IE University IE International Policy Review (IPR)
Journal **7 Issue 1** (2026)
https://ipr.blogs.ie.edu/

The Rise of Cyber Threats: Their Impact, Their Mitigation

Josephine Felappi

Sciences Po Paris, Reims, France.
Political Science.

E-mail: josephine.felappi@sciencespo.fr

Published January 2026

Editor: Uma Terpend, IE University

Abstract

The advent of artificial intelligence and technology in general has catalysed a paradigm shift in the way we approach militarism and military security on land. Our increased dependence on technology places it amongst our greatest vulnerabilities and makes the development of cybersecurity policies paramount to prevent potentially disastrous situations. This paper analyses how cyberspace has transformed warfare and security on land, bringing to light the fact that, at an international level, frameworks should be put in place to regulate cyber warfare. At a national level, this paper shows that it is necessary for states to set a uniform protocol for the response to cyber threats and invest in research and expertise on cybersecurity to maximise effective prevention of such threats.

Keywords: cybersecurity, security on land, cyber warfare, Russia, Ukraine, U.S., Colonial Pipelines, IT

1. Introduction

The advent of artificial intelligence (AI) and technology in general has catalysed a paradigm shift in the way we approach militarism and military security. On 28 April 2025, Spain, Portugal, and a part of France experienced a complete power outage, considered "the most severe blackout incident on the European power system in over 20 years, and the first ever of its kind."[1] While the hypothesis of the blackout's cause being rooted in a cyberattack was dismissed by the Spanish environmental minister, Sara Aagesen, the consequences have alarming implications for the potential magnitude of a malignant attack on electrical grids. ATMs were left unable to release cash; bus lines shut down; traffic lights went dark; malfunctioning phone networks impeded communication. This power outage was not simply an unprecedented event; it was a wake up call, showing how dependent our societies have become on technological tools and networks and how vulnerable states can be if struck at the heart of that system. Some military bodies have already conceived this and are using it to their advantage. For example, Russia's Sandworm hacker group, which belongs to Russia's

[1] '28 April 2025 Blackout', accessed 16 November 2025, https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.

military intelligence agency, the Main Directorate of the General Staff, caused power outages targeting power plants in Ukraine in 2015, and multiple times since.[2] The prevalence of technology on an international level and the extent to which it is interconnected with societies on all levels make such warfare a crucial element for nations to consider in regards to security on land. As such, this paper will attempt to answer the following question: How effective are cybersecurity measures in the mitigation of threats arising from the changing field of land-based militarism through new technological warfare?

2. Background

The Cyber Era began in the 1980s, with the diffusion of the internet, and the global connection of individuals made possible through the World Wide Web. The concept of cyber warfare was coined in a 1993 article published by the RAND Corporation, an American think tank. The article defines it as "a series of attacks and defensive actions against the enemy's network information system, aiming at disrupting and destroying its network information system to ensure the normal operation of its own network information system."[3] 21 October 2002 saw the first large-scale Distributed Denial of Service (DDoS) attack, which is "a cyber-attack that aims to make a computer system or network unavailable by flooding the target with useless and redundant request inputs in order to overload and saturate it."[4] A month later, in November, the Prague Summit took place, where North Atlantic Treaty Organisation (NATO) member states issued a statement announcing their commitment to the protection against cyber threats.[5] Despite this, cyberattacks became more frequent and more consequential. Estonia experienced the world's "first recognized case of cyber aggression between state actors" in 2007, perpetrated by the Russian government over the relocation of the Soviet-era Bronze Soldier of Tallinn war memorial.[6] Several crucial Estonian information networks went down due to this attack, showing the risks and gravity of the threat. The 2008 Bucharest Summit then saw the development of NATO's cyber defence strategy, which was defined to include two pillars: shared responsibility and requested assistance. Several summits followed, further expanding and building on the alliance's cybersecurity policy, culminating in the 2014 Wales Summit, which introduced the Enhanced Cyber Defence Policy. This recognised that international norms applied to cyberspace, a turning point in cyber warfare and security, and was further strengthened in the 2016 Warsaw and 2018 Brussels Summits, which expanded the definition of hybrid warfare to include disinformation campaigns and malevolent cyber activity.[7]

