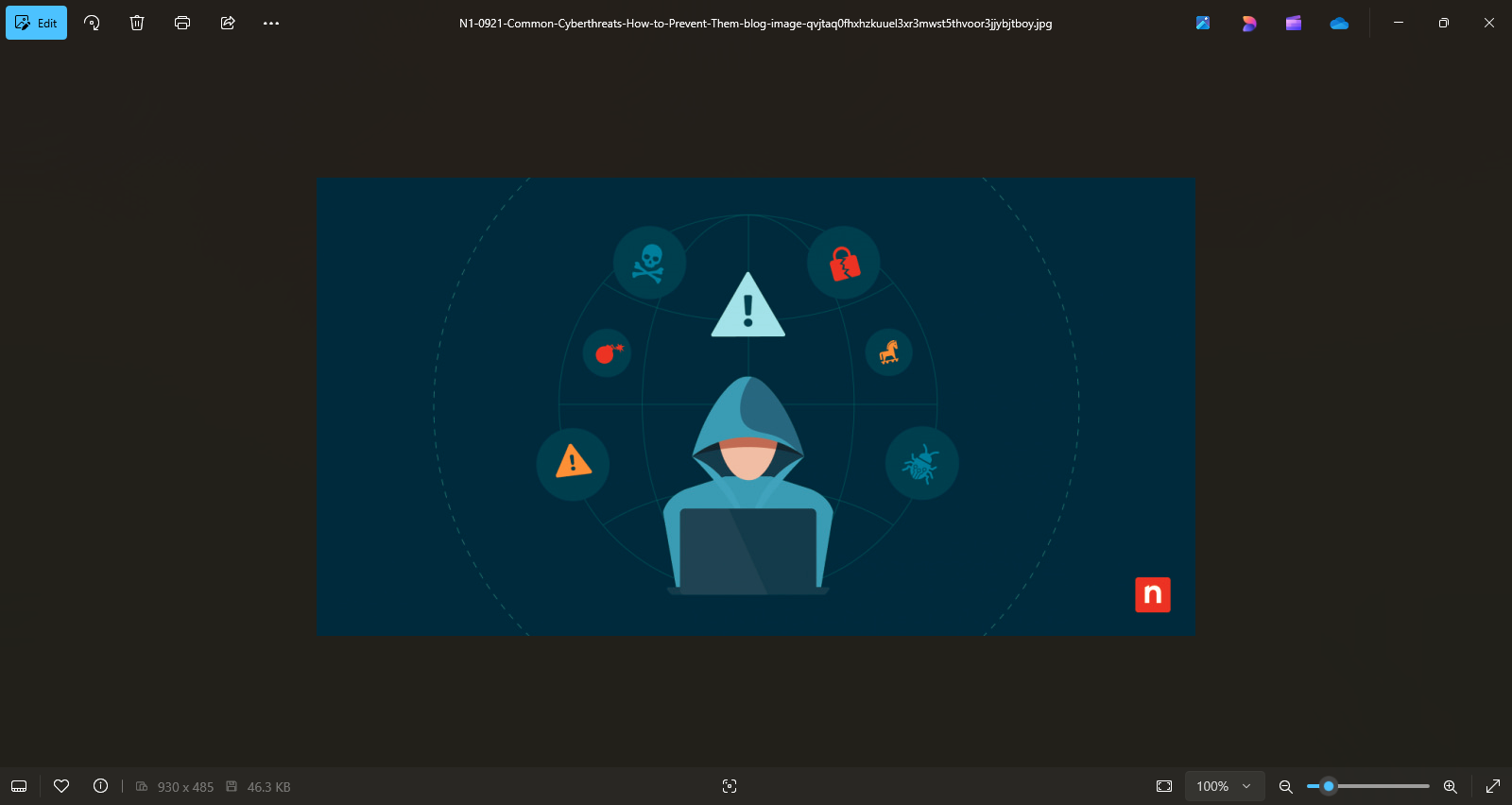
Project Title: **State-sponsored cyberterrorism in global politics**

**Significance/Contribution to the discipline/Research Problem**



(NinjaOne. 2025)

Cyberterrorism in global politics has become a complicated common phenomenon which is gaining momentum. It has become an event of significance which has garnered material investments in research and development, resources and infrastructure. The impact of State-sponsored cyberterrorism in our economy and world of politics creates a topic for discussion as to the pros and cons, as well as consequences to any actions taken around this topic.

