CYBERATTACKS AS GROUNDS FOR THE DECLARATION OF A STATE OF EMERGENCY

*Doc. dr. sc. Rok Dacar**

UDK 343.2:004.7(410)
https://doi.org/10.30925/zpfsr.46.3.5
Ur.: 9. svibnja 2025.
Pr.: 25. lipnja 2025.
Izvorni znanstveni rad

Summary

This article examines whether large-scale cyberattacks can be a legitimate reason for declaring a state of emergency. The central thesis is that while cyberattacks do not fit into the traditional categories of emergencies, their increasing capacity to seriously disrupt essential state functions calls for a reassessment of the legal thresholds for the use of emergency powers. The article argues that a cyberattack can justify the declaration of a state of emergency if it causes a systemic disruption to critical infrastructure, public order or national security and reaches a level of severity comparable to conventional emergencies. Real-world examples such as the cyberattacks on Estonia in 2007 and the ransomware crisis in Costa Rica in 2022 show different state responses and the evolving legal perception of cyber threats. At the same time, the article warns against the normalization of emergency regimes in response to persistent or unclear threats in cyberspace. The risk is that democratic governance is undermined by the prolonged or unjustified use of exceptional measures. While cyberattacks can in certain and extreme circumstances justify a state of emergency, such decisions must remain the exception and subject to the principles of necessity, proportionality and democratic control.

Keywords: *cyberattacks; state of emergency; emergency powers; national security law; constitutional crisis management.*

1 INTRODUCTION

In the 2007 film Live Free or Die Hard (also known as Die Hard 4.0), resilient police officer John McClane foils a plot by cyber terrorists to paralyse the United States of America by stealing financial data. In true Hollywood style, his fight against digital warfare escalates to the point where he jumps on a flying fighter jet. Although the action-packed depiction of cyberattacks in the film may seem exaggerated, the

* Rok Dacar, Ph.D., Assistant Professor, University of Maribor, Faculty of Law; rok.dacar@um.si. ORCID: https://orcid.org/0000-0001-8936-9311.

underlying threat is very real.

Modern cyberattacks have the potential to disrupt critical infrastructure, cripple governments and endanger human lives, raising serious questions about how States[1] should respond. When a cyberattack reaches the level of a national emergency, what legal and constitutional measures should be taken? This article examines the legal framework for declaring a state of emergency in response to cyberattacks.

A state of emergency has long been a legal tool that allows the executive branch to temporarily suspend normal democratic processes in response to crises. Traditionally, these declarations have been used in cases of military conflict, terrorist attacks, natural disasters and public health emergencies. However, the increasing prominence of cyberattacks as a national security threat raises the question of whether the existing legal framework for emergency powers can be extended to large-scale cyberattacks. This paper examines whether the national constitutional provisions on a state of emergency can be applied to cyberattacks and seeks to answer the research question: How can cyberattacks be addressed within the existing frameworks of states of emergency, and under what conditions might they justify the use of emergency powers?

The declaration of a state of emergency remains the responsibility of the individual States. Each country has its own legal framework for determining when and how emergency powers can be invoked. Despite these differences, most legal systems rely on similar criteria when assessing whether a situation justifies the declaration of a state of emergency, and the European Court of Human Rights (hereinafter: ECtHR) has also developed standards to guide such assessments. These common legal principles provide a useful benchmark for assessing whether cyberattacks meet the threshold for emergency action.

The paper will begin by defining cyberattacks and outlining their key characteristics. It will then examine the concept of a state of emergency and identify the common legal criteria for its declaration. These criteria will serve as a reference point for assessing whether cyberattacks could justify the invocation of emergency powers. Finally, the paper will summarize the main findings and provide an answer to the research question.

Although cyberattacks are receiving increasing attention in legal scholarship, particularly in the fields of international humanitarian law and cybersecurity law and policy, their interaction with national constitutional frameworks for states of emergency remains unexplored. Much of the existing literature focuses either on the categorization of cyber operations under international law or on policy discussions about deterrence. What remains unexplored is a doctrinal and comparative constitutional analysis of whether and under what conditions cyberattacks can lead to the triggering of emergency powers at the national level. This paper attempts to fill this gap by examining the extent to which existing constitutional provisions on emergencies can be extended to digital rather than kinetic crises and the thresholds

1 In this text, State (capitalized) refers to a sovereign political entity, such as a country (e.g., the State of Slovenia), whereas state (lowercase) denotes a legal or factual condition, such as a state of emergency or state of law.

that must be met for States to lawfully invoke extraordinary powers. In this way, it seeks to clarify the extent to which the traditional legal framework for states of emergency is fit for purpose in case of large scale and highly destructive cyberattacks. The paper thus aims to generate new knowledge by offering an in-depth doctrinal and comparative constitutional analysis of how national emergency frameworks can respond to large-scale cyberattacks.