While these declarations and the codification of cyber

[2] Carlo Disma, *The Evolving Cyber Warfare Landscape*, The Alliance Five Years after Crimea: (NATO Defense College, 2019), 79, https://www.jstor.org/stable/resrep23664.12.
[3] He Xiaotong, 'The Impact of Russia-Ukraine Cyberwarfare on the Application of the Right to Self-Defense in Cyberspace and Implications', *US-China Law Review* 20, no. 3 (2023), 115 https://doi.org/10.17265/1548-6605/2023.03.003.
[4] Disma, 72
[5] 'Prague Summit Declaration', NATO.Int, accessed 16 November 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/21/prague-summit-declaration.
[6] Disma, 72
[7] Disma, 74

warfare within international law represented a large leap forward in the domain, cyber wars still "offer varying degrees of covertness and their treatment under international law remains ambiguous".[8] As time passes, concern continues to grow as the technologies employed for these attacks gain in sophistication and frequency. The most common uses of cyber warfare in war on land are "semantic attacks", which target infrastructures or information technology (IT) through the unnoticeable modification of data, as well as cyber espionage.[9] Moreover, the rise of Artificial Intelligence (AI) exacerbates the issue. AI can predict the supply-chain processes for multidomain task forces and provide strategic and tactical advice.[10] The rapid progress of cyber warfare and the potential that AI offers for this form of war-making increase the urgency for states to implement robust cybersecurity policies to protect their territory.

3. Analysis

3.1 Russia and Ukraine

As mentioned above, the first large-scale cyberattacks were carried out by Russia. This tactic was soon integrated into Russian warfare, as evidenced by the war in Ukraine. In fact, while offensive cyber operations against Ukraine began in 2014, they are still present to this day. During the first 11 months of the war, over 2,194 cyberattacks were reported as perpetrated by Russia.[11] The importance of cyber warfare in the conflict is greatly debated, with some academics claiming that Russia is underutilising its power—a full-scale cyber assault on Ukraine could shut down its power grid, disable heating systems, and disrupt all military command centres and cellular communications systems[12]—and others claiming that cyber warfare has become one of the main strategic tools in the war.[13] Regardless of which account is perceived as most convincing, it is impossible to deny the use of cyber warfare in the conflict, thus making it a reliable case study for the successes and failures of security for cyber threats.

A large part of Russian operations has been in search of information, gathering intelligence, stealing technology, and driving public narratives and diplomatic debates.[14] This has been conducted from both sides, with the independent Ukrainian Cyber Alliance targeting Russian websites to leak sensitive data–including emails belonging to one of President Putin's top advisors, providing evidence of previously denied attempts to destabilise Ukraine.[15] This is not the only objective, however, as some cyberattacks also aim to target physical infrastructure. On the first day of the invasion, tens of thousands of satellite modems in Ukraine and other parts of Europe suffered

[8] Cholpon Abdyraeva, *Cyber Warfare*, The Use of Cyberspace in the Context of Hybrid Warfare. (OIIP - Austrian Institute for International Affairs, 2020), 16, https://www.jstor.org/stable/resrep25102.7.

[9] Abdyraeva, 19

[10] Atin Basuchoudhary, 'AI and Warfare: A Rational Choice Approach', *Eastern Economic Journal* 51, no. 1 (2025): 76, https://doi.org/10.1057/s41302-024-00280-7.

[11] Emily Stubblefield, 'HACKTIVISTS AS COMBATANTS: WHAT UKRAINE'S COUNTEROFFENSIVE TO RUSSIA'S CYBERWARFARE MEANS FOR CIVILIAN HACKERS' STATUS UNDER THE LAWS OF WAR', The Fordham urban law journal, October 2024, 218.

[12] Herbert Lin, 'Russian Cyber Operations in the Invasion of Ukraine', *The Cyber Defense Review* 7, no. 4 (2022): 31.