T~~he key question is around if research would be required into cyber defense, specifically around state assets and data.~~

**Research Question:** Could state-sponsored cyberterrorism lead to war, and what are the considerations or criteria that should be taken into account when deciding on what motivates such sponsorships?

**Aims and Objectives**



(Identity Management Institute. 2025)

The main objective would be to understand the necessity, criteria and considerations should go into deciding on state sponsored cyberterrorism. The research will delve into why certain states selected in the investigation decide to use cyberterrorism to achieve the disruption or noise they require in respect of politics. Further, the research is likely to provide evidence that specific attacks come from specific countries. Part of the aim will be to find underlying reasons for such attacks and how countries are adapting their laws and strategies in terms of cyberterrorism.

**Key literature related to the project**

There are various online journals and discussion papers on this topic that is coming to the fore. Both these journals and discussion papers will be reviewed and analysed in providing a view on this top and substantiating the criteria, considerations and pros and cons.

Focus will be given on particular countries in order to provide substantive evidence to support the research question. There will be a critical evaluation to provide an understanding of the current state of knowledge on the topic/research question, identifying possible gaps and highlighting areas for future research.

**Literature Review:**



(Statista. 2025)

The last two decades have seen cyber incidents become more expensive, more intrusive, more disruptive, and most definitely more political. My research into this topic has been to understand the various factors that have contributed to the inclusion of cyberterrorism in political warfare.

A unique dataset was used by Hunter, Lance et al. 2021, in their journal ’‘ Factors that motivate state-sponsored cyber-attack”, which mentions that wars will be fought in the future via mouse clicks rather than via physical invading forces and bombs dropping (Hunter, 2021). The impact cyberterrorism has on state-politics can be seen from a response the US Senator John McCain made, when he called the Russians meddling in the US 2016 elections an act of war (Hunter, 2021). War in political rhetoric is a power play and is often used to exaggerate the media and create a war of words (Lotrionte, 2018). War definitions legally grant varying powers to politicians and in terms of Cyber war or cyber terrorism there are fewer definitions of what prescribes substance for retaliation and which international laws that can be used to defend the relevant actions (Lotrionte, 2018).

The United Nations Charter and the law of armed conflict do not have sections which one can say are directly attributable (Lotrionte, 2018).

From the article, Cyber Terrorism to State Actors’ Covert Cyber Operations by Kallberg and Thuraisingham, is discussed showing how covert state actors are likely to use criminal organisations to act as proxies to execute covert cyber terrorisms acts. This appears to have become a more regular occurrence than previously and is being used for various purposes. Hackers have moved from being viewed as small scale obstacles to well organised and extremely well paid jobs because of state funded cyber-attacks (Kallberg and Thuraisingham 2013). An interesting interpretation of this is that the US considers an attack on its industries, military networks, and infrastructure as an attack on the state itself (Kallberg and Thuraisingham 2013). Morals and ethics seem to take a sidestep, as covert operations sponsored by the state result in payment to criminal networks in a variety of ways such as drugs, weapons, or any currency (Kallberg and Thuraisingham 2013). The lack of the ability to point blame at any one party or person directly removes the capacity for retribution, noting that the computers and networks used during the attack are removed or never used again (Kallberg and Thuraisingham 2013).

Some political power plays were attributed to cyberattacks as in 2019 when allegedly the US attacked Venezuela's power systems causing widespread panic, looting and deaths as they wanted revenge against the then President Maduro for insulting the US and they wanted him out. Brazil had a similar story, but it was denied by the government ( Libicki, 2020). The only verified cyber-attack on a power grid happened in Ukraine in 2015 and 2016 (Libicki, 2020). Due to the threat of malware disrupting the nuclear weapon control systems in Russian, they moved some of their nuclear weapons to Cuba (Libicki, 2020). What is interesting is that Ukraine power grid has been under attack since 2016 for sharing electricity with the Crimea region and since this did not work as a deterrent, Russia and Ukraine are now at war (Libicki, 2020). We can infer from this incident that cyberattacks could become a precursor to forcible attacks. The journal Cyberterrorism, Postmodern state of Chaos introduces the concept of cascading failures through cyberterrorism causing chaos (Matusitz, 2008) This article is slightly dated as in 2008 the concern seems to be focused on physical destruction such as breaching power grids, or creating compromising situations but in the more recent articles the concern is still around physical attacks with the included threat of information / data breaches and losses.