2 THE NOTION OF CYBERATTACKS

The notion of cyberattacks is notoriously difficult to define and is often used "without clarifying what it is meant to include and exclude".[2] Closer analysis reveals that a cyberattack can take the form of cybercrime, cyber espionage or cyber warfare.[3] All three forms have the common feature of being unauthorized intrusions into cyber systems but differ in their objectives and scope.

Firstly, cybercrime refers to illegal activities carried out using digital technology or targeting computer systems, networks or data. This includes offenses such as hacking, identity theft, financial fraud, online harassment and the distribution of malware or ransomware. The Budapest Convention on Cybercrime[4] is the most important international legal framework for combating cybercrime. Cybercrime is generally subject to national criminal law, with jurisdiction and enforcement governed by national legal systems.

Ahead, cyberespionage refers to unauthorized digital intrusions by individuals, organizations, or governments aimed at accessing confidential information for strategic, economic, or political gain. It is used to steal trade secrets and intellectual property, to benefit domestic industries, to gain insight into foreign policy strategies and diplomatic communications, and to access classified defence information to enhance military capabilities.[5] Notable examples include Operation Socialist, a cyberattack carried out by the British Government Communications Headquarters (GCHQ) on the Belgian telecommunications operator Belgacom (now Proximus). The attack used malware-laden fake LinkedIn pages to infiltrate the systems of Belgacom engineers and enable long-term surveillance.[6] Another high-profile case is the reported attack on French President Emmanuel Macron's cell phone using

2 Oona Hathaway et al., "The Law of Cyber-Attack," *California Law Review* 100, no. 4 (2012): 822.

3 Joseph Eliezer, "Cyberwar: A Critical Analysis of Schmitt and the Tallinn Manual," *University of New South Wales Law Journal* 28 (2021); James McGhee, "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law," *Journal of Law & Cyber Warfare* 4, no. 1 (2014): 14.

4 The Convention on Cybercrime (Budapest Convention) and Its Protocols, European Treaty Series no. 185, of November 23, 2001.

5 Gary Brown, "Spying and Fighting in Cyberspace: What is Which," *Journal of National Security Law & Policy* 8 (2017): 622-624; "Cyberespionage Explained," accessed March 7, 2025, https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.

6 "British Spies 'Hacked into Belgian Telecoms Firm on Ministers' Orders'", accessed March 7, 2025, https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.

Pegasus spyware, which was allegedly orchestrated by Morocco's foreign intelligence service, although Morocco denies the allegations.[7]

Lasty, the term cyberwarfare is not a legally defined concept in authoritative sources. Instead, it is commonly used in a broad and informal manner to describe a range of harmful activities conducted by States in cyberspace, including cyberattacks on critical infrastructure, espionage, and disinformation campaigns.[8] Cyberwarfare consists of cyberattacks that either qualify as armed attacks under international law or take place in the context of an ongoing armed conflict.[9] Cyberwarfare actions can be used either as a complement to kinetic warfare to reinforce traditional military operations, or as a stand-alone method of conflict to achieve strategic objectives without physical force. In hybrid conflicts, cyber operations are often used alongside conventional military actions to disrupt infrastructure, weaken the enemy and manipulate the information environment. In Operation Orchard, for example, Israeli forces used cyber means to support a kinetic attack (air strike) on an alleged Syrian nuclear construction site. Similarly, in the 2008 Russian-Georgian war, the Russian armed forces supplemented traditional military manoeuvres with cyber operations.[10] Cyberwarfare can also be used as an independent instrument of State aggression to achieve strategic goals without the need for direct military confrontation. For example, the Stuxnet attack, widely attributed to the US and Israel, sabotaged Iran's nuclear centrifuges and set back Iran's nuclear program without a single missile attack.[11] In this regard, Atrews rightfully points out that over the last decade, the "traditional view of war has been shifting to a cyber battlefield rather than a literal battlefield".[12]