[13] Xiaotong, 113

[14] Lin, 32

[15] Stubblefield, 222

cyberattacks, resulting in widespread loss of internet access within the area affected. Internet services were also temporarily disrupted on 9 March, 13 March, and 28 March due to attacks on telecommunications providers Triolan, Vinasterisk, and Ukrtelecom. In addition, the attack caused permanent damage to the modems by destroying key data contained within, rendering them indefinitely inoperable.[16] While these attacks have a relatively narrow target—internet provision—the Iberian blackout clearly showed the potential scale of such infrastructural deficiencies, highlighting the menace of such tactics. Moreover, Ukrainian systems, including government, financial, information technology, and energy sectors, suffered the presence of Russian wiper malware programmes which erase user data, programmes, and hard drives.

Despite these various measures, it also appears that many attacks were rendered unsuccessful or had reduced consequences due to effective measures of cybersecurity. In March, Starlink terminals deployed by SpaceX to improve its satellite communications capability were the targets of cyberattacks which succeeded for several hours, until the company updated the software to resist such attacks.[17] The rapid reaction and adaptability of the cybersecurity plan in place was key to its mitigation of the damages arising from the attack. Moreover, many disinformation campaigns have been launched in Ukraine, including fake social media behaviour, brief takeovers of media channels, and the compromise of social media accounts. Despite the volume of these attacks, the Security Service of Ukraine announced on 28 March that it had shut down five disinformation-spreading bot farms responsible for over 100,000 social media accounts.[18] It is crucial for government services to be aware of the cyber threats they are facing and proactively seek them out to undermine them.

In the case of the Russia-Ukrainian war, there have also been attempts at prevention against cyberattacks, not only acts of reparation. In fact, the United States (U.S.), the European Union (EU), and NATO member states have provided cybersecurity assistance to Ukraine. The U.S. Agency for International Development announced its $38 million investment in Ukrainian cybersecurity in 2020 over a four-year period. The U.S. has additionally aided in the fostering of various public-private partnerships between Ukraine and Western IT companies like Microsoft or Google. These companies managed to identify and block Russian cyber threats in near real-time.[19]

A further development of Russian cyberattacks against Ukraine has been the proliferation of offensive cyber operations by Ukraine against Russian hackers to disrupt cyberattacks against Ukraine.[20] After Russia's invasion of Ukraine, the Vice Prime Minister, Mykhailo Fedorov, issued a call for hackers all over the world to defend Ukraine's vital infrastructure and target Russian infrastructure, which initially included a list of 31 Russian

[16] Lin, 32
[17] Lin, 33
[18] Lin, 33
[19] Lin, 36
[20] Lin, 36

government, bank, and corporation websites. Over 400,000 volunteers responded in a matter of days, creating an international hacktivist movement known as the Ukrainian IT Army.[21] Once again, the effective response and protection of Ukrainian cybersecurity rested on officials' understanding and knowledge of IT and its potential dangers. The IT army has been successful in shutting down the Moscow Stock Exchange and the largest Russian bank, Sberbank, causing electrical outages in the Leningrad region, and attacking the servers of the Gazprombank bank, a state-owned energy company. In mid-2022, the IT army had leaked over two terabytes of data from crucial governmental institutions and other organisations.[22] It is important to note that the status of the Ukrainian IT members is ambiguous under international law. According to the Red Cross Standard of Direct Participation or the U.S.' definition of direct participation, they are not direct participants in hostilities.[23] Not being combatants, they are not legitimate military targets under the conventions of just war, which allows them to act beyond the constraints that the state itself faces.

In fact, cyber warfare does not require an open declaration of war, which is why it is greatly employed in the period leading up to open conflict. The strength of cyber warfare lies in its discretion and anonymity.[24] This greatly explains the apparent inability of Ukrainian cybersecurity to thwart information-gathering attacks by Russia, as identifying the perpetrator is difficult, if not impossible.