Back in the 1990’s Russia considered information as a weapon and declared a threat of nuclear strike against any nation that would attack their information systems (Thomas, 2020). They further break down information into information-technical and information-psychological (Thomas, 2020), which gives some insight into the way the Russian government thinks and manages it information. This breakdown of information as weapons allows Russia to destroy, distort, mine or obtain information after penetrating defense systems / firewalls (Thomas, 2020). The patriot act of the US allows them to request personal information for investigative purposes (Dept of Justice. N.D). It is possible that other countries are doing the same under legal protection such as state terrorism acts of some sort.



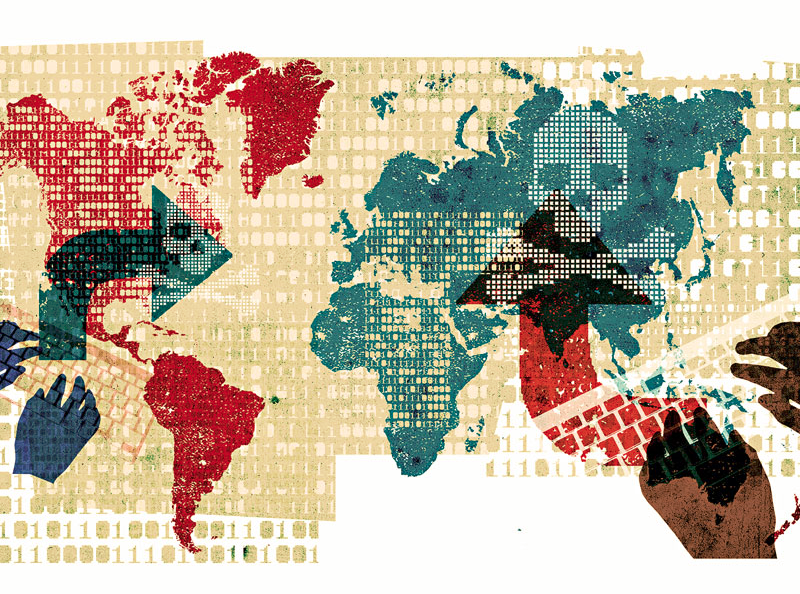
(Wikipedia contributors. 2025)

Currently Russia is systematically attacking Ukraine's energy sector, banking systems and other objects critical to the economy to look for areas of weaknesses to use against them (Kormych and Zavhorodnia, 2023). In retaliation, a rapid response program for cyber-attacks was announced at the Madrid NATO summit (Kormych and Zavhorodnia, 2023).

In a similar manner, the US joint chiefs of staff use the term information warfare to describe the growing threats of cyberterrorism, electromagnetic and informational activities that could be used to destabilize the US and its (Fogarty et al., 2020). It currently has an army cyber command set up to defend its systems known as ARCYBER. ARCCYBER is the foundation for the Department of Defenses (DoD) information network who to successfully defend the network, data and interconnected weapons platforms from attacks as a prerequisite for a successful Army and Joint operations (Fogarty et al., 2020). The Marine corps have followed suit and have an information warfighting function (Paul, 2020). The DoD produced the first Strategy for operations in information environment in 2016 (Paul, 2020). The paper by Paul, C. 2020, “Understanding and Pursuing Information Advantage”, looks for the definition of information advantage and reviews in depth at this concept.

Cyber terrorism is a strategic low risk for state sponsors, as it collects vulnerabilities from its opposition, builds its cyber weapons, creates disruption but uses a proxy to do the actual attack (Kallberg and Thuraisingham 2013). A political cyber-attack can provoke international conflict, but consideration should be considered for the difficulty of determining the source and probability of an incorrect assessment of the situation (Kormych and Zavhorodnia, 2023).