Cyberattacks can cause serious damage, especially when they are orchestrated by States rather than individual hacker groups. These attacks range from intellectual property theft, such as the North Korean hack of Sony Pictures in retaliation for the release of the movie The Interview, to far more dangerous scenarios that threaten lives and national stability. For example, in late 2022, Russian forces carried out an attack that paralysed part of Ukraine's power grid, showing that cyberwarfare can affect critical infrastructure.[13] Similarly, in 2021, the Colonial Pipeline, a major US

7 "Projet Pegasus: un téléphone portable d'Emmanuel Macron dans le viseur du Maroc," accessed March 8, 2025, https://www.lemonde.fr/projet-pegasus/article/2021/07/20/projet-pegasus-un-telephone-portable-d-emmanuel-macron-dans-le-viseur-du-maroc_6088950_6088648.html.

8 "Cyber Warfare," accessed March 6, 2025, https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0087.xml.

9 Delbert Tran, "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack," *Yale Journal of Law and Technology* 20 (2018): 380.

10 Mika Kerttunen, "Cyber Warfare - from Science Fiction to Reality," *Security and Peace* 36, no. 1 (2018): 27.

11 Irwing Lachow, "The Stuxnet Enigma: Implications for the Future of Cybersecurity," *Georgetown Journal of International Affairs,* special edition "International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity" (2011): 118-126.

12 Ridge Atrews, "Cyberwarfare: Threats, Security, Attacks, and Impact," *Journal of Information Warfare* 19, no. 4 (2020): 17.

13 "Russian Spies behind Cyber Attack on Ukraine Power Grid in 2022," accessed March 7, 2025, https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-

oil pipeline system, was the victim of a ransomware attack that forced a six-day shutdown.

3 STATE OF EMERGENCY

The state of emergency (also called state of danger [Hungary], state of crisis [Luxembourg], state of alarm [Spain], etc.) is an extraordinary legal measure, a temporary suspension or derogation from the normal constitutional order. It empowers the executive branch with extraordinary powers to respond to crises that threaten national security, public order or essential functions of the State. While it is necessary in extreme situations, it also raises concerns about the balance between security and fundamental rights.

3.1 Historical Dimensions of States of Emergency

The concept of the state of emergency was already known in ancient Athens and Rome. In Athens, legal norms could be temporarily suspended in times of crisis to protect the city-state. Rome, on the other hand, developed a more structured approach. In times of the Republic, a dictator was appointed to deal with emergencies such as wars or unrest. This office was strictly limited in both duration and scope to ensure that extraordinary powers were not abused. As Rome's political landscape became increasingly turbulent, the Senate began to rely on the *Senatus Consultum Ultimum* as an alternative to dictatorship. Instead of appointing a single ruler, it authorized consuls or other magistrates to take extraordinary measures to protect the Republic. In contrast to the dictatorship, which had a precisely defined legal framework and a time limit, the *Senatus Consultum Ultimum* was more flexible, but also legally more ambiguous. Over time, it became a means for the Senate to circumvent "constitutional" procedures, which often led to abuse, especially in the suppression of political opponents.[14] One of the most notorious cases occurred in 121 BC, when the Senate used it against Gaius Gracchus and ordered the consul Lucius Opimius to suppress him and his supporters. The decree led to violent clashes that forced Gracchus to flee; it is unclear whether he eventually took his own life or was killed. The concept of a state of emergency was later taken up again by thinkers such as Machiavelli, Locke and Rousseau, who saw emergency powers as essential for the preservation of constitutional systems. After the first world war, countries such as Germany and France formalized emergency provisions, most notably in the Weimar Constitution, whose emergency provisions have been invoked more than 200 times.[15]

In theory, there are two general views on the state of emergency. One, associated with Carl Schmitt (who coined the term state of exception, Ger. *Ausnahmezustand*), holds that legal norms are insufficient to deal with all crises and that in times of

ukrainian-power-grid-2022-researchers-2023-11-09/.

14 For more see: Robert Bonner, "Emergency Government in Rome and Athens," *The Classical Journal* 18, no. 3 (1922): 144-152.