3.2 US Colonial Pipeline Attack

Cyberattacks do not always originate from states and do not always occur in times of war. On 7 May 2021, a ransomware attack shut down 5,500 miles of petroleum pipeline on the East Coast of the United States.[25] The attack on the pipeline, owned by the company Colonial Pipeline, caused widespread chaos, with Americans along the coast queueing at gas stations and even filling bags with fuel.[26] The attack actually began on 6 May, when Colonial Pipeline networks were breached, allowing the theft of 100 GB of information. The Russian-based ransomware group, DarkSide, demanded a ransom in order to provide the necessary decryption tool—called "Jacobs"—to restore access to the IT systems. The group requested a ransom of approximately $4.4 million in Bitcoin, which was paid in just a few hours by Colonial Pipelines, in close collaboration with the Federal Bureau of Investigation (FBI).[27] The shutdown lasted a total of five days, resulting in about $1 billion worth of impact to the company,

[21] Stubblefield, 224
[22] Stubblefield, 226
[23] Stubblefield, 232
[24] Xiaotong, 115

[25] U.S. GOVERNMENT PUBLISHING OFFICE, *CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK*, 15 June 2021, 9.
[26] CISA, 'The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA', 7 May 2023, https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.
[27] Christopher Whyte, 'Searching for Cyberspace: The Colonial Pipeline Ransomware Attack through the Lens of Search Engines', *Journal of Information Technology & Politics* 0, no. 0 (n.d.): 6, https://doi.org/10.1080/19331681.2024.2422908.

making it the "single largest assault on American critical infrastructure in history in terms of financial damage and number of people directly affected".[2829] Once again, a parallel can be drawn between such a shutdown and the April blackouts in Spain and Portugal, where the vulnerability of states in regards to their infrastructure's dependence on cyberspace becomes apparent.

An interview with Frank Abagnale, an ex-hacker who now works in close collaboration with the FBI, sheds some light on the attack and the reasons behind its success.[30] He states that companies are easy targets as they often choose not to adopt the proper technology that is available to protect them against cyber threats. Companies tend to believe that the attack will not happen to them, he explains, and that it is not worth spending the money on a proper cybersecurity system, despite the existence of technology that would effectively thwart such attacks. DarkSide stole Colonial Pipeline's passwords in the attack, enabling access to the system. Although the technology exists that would allow companies to stop using passwords, the reliance on somewhat outdated technologies and a lack of awareness of the necessity to progress were chief reasons leading to the ransomware attack's success, according to Abagnale. Moreover, the impact of the attack was so vast due to the inflexibility of the American oil industry's supply chain, which had no backup plan once one branch was rendered temporarily inoperable.[31] In fact, while the main pipeline was shut down, only a few subsidiary branches remained online. Furthermore, the hackers knew to target the vulnerabilities of the American system. In fact, a significant weakness in the U.S. is the lack of monitoring and detection within critical infrastructure systems, which would have been able to detect disruption.[32]

Beyond the able exploitation of vulnerabilities by the DarkSide group, a large part of the success of the attack was due to failures on the part of American cybersecurity. In the aftermath of the attack, the U.S. Government recognised that, for the benefit of national security, a partnership between the private sector and the federal government was necessary.[33] In fact, while the U.S. Government has invested in cybersecurity, cyber warfare is transforming the nature of militarism, targeting private actors in order to impact the public. As such, the security of private companies is just as crucial to the federal government as the cybersecurity of the nation as a whole. Furthermore, a great gap in the application of cybersecurity in this affair was the disproportionate focus on reparation, rather than prevention. After the attack, the FBI and other federal partners immediately began to gather information to potentially aid other victims of such

[28] EBSCO, 'Two Years After the Colonial Pipeline Attack.', accessed 17 November 2025, https://research-ebsco-com.scpo.idm.oclc.org/c/5v7is5/viewer/html/5sbqz3bnhj?route=details.
[29] Whyte, 6
[30] Jane Wollman Rusoff, *Legendary Ex-Fraudster Says Colonial Pipeline Attack Could Have Been Avoided*, (New York, United States), ALM Media Properties, LLC, 2021, https://www.proquest.com/docview/2541268283/abstract/35DC6E329E8549BDPQ/1.
[31] Whyte, 7
[32] EBSCO, 'Two Years After the Colonial Pipeline Attack.'
[33] U.S. GOVERNMENT PUBLISHING OFFICE, 10

campaigns.[34] The Cybersecurity and Infrastructure Security Agency (CISA) has created stopransomware.gov as a result of the attack to provide a centralised area to gather alerts and guidance.[35] Moreover, the federal government has recovered approximately 75% of the money paid as ransom for Colonial Pipeline.[36] While it *is* important to ensure reparation for victims of such attacks, it is an even more important cybersecurity strategy to address them at their root and eliminate them before they can involve any victims.