**Countering Threats**

****

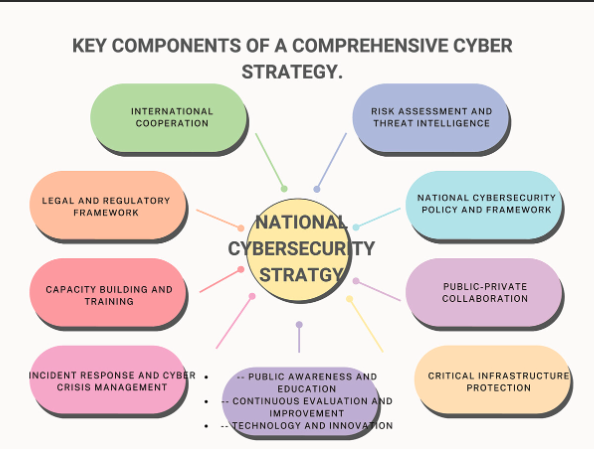
(Science Photo Library. 2025)

The journal on Cyber threat characterization speaks to threat modeling, by Jabbour, Kamal T., and Erich Devendorf 2017, which might be considered slightly outdated as at the time AI and machine learning were not included in many threat models. Countering cyberterrorism journal by Henry, Shawn, and Aaron F. Brantly (2018) shows that the sharing of information in a co-operative Government and public sector worked better after the 9/11 attacks and legislative changes due to the attacks. This might be a guideline that the international law and co-operation between allies need to follow. Digital and cyber diplomacy is an abstract that is discussed in the article by Y. Maulana and I. Fajar, on Analysis of Cyber diplomacy and its Challenges for the Digital era community. It also mentions that cyber diplomacy is a requirement to help prevent open cyber war (Maulana and Fajar, 2023).

The “Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security” known as the UN GGE is where the international community discussion cyber terrorism (Broeders et al., 2021). This is run by the US and its allies (Broeders et al., 2021). A parallel group established by Russia, China and their allies known as the UN Open-Ended Working Group (OEWG) for cyberspace with the same agenda (Broeders et al., 2021). Broeder’s article looks at the development of international cyber legislation. The US strategy on cyber terrorism looks at it from an international co-operation, the over confidence in their software power, whilst the UK admits that their current technical abilities are low (Broeders et al., 2021). The French have taken the same stance as the UK in that even if the cyber-attack is a low risk event, the publicity gain from such an attack may cause more damage than expected in terms of reputation and exposing vulnerabilities. They therefore base their response on the public’s response to the cyber-attack (Broeders et al., 2021).

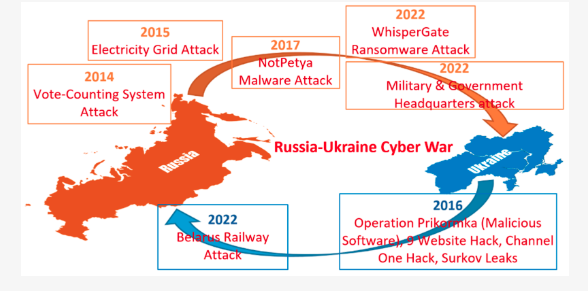
The Chinese as per their Cyber security law, integrate into the Chinese party state to fully regulate and surveil its cyberspace (Broeders et al., 2021). Since cyberspace has no boundaries, it means that Chinese law allows them to therefore surveil the internet. Russia has gone one step further in efforts to protect itself in that they require all internet service providers to utilise software to allow them to block and access content (Broeders et al., 2021). China also operates one of the most sophisticated systems of online censorship to safeguard its citizens against cyber terrorism. Islamic state threat actors’ online activities have not scared nations into consensus on international law on cyber terrorism (P,2016).

**Conclusion**

****

(Chitando, Mafumbate. & Chari. 2024)

Most literature on the topic seems to be published from countries who are engaged with nuclear weapons, and their thoughts around the protection of these should a cyberterrorist act occur. Further investigation needs to be put into place for NATO countries that do not have nuclear weapons, as they are not necessarily excluded from attacks, and very little literature about their cyber view. Further this may be an angle hackers could use to infiltrate joint command centers to obtain confidential information. If army command centers use standard operating software, then they are vulnerable to the same malware exploits as corporations which in this day and age would be disastrous. The secondary, but just as devastating consequence would be an attack on all major corporations that deal with the majority of the IT sector. If a combined state-sponsored attack on all these companies took place at once bringing down digital financial systems for a few days, this would have catastrophic effects on global markets.