15 "Emergency Powers," accessed March 8, 2025, https://www.britannica.com/topic/constitutional-law.

emergency, the executive must have the power to act beyond the limits of general law to protect the State and its constitutional order. For Schmitt, sovereignty is ultimately defined by the power to suspend the legal framework in exceptional situations.[16] Schmitt's theory laid the foundation for modern scholars, particularly Giorgio Agamben, who argues that the state of exception has become the defining paradigm of contemporary politics. According to Agamben, modern governments increasingly normalize states of exception by blurring the line between emergency regulations and normal governance, thereby legitimizing actions that lie beyond the boundaries of the law.[17] The other, more liberal, theory argues that emergency situations should be handled within the existing legal framework to prevent abuse of power. This view emphasizes the importance of maintaining legal constraints even in times of crisis to ensure that emergency measures remain subject to democratic control and the rule of law.[18] A balanced perspective between the two opposing views is the theory that an emergency constitution serves as the most effective mechanism for enabling swift and decisive action in times of crisis while simultaneously safeguarding fundamental rights from excessive or unwarranted restrictions.[19]

3.2 States of Emergency in Modern Constitutional Practice

"Today, emergency provisions are common institutional features of democratic States with a variety of constitutional arrangements".[20] What they have in common is that they reflect the enduring belief that decisive leadership is crucial in times of crisis.[21] The concentration of power in a single leader (or institution) helps to prevent the paralysis that can result from the separation of powers and the complexity of governance in modern democracies. At the same time, as Rositer points out, freeing that power from certain constitutional constraints allows the government to act without the limitations imposed by the protection of (relative) human rights.[22] In other words, when a state of emergency is declared, the traditional balance of power shifts considerably, as authority passes from the legislative to the executive. This

16 See: Duncan Kelly, "Carl Schmitt's Political Theory of Dictatorship," in *The Oxford Handbook of Carl Schmitt*, eds. Jens Meierhenrich, and Oliver Simons (Oxford: Oxford University Press, 2013), 217-244; Carl Schmitt, *Die Diktatur: von den Anfängen des modernen Souveränitätsgedankens bis zum proletarischen Klassenkampf* (Berlin: Duncker & Humblot, 1928).

17 Giorgio Agamben, *State of Exception* (Chicago: The University of Chicago Press, 2004).

18 Anna Khakee, "Securing Democracy? A Comparative Analysis of Emergency Powers in Europe," *Geneva Centre for the Democratic Control of Armed Forces Policy Papers*, no. 30 (2009): 7.

19 See: Bruce Ackerman, "The Emergency Constitution," *Yale Law Journal* 113, no. 5 (2004): 1029-1091.

20 Bryan Rooney, "Emergency Powers in Democracies and International Conflict," *The Journal of Conflict Resolution* 63, no. 3 (2019): 648.

21 As Charles de Gaulle famously stated, "Délibérer, c'est l'affaire de plusieurs, agir, c'est l'affaire d'un seul" [Deliberation is for many, but action is for one].

22 Clinton Rossiter, *Constitutional Dictatorship* (Princeton: Princeton University Press, 1948), 288.

shift gives the executive broader powers, often allowing it to take actions and make decisions with greater speed and less scrutiny than under normal circumstances. However, it is "frequently not specified what actions short of open warfare warrant the declaration of a state of emergency".[23] A state of emergency is usually declared in response to events such as civil unrest, rebellion, natural disasters or threats to national sovereignty and the stability of State institutions. In this context, it is important to distinguish between an emergency situation and a formally declared state of emergency. Although an emergency situation can lead to the declaration of a state of emergency, this is not always the case. The Covid pandemic has highlighted this divergence in approaches, as different countries have responded in different ways. Some declared a state of emergency, while others took emergency measures without formally declaring a state of emergency.[24] This underlines that emergency situations can be addressed through two different approaches: either by declaring a state of emergency or by using existing legal frameworks and regular legal instruments. In the latter case, all legal guarantees and constitutional safeguards remain fully intact. Although the state of emergency is primarily regulated by national constitutions, countries are also bound by internationally recognized legal instruments. Among the most important are the European Convention on Human Rights[25] (hereinafter: ECHR) and the International Covenant on Civil and Political Rights[26] (hereinafter: ICCPR), both of which establish a number of non-derogable human rights. Among these are the prohibition of torture and retroactive criminal punishment, which cannot be restricted or suspended under any circumstances, including during states of emergency or war. The ECHR also contains a vague definition of when a state of emergency exists. According to Article 15, derogations from the Convention's rights are only permitted in times of "war or other public emergency threatening the life of the nation." The requirement that the emergency must threaten "the life of the nation" refers to "an exceptional situation of crisis or emergency which affects the whole population and constitutes a threat to the organised life of the community of which the State is composed."[27] Ahead, the crisis or danger must be exceptional in that the normal measures or restrictions permitted by the ECHR for the maintenance of public safety, health and order are plainly inadequate.[28] Some examples of situations that were deemed as emergencies that threaten the life of the nation are

23 "Emergency Powers", 648.