4. Policy Recommendations

The two case studies, spanning various types of cyber threats and cybersecurity responses, offer critical insight into what states can implement and improve in terms of cybersecurity policies.

The case of the Russia–Ukraine war highlights the limits and risks of cyber threats when employed within the context of ongoing conflict between states. The main takeaway seems to be that an international agreement on the definition of cyber warfare, and on its recognition of its status within the framework of traditional warfare, is long overdue. No meaningful regulations can be put in place without it, which creates the grey space of uncertainty in which cyberattacks may be conducted without an open declaration of war, greatly restraining possible cybersecurity responses. A shared definition would also ensure a more even implementation of regulation on cybercrimes, enhancing international security. This is also apparent in the case of the attack on Colonial Pipeline, which saw the Russian government exercising greater leniency on the DarkSide group than the U.S. state would have liked. An internationally ratified resolution or treaty on the matter would avoid this misalignment.

Additionally, the case of the Colonial Pipeline attack presents a different facet of the issue. It shows how states must remain permanently vigilant regarding their cybersecurity, not only during times of tensions or conflict. The case further highlights that a clear definition of cybersecurity procedures must be promulgated at the national level. The interview with Abagnale reveals that ransomware attack groups are searching for an easy success rather than a challenge. Thus, the immediate concession of the company and the FBI in paying the ransom may have inadvertently encouraged attacks of the same nature.[37] As such, it is necessary for the state to set a definite reaction, perhaps by categorising cyber threats as terrorism, which would prohibit the payment of the ransom in a uniform manner and act as a preventative measure to discourage further attacks.

The various successes of Ukrainian cybersecurity against Russian attacks show that a contemporary and comprehensive knowledge of cyber threats and cybersecurity is essential if these threats are to be thwarted. The U.S. case also highlights this by showing its opposite: the failure to update company cybersecurity systems and lack of foresight enabled the attack to have severe

[34] U.S. GOVERNMENT PUBLISHING OFFICE, 16
[35] CISA, 'The Attack on Colonial Pipeline'
[36] Rusoff, *Legendary Ex-Fraudster*
[37] Rusoff, *Legendary Ex-Fraudster*

consequences on the population and the nation as a whole. As such, it is essential for nations to invest in cybersecurity as well as security education to ensure that states and actors within the state are aware of the technology required to respond effectively to potential physical threats perpetrated through cyberspace. This would allow the application by systems of cyber-informed engineering (CIE) and consequence-driven, cyber-informed engineering (CCE), which is essential to ensure the protection of the core of the company in the case of an attack, even if some less critical components are impacted.[38] This knowledge, however, can only be acquired by states if specific commissions of experts are set up with the aim of researching cybersecurity and cyber warfare. The U.S., during the post-Colonial Pipeline period, set up a number of these, such as the Joint Cyber Defense Collaborative (JCDC) and Joint Ransomware Task Force—a collaboration between the FBI and the CISA—which aim to research and conduct the federal response to cyber threats.[39] However, these measures will offer no fruition unless their findings are translated into tangible cybersecurity protocols and procedures created with the intention of preventing and thwarting attacks before they occur, which must be standardised through statewide protocols, as aforesaid.