(Sufi, F. 2023)

There seems to be a lot of journal literature available on the subject which is interesting, and certain views can be made such as the Ukraine cyber-attack being a prelude to a war. So, there is no doubt that cyberterrorists are an act of war. Various literature seems to discuss and argue the behaviour of intelligence agencies when it comes to cyberterrorism, and other literature speaks to the knowledge of IT Security companies and their risk assessment and mitigation tactics in providing a solution to the world.

Based on the information available there seems to be a lot of loopholes available for hackers to hide behind and international law is still catching up with the rate of technological advancement. Despite the situations which have arisen over many years and the devastating impact of the attacks certain countries have had to experience, the law has not yet catered for a manner in which to deal with the perpetrators. For example, the US patriot act has only recently added to their wiretap options to include new technologies and new threats (Depart of Justice N.D).

In 2021 NATO’s comprehensive cyber defense policy was approved with the aim of achieving a peaceful and secure cyberspace (Kormych and Zavhorodnia, 2023).

All the journals have been research-based papers however with none having qualitative data to support evidence of cyber terrorism attacks. This could easily be explained, due to the sensitivity and secrecy of the data sets that would allow research of such attacks, also the sheer volume of attacks that occur daily and determining state-sponsored attacks for specific reasons would be difficult to prove and would be conjecture.

Technological advancements over the centuries have changed warfare from the development of gunpower, through the industrial revolutions and the information revolution that has increased the growth of cyberspace (Ball and Gary, 2013).

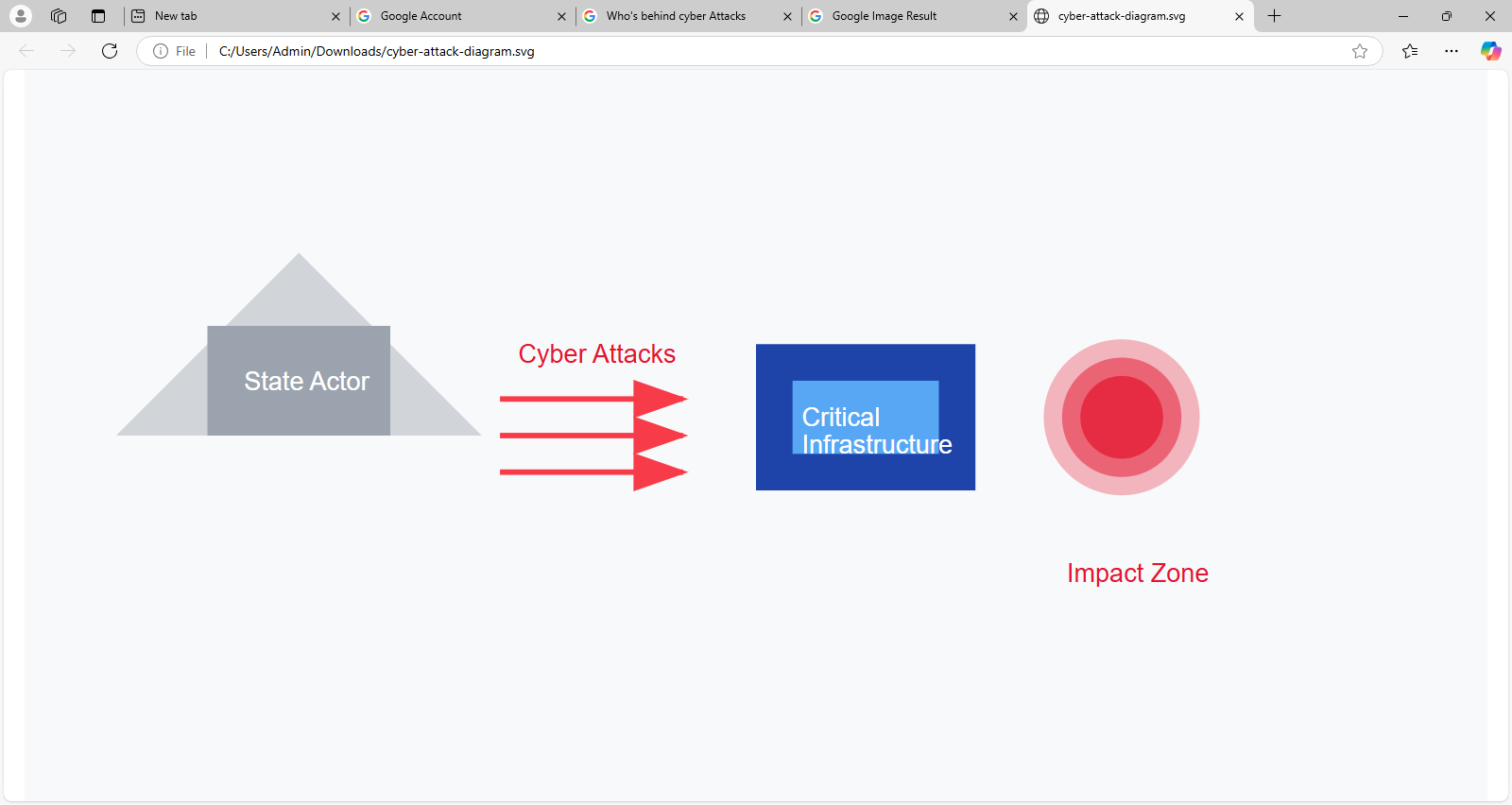
The further reality is that societies in many parts of the world rely on uninterrupted supply of digital technology for the delivery of many services. Some of those services run into the political arena like elections, which means that the prominence of these events requires more answers and interventions to counter these threats adequately.