24 European Parliament Research Service, *States of Emergency in Response to the Coronavirus Crisis* (Brussels: European Parliament, 2020), 11-14.

25 Convention for the Protection of Human Rights and Fundamental Freedoms, European Treaty Series no. 5, of November 4, 1950.

26 International Covenant on Civil and Political Rights, United Nations Treaty Series no. 14668, of December 16, 1966.

27 ECtHR, Ireland v. the United Kingdom, App. no. 5310/71, Judgment of January 18, 1978, para 28.

28 European Court of Human Rights, *Guide on Article 15 of the European Convention on Human Rights* (Strasbourg: Council of Europe, 2014), 6; also see: European Commission of Human Rights, Denmark, Norway, Sweden and the Netherlands v. Greece, App. no. 3321/67, Judgment of October 5, 1969, para 153.

IRA's terrorist activities in Northern Ireland[29] and the PKK's terrorist activities in south-east Turkey,[30] the Paris terrorist attacks of 2015[31] and the failed 2016 coup attempt in Turkey.[32]

The conditions for declaring a state of emergency and the procedures involved differ significantly across legal systems, reflecting historical experience, constitutional structures and political priorities. In most European countries, however, the declaration of a state of emergency is part of a general constitutional framework, with notable exceptions such as Italy, Belgium and Norway, which have no explicit constitutional provisions for such measures. Some countries have a single, general state of emergency that applies to all crises, while the majority have developed multiple categories tailored to different types of threats. For example, Article 92 of the Slovenian Constitution[33] declares that a state of emergency is declared when a major and general danger threatens the existence of the State. Similarly, Article 125 of the North Macedonian Constitution[34] states that a state of emergency exists when major natural disasters or epidemics occur. Both constitutions distinguish between a state of emergency and a state of war. The latter is triggered by actual or potential armed aggression or a formal declaration of war, while a state of emergency applies to other crises such as natural disasters or pandemics.

The Croatian Constitution does not explicitly recognize a "state of emergency" but instead differentiates between a state of war or an imminent threat to the independence and unity of the Republic of Croatia (Cro. *ratno stanje ili stanje neposredne ugroženosti neovisnosti i jedinstvenosti države*) and a natural disaster (Cro. *prirodna nepogoda*).[35] In both scenarios, the exercise of certain human rights may be restricted, provided such measures are approved by a two-thirds majority in the Croatian Parliament (Cro. *Sabor*). The Basic Law for the Federal Republic of Germany[36] contains detailed provisions on emergency situations. The state of tension (Ger. *Spannungsfall*) under Article 80a of the Basic Law is a precautionary measure

29 ECtHR, Ireland v. the United Kingdom, App. no. 5310/71, Judgment of January 18, 1978.

30 ECtHR, Aksoy v. Turkey, App. no. 21987/93, Judgment of December 18, 1996.

31 ECtHR, Domenjoud v. France, App. nos. 34749/16 and 79607/17, Judgment of January 25, 2024.

32 ECtHR, Mehmet Hasan Altan v. Turkey, App. no. 13237/17, Judgment of March 20, 2018.

33 *Ustava Republike Slovenije* [Constitution of the Republic of Slovenia], Official Gazette of the Republic of Slovenia, no. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.

34 *Устав на Република Северна Македонија* [Constitution of the Republic of North Macedonia], Official Gazette of the Republic of North Macedonia, no. 52/91, with latest amendment no. 6/19.

35 *Ustav Republike Hrvatske* [Constitution of the Republic of Croatia], Official Gazette of the Republic of Croatia, no. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14.