5. Conclusion

The issue of cybersecurity is one that casts a shadow over national security at all times. The accessibility of cyber warfare to both state and non-state actors makes it a critical threat to which any state may be subject at any moment in time. In some cases, cyberattacks take place during an open conflict between two states, as is the case between Russia and Ukraine. To improve both national and international security, it is imperative for an international framework on cyber warfare to be established and recognised, in order to regulate cyber warfare in a similar manner to traditional militarism. Moreover, cyberattacks may take place in a moment of apparent peace, from a non-state actor, impacting either state or non-state actors, as was the case in the Colonial Pipeline attack. This case underlined the necessity for a uniform response across all attacks, pointing towards the creation of a statewide protocol. The case also highlighted the importance of focusing on prevention, and not simply putting in place policies for reparation after the fact. For this to be effective, the investment in research and expertise on the topics of cyber warfare and cybersecurity is imperative. Without these measures, our biggest vulnerability—our dependence on technology—remains unguarded, and an attack could induce nationwide chaos as the 2025 Iberian Peninsula blackout experienced.

[38] EBSCO, 'Two Years After the Colonial Pipeline Attack.'
[39] CISA, 'The Attack on Colonial Pipeline'

Bibliography

'28 April 2025 Blackout'. Accessed 16 November 2025. https://www.entsoe.eu/publications/blackout/28-april-2025-iberian-blackout/.

Abdyraeva, Cholpon. *Cyber Warfare*. The Use of Cyberspace in the Context of Hybrid Warfare. OIIP - Austrian Institute for International Affairs, 2020. https://www.jstor.org/stable/resrep25102.7.

Basuchoudhary, Atin. 'AI and Warfare: A Rational Choice Approach'. *Eastern Economic Journal* 51, no. 1 (2025): 74–86. https://doi.org/10.1057/s41302-024-00280-7.

'CYBER THREATS IN THE PIPELINE: LESSONS FROM THE FEDERAL RESPONSE TO THE COLONIAL PIPELINE RANSOMWARE ATTACK'. *U.S. GOVERNMENT PUBLISHING OFFICE*, 15 June 2021.

Disma, Carlo. *The Evolving Cyber Warfare Landscape*. The Alliance Five Years after Crimea: NATO Defense College, 2019. https://www.jstor.org/stable/resrep23664.12.

EBSCO. 'Two Years After the Colonial Pipeline Attack.' Accessed 17 November 2025. https://research-ebsco-com.scpo.idm.oclc.org/c/5v7is5/viewer/html/5sbqz3bnhj?route=details.

Grid Incident in Spain and Portugal on 28 April 2025 » ICS Investigation Expert Panel » Factual Report » 3 October 2025. n.d.

He Xiaotong. 'The Impact of Russia-Ukraine Cyberwarfare on the Application of the Right to Self-Defense in Cyberspace and Implications'. *US-China Law Review* 20, no. 3 (2023). https://doi.org/10.17265/1548-6605/2023.03.003.

Jones, Sam. 'Spanish Minister Rules out Cyber-Attack as Cause of April Blackout, after Expert Report'. World News. *The Guardian*, 17 June 2025. https://www.theguardian.com/world/2025/jun/17/expert-report-rules-out-cyber-attack-for-spain-and-portugal-april-blackout.

Lin, Herbert. 'Russian Cyber Operations in the Invasion of Ukraine'. *The Cyber Defense Review* 7, no. 4 (2022): 31–46.

NATO.Int. 'Prague Summit Declaration'. Accessed 16 November 2025. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2002/11/21/prague-summit-declaration.

Rusoff, Jane Wollman. *Legendary Ex-Fraudster Says Colonial Pipeline Attack Could Have Been Avoided*. (New York, United States), ALM Media Properties, LLC, 2021. https://www.proquest.com/docview/2541268283/abstract/35DC6E329E8549BDPQ/1.

Stubblefield, Emily. 'HACKTIVISTS AS COMBATANTS: WHAT UKRAINE'S COUNTEROFFENSIVE TO RUSSIA'S CYBERWARFARE MEANS FOR CIVILIAN HACKERS' STATUS UNDER THE LAWS OF WAR'. The Fordham urban law journal, October 2024.

'The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years | CISA'. 7 May 2023. https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years.

Whyte, Christopher. 'Searching for Cyberspace: The Colonial Pipeline Ransomware Attack through the Lens of Search Engines'. *Journal of Information Technology & Politics* 0, no. 0 (n.d.): 1–20. https://doi.org/10.1080/19331681.2024.2422908.