(The Time. 2025)

A quote from Kormych and Zavhorodnia sums it up nicely that “The political elite uses the results of the confrontation as a platform for legitimizing personal decisions and realizing goals at the geopolitical level. “

**Methodology/Development strategy/Research Design**



**The research methodology will look at reviewing and analysing existing information and articles in terms of State-sponsored cyberterrorism in global politics. The data will most likely be qualitative versus quantitative due to the research question under consideration. Most information on this topic is of a qualitative nature, and therefore the selection of either certain authors or countries as noted above will be refined in order to provide an argumentative viewpoint on the research topic. A possible challenge will be finding articles which are factual versus opinionated to provide proper evidence in this thesis. I will ultimately look to explain whether the research provides conclusive evidence to support the my objective of the research question.**

**Ethical considerations and risk assessment (as part of your ethical approval application)**

**In preparation of this thesis, areas focused on from an ethical standpoint will include informed consent if applicable, confidentiality, anonymity, respect, beneficence and no-maleficence and justice. The thesis provided will be Plagiarism free.**

**Description of artefact(s) that will be created (if applicable)**

**It is unlikely that artefacts will be created as research will be based on analysis of existing data instead of a set up of new investigative data.**

**Timeline of proposed activities**

**This research and thesis will be conducted over a 6 month period based on the timelines provided for this submission.**

**References:**

Ball, Desmond, and Gary Waters.(2013) “Cyber Defence and Warfare.” *Security Challenges*, vol. 9, no. 2, 2013, pp. 91–98. *JSTOR*, http://www.jstor.org/stable/26462919. Accessed 10 Nov. 2024.

Broeders, D., Cristiano, F. and Weggemans, D. (2021) ‘Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy’, *Studies in Conflict & Terrorism*, 46(12), pp. 2426–2453. doi: 10.1080/1057610X.2021.1928887.

Dept of Justice (no date) *The USA PATRIOT Act: Preserving Life and liberty*, *The USA PATRIOT Act: Preserving Life and Liberty*. Available at: https://www.justice.gov/archive/ll/what\_is\_the\_patriot\_act.pdf (Accessed: 09 November 2024).

Fogarty, Stephen G., and Bryan N. Sparling (2020) “Enabling the Army in an Era of Information Warfare.” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 17–28. *JSTOR*, https://www.jstor.org/stable/26923519. Accessed 9 Nov. 2024.Hunter, Lance Y., et al.(2021) “Factors That Motivate State-Sponsored Cyberattacks.” *The Cyber Defense Review*, vol. 6, no. 2, 2021, pp. 111–28. *JSTOR*, https://www.jstor.org/stable/27021379. Accessed 5 Nov. 2024.

Fogarty, Stephen G., and Bryan N. Sparling (2020) “Enabling the Army in an Era of Information Warfare.” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 17–28. *JSTOR*, https://www.jstor.org/stable/26923519. Accessed 9 Nov. 2024.

Lotrionte, Catherine. (2018) “Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law.” *The Cyber Defense Review*, vol. 3, no. 2, 2018, pp. 73–114. *JSTOR*, http://www.jstor.org/stable/26491225. Accessed 9 Nov. 2024.