36 *Grundgesetz für die Bundesrepublik Deutschland* [Basic Law for the Federal Republic of Germany], Official Gazette of the Federal Republic of Germany, no. 1/49, with latest amendment no. 94/25.

that allows for preparatory military measures if an armed conflict appears imminent and requires the approval of the Bundestag to prevent arbitrary activation. The state of defence (Ger. *Verteidigungsfall*) under Article 115a of the Basic Law comes into effect if Germany is attacked by armed forces or if there is an imminent military threat, and triggers comprehensive defence measures. The internal state of emergency is regulated in Article 91 of the Basic Law, which allows the federal government to intervene in the event of serious unrest or a breakdown of constitutional order, if the federal States are unable to contain the crisis. In contrast, Article 35 of the Basic Law deals with natural disasters, and allows State governments to request assistance from the federal government, including the deployment of the Bundeswehr to coordinate disaster relief while respecting the separation of powers. Public health emergencies, such as those that occurred during the Covid pandemic, are regulated by the Infection Protection Act[37] and not by a constitutional state of emergency, which allows temporary restrictions of fundamental rights but is subject to judicial review.[38] The Hungarian Constitution distinguishes between four types of emergency regimes: state of emergency, state of preventive defence, state of terror threat and state of danger. The first three categories, state of emergency, state of preventive defence and state of terror threat, are declared when there is a risk of armed attack, whether through internal insurrection, external military threats or acts of terrorism. A state of emergency is declared when armed attempts are made to overthrow lawful order, usurp power or commit large-scale acts of violence that endanger life and property. The state of preventive defence is declared when there is a threat of an armed attack from the outside or when Hungary must fulfil alliance obligations. The state of terrorist threat is declared if there is a significant and immediate terrorist threat or a terrorist attack. In contrast, a state of danger is declared in the event of natural disasters, industrial accidents or other catastrophic events that endanger life and property to mitigate their consequences.[39] The Spanish constitution of 1978 provides for three states of emergency: state of alarm (Sp. *estado de alarma*), state of emergency (Sp. *estado de excepción*) and state of siege (Sp. *estado de sitio*). The state of alarm, the least serious emergency measure, can be declared in response to natural disasters, pandemics or serious disruptions to public services, as was the case during the Covid pandemic. The state of emergency is used in the event of serious disruptions to public order that cannot be dealt with by the usual legal means. It requires prior authorization from the Congress and allows temporary restrictions on fundamental rights such as freedom of movement or assembly, but is subject to judicial review. The state of siege, the most extreme measure, is imposed in the

37 *Infektionsschutzgesetz (Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen)* [Infection Protection Act], Official Gazette of the Federal Republic of Germany, no. 33/00, with latest amendment no. 359/23.

38 See: Carl Christoph Schweitzer, "Emergency Powers in the Federal Republic of Germany," *The Western Political Quarterly* 22, no. 1 (1969): 112-121; Anna-Bettina Kaiser, "The State of Exception under German Law and the Current Pandemic: Comparative Models and Constitutional Rights," *e-Pública* 7, no. 3 (2020).

39 Articles 50-53 of the *Magyarország Alaptörvénye* [Fundamental Law of Hungary], Official Gazette of the Republic of Hungary, no. 43/11, with latest amendment no. 46/25.

event of armed rebellion or an attack on Spain's sovereignty or territorial integrity. It can only be declared by the Chamber of Deputies and gives the government and the military extraordinary powers to restore order.[40]

Although the regulations governing the state of emergency vary from country to country, common reasons for declaring a state of emergency can be found in all legal systems. Firstly, external threats such as foreign invasions or armed attacks justify emergency measures to protect the territorial integrity of the State. Secondly, internal disturbances such as civil unrest, threats to public order or the destabilization of the constitutional order can also trigger emergency provisions. Third, large-scale natural disasters and calamities, whether caused by natural phenomena such as earthquakes, floods and fires or by man-made environmental or industrial accidents, often require extraordinary government powers to protect life, health and property.[41]

3.3 Towards a European State of Emergency?

In recent years, scholars have increasingly debated what is becoming known as "EU emergency law," and examined whether the EU's legal framework provides adequate mechanisms for effective crisis management.[42] In contrast to national systems, where emergency powers are usually embedded in constitutional structures, there is no general emergency clause in the EU. Instead, it relies on sector-specific provisions and institutional flexibility to deal with unforeseen challenges. The lack of a centralized framework for emergencies has led to legal and political tensions, especially when EU measures interfere with national sovereignty. The emergence of "EU emergency law" dates back to the euro crisis, when legal hurdles were first circumvented by emergency policies that broke with established norms and rules.[43] An important example was the creation of the intergovernmental European Stability Mechanism outside the EU institutional framework, bypassing existing legal restrictions. This trend continued during the migration crisis, when Frontex was given extraordinary powers.[44] Since then, EU emergency policy has been characterized by executive self-empowerment, rule circumvention, rule bending, domination and judicial deference. In the absence of a clear legal framework for dealing with crises, executive bodies have extended their powers beyond existing norms, as demonstrated by the ECB's role as lender of last resort and the implementation of austerity policies. The circumvention of rules has enabled the creation of alternative institutions such as the EFSF and ESM outside EU law, bypassing constitutional

40 José Manuel Vera Santos, "The Notion of Exception in the Spanish Constitution of 1978: Theory and Practice," in *Legal Implications of Territorial Secession in Spain*, ed. Carlos Fernández de Casadevante Romani (Berlin: Springer Nature, 2022), 403-437.

41 Khakee, "Securing Democracy?,"12.

42 Salvatore Nicolosi, "Addressing a Crisis through Law: EU Emergency Legislation and its Limits in the Field of Asylum," *Utrecht Law Review* 17, no. 4 (2021): 19-29; Christian Kreuder-Sonnen, "Does Europe Need an Emergency Constitution?" *Political Studies* 71, no. 1 (2021): 125-144; Ester Herlin-Karnell, "Republican Theory and the EU: Emergency Laws and Constitutional Challenges," *Jus Cogens* 3 (2021): 209-228.

43 Jonathan White, "Emergency Europe," *Political Studies* 63, no. 2 (2015): 302-303.

44 Kreuder-Sonnen, "Does Europe Need", 126.

constraints and undermining democratic accountability. These measures were further legitimized through flexible legal reinterpretations, as demonstrated by the ECB's shifting stance on bond purchases and quantitative easing. This unchecked authority has often led to domination, with powerful States imposing measures on weaker States, as exemplified by the Troika enforcing strict economic reforms in debtor countries, effectively stripping them of fiscal sovereignty. In this regard, Joerges concluded that such decision-making is "neither based upon democratic process, nor upon an exchange of reasons among equals; this is an authoritarian type of rule characterized by the kind of decision-making which Carl Schmitt foresaw and asked for in a state of emergency".[45] Meanwhile, judicial deference has contributed to the legal normalization of these extraordinary powers. The European Court of Justice, reluctant to question emergency measures for fear of economic collapse, has upheld them under the argument of necessity, further strengthening executive.[46] The Court's position could be compared to the "political question doctrine" established by the United States Supreme Court, which holds that certain questions are inherently political, not legal, and therefore not subject to judicial review. Under this doctrine, the judiciary refrains from adjudicating matters that it considers to be within the exclusive purview of the legislative or executive branches, recognizing that such decisions require political judgment rather than legal interpretation.[47]

The lack of explicit provisions on the state of emergency in the Treaties was addressed by the European Parliament, which adopted a Resolution to amend the Treaties[48] in November 2023, following the Conference on the Future of Europe. It is important to point out that the Resolution has no legally binding character. This Resolution contains 245 proposed amendments, 4 of which relate to the EU state of emergency context. The European Parliament's proposal for treaty reform aims to extend the EU's emergency powers and strengthen the involvement of the European Parliament in crisis management. Firstly, protection against cross-border health threats and civil protection are to be upgraded from supporting competences to areas of shared competence, so that the EU can act more directly in these areas. Secondly, it calls for the creation of a defence union, which would allow the deployment of military units under the operational command of the EU with parliamentary approval when a Member State is confronted with aggression. Thirdly, the proposal suggests to amend Article 78(3) of the Treaty on the Functioning of the European Union

45 Christian Joerges, "Three Transformations of Europe and the Search for a Way Out of Its Crisis," in *The European Crisis and the Transformation of Transnational Governance. Authoritarian Managerialism Versus Democratic Governance*, eds. Christian Joerges, and Carola Glinski (London: Hart Publishing, 2014), 34; Herlin-Karnell, "Republican Theory," 217.

46 Kreuder-Sonnen, "Does Europe Need", 128-129. Also see: Hjalte Lokdam, "We Serve the People of Europe: Reimagining the ECB's Political Master in the Wake of Its Emergency Politics," *Journal of Common Market Studies* 58, no. 4 (2020): 978-998.

47 For more see: Graham Butler, "In Search of the Political Question Doctrine in EU Law," *Legal Issues of Economic Integration* 45, no. 4 (2018): 329-354.

48 European Parliament Resolution of 22 November 2023 on proposals of the European Parliament for the amendment of the Treaties, 2022/2051(INL).