Jabbour, Kamal T., and Erich Devendorf.(2017) “Cyber Threat Characterization.” *The Cyber Defense Review*, vol. 2, no. 3, 2017, pp. 79–94. *JSTOR*, http://www.jstor.org/stable/26267387. Accessed 10 Nov. 2024.

Kallberg, J. and Thuraisingham, B., (2013). Chapter 19 - From Cyber Terrorism to State Actors’ Covert Cyber Operations [online]. *https://doi.org/10.1016/B978-0-12-407191-9.00019-3*. [Viewed 3 December 2024]. Available from: <https://www.sciencedirect.com/science/article/abs/pii/B9780124071919000193>

Kormych, L. and Zavhorodnia, Y., (2023). The concept of modern political confrontation in cyber space. *Journal of Cybersecurity* [online]. **9**(1). [Viewed 8 December 2024]. Available from: doi: 10.1093/cybsec/tyad017

Libicki, Martin. (2020) “Cyberwar Is What States Make of It.” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 77–88. *JSTOR*, https://www.jstor.org/stable/26923524. Accessed 9 Nov. 2024.

Matusitz, J.(2008) cyberterrorism: Postmodern State of Chaos, Information Security Journal: A Global Perspective, 17:4, 179-187, https://doi.org/10.1080/19393550802397033. Accessed on 3 Dec. 2024.

Maulana, Y. I. and Fajar, I. (2023) “Analysis of Cyber Diplomacy and its Challenges for the Digital Era Community”, *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, 4(2), pp. 169–177. doi: 10.34306/itsdi.v4i2.587.

P, F. D., (2016). Cyberspace, Terrorism and International Law [online]. *OUP Academic*. [Viewed 7 December 2024]. Available from: <https://academic.oup.com/jcsl/article-abstract/21/3/475/2525373>

Paul, Christopher.(2020) “Understanding and Pursuing Information Advantage.” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 109–24. *JSTOR*, https://www.jstor.org/stable/26923526. Accessed 10 Nov. 2024.

Thomas, Timothy L. (2020) “Information Weapons: Russia’s Nonnuclear Strategic Weapons of Choice.” *The Cyber Defense Review*, vol. 5, no. 2, 2020, pp. 125–44. *JSTOR*, https://www.jstor.org/stable/26923527. Accessed 9 Nov. 2024.

Sufi, F. (2023). Social Media Analytics on Russia–Ukraine Cyber War with Natural Language Processing: Perspectives and Challenges. *Information*, *14*(9), 485. https://doi.org/10.3390/info14090485

The Times. (2025). America's enemies denied their liberty at the United Nations. [Online] Available at: https://www.thetimes.com/article/americas-enemies-denied-their-liberty-at-the-united-nations-63n3w9fpb?region=global [Accessed 11 January 2025].

Identity Management Institute. (2025). State-Sponsored Cyber Warfare. [Online] Available at: https://identitymanagementinstitute.org/state-sponsored-cyber-warfare/ [Accessed 11 January 2025].

NinjaOne. (2025). Häufigste Arten von Cyber-Attacken. [Online] Available at: https://www.ninjaone.com/de/blog/haeufigste-arten-von-cyber-attacken/ [Accessed 11 January 2025].

Wikipedia contributors. (2025). 2022 Madrid summit. Wikipedia, The Free Encyclopedia. [Online] Available at: https://en.wikipedia.org/wiki/2022\_Madrid\_summit [Accessed 11 January 2025].

Statista. (2025). Countries responsible for the largest share of cyber incidents. [Online] Available at: https://www.statista.com/chart/31805/countries-responsible-for-the-largest-share-of-cyber-incidents/ [Accessed 11 January 2025].

Science Photo Library. (2025). Computer hackers and global cyber attack, illustration. [Online] Available at: https://www.sciencephoto.com/media/939636/view/computer-hackers-and-global-cyber-attack-illustration [Accessed 11 January 2025].

Chitando, E., Mafumbate, P. & Chari, T., 2024. Lamentations of political violence: Joshua Mqabuko Nkomo and the Gukurahundi conflict. *Journal of Southern African Studies*, 50(1), pp.1-17. Available at: https://doi.org/10.1080/23742917.2024.2312671 [Accessed 11 January 2025].