(hereinafter: TFEU),[49] which currently allows the Council to act in migration-related emergencies, by giving the European Parliament a right of initiative alongside the European Commission, thus strengthening democratic influence in migration-related emergencies. Finally, the most important proposed structural change is the deletion of Article 122 TFEU, which currently allows the Council to adopt emergency measures with minimal parliamentary scrutiny. Instead, a new emergency clause (Article 222(1) TFEU) is to be introduced, enabling the Parliament and the Council to confer extraordinary powers on the Commission for a certain period of time in times of crisis. Modelled on national emergency provisions, this clause aims to formalize the EU's emergency powers while addressing concerns about democratic legitimacy and institutional accountability in decision-making in times of crisis.[50]

4 CYBERATTACKS AS GROUNDS FOR DECLARING A STATE OF EMERGENCY

When analysing the question of whether cyberattacks can justify the declaration of a state of emergency, two key situations must be distinguished. First, a cyberattack may constitute an act of war that triggers the legal framework for armed conflict and national defence. Second, although a cyberattack may not reach the threshold of an act of war, it may nevertheless have serious consequences for critical infrastructure, public security or national stability, requiring emergency measures.

4.1 Cyberattacks as Acts of War

If a cyberattack can be considered an act of war and a State has the necessary legal framework, a constitutional state of war can be declared. Most states recognize a formal state of war, even if they use different terms. France recognizes a "state of siege" (Fr. *état de siège*),[51] Germany speaks of a "state of defense" (Ger. *Verteidigungsfall*)[52] in its Basic Law, Spain permits the "state of siege" (Sp. *estado de sitio*),[53] while Poland recognizes the "state of war" (Pl. *stan wojny*).[54] North Macedonia and Slovenia both refer to a "state of war" (*voena sostojba, vojno stanje*)

49 Consolidated Version of the Treaty on the Functioning of the European Union, OJ C 326 of October 26, 2012.

50 Guido Bellenghi, "The European Parliament's Proposal for an EU State of Emergency Clause: A Comparative and Constitutional Analysis," *Croatian Yearbook of European Law and Policy* 20 (2024): 1-2.

51 *Constitution de la Cinquième République* [Constitution of the Fifth Republic], Official Gazette of the French Republic, no. 0234/58, no. 0234/58, with latest amendment no. 2024/200.

52 Article 115a of the *Grundgesetz für die Bundesrepublik Deutschland* [Basic Law for the Federal Republic of Germany], Official Gazette of the Federal Republic of Germany, no. 1/49, with latest amendment no. 94/25.

53 Article 116 of the *Constitución Española* [Spanish Constitution], Official Gazette of the Kingdom of Spain, no. 1978-31229, with latest amendment no. 2024-3099.

54 Article 116 of the *Konstytucja Rzeczypospolitej Polskiej* [Constitution of the Republic of Poland], Official Gazette of the Republic of Poland, no. 78/97, item 483, with latest amendment no. 114/09, item 946.

in their Constitutions.[55] If such a framework does not exist or the attack does not meet the threshold of an act of war, a state of emergency may be declared instead.

It is crucial to distinguish war in the sense of international law from a state of war in constitutional law. The former refers to an armed conflict between States or between State and non-State actors, governed by the laws of war, including the *jus ad bellum* (right to war) and the *jus in bello* (laws governing conduct in war). The latter, a state of war in constitutional law, is a legal state declared by a State in response to an external attack, the imminent threat thereof, or a formal declaration of war, and gives the executive extraordinary powers. As a rule, the existence of an armed conflict in the sense of international law usually serves as the legal basis for the declaration of a state of war prescribed by constitutional law. It is therefore important to carefully examine the conditions under which a cyberattack is considered an act of war. Cyberspace remains a legally ambiguous area where the threshold for war is not clearly defined. "The reason such difficulty arises in labelling cyberattacks as an act of war is their inherent nature. They are not exactly armed conflict nor always a display of force".[56]

An important interpretative aid in this context is the Tallinn Manual, a comprehensive legal study developed under the direction of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia. Although it has no binding legal authority, the Manual provides important guidance on the application of international law to cyber operations. It states that "the mere fact that a computer (rather than a more traditional weapon, weapon system, or platform) is used during an operation has no bearing on whether that operation amounts to a use of force".[57] This suggests that the method of attack is less important than its effects in determining whether a cyberattack crosses the legal threshold of war.

Not every use of force, whether kinetic or online, constitutes an act of war. The extent, intention and consequences of an action are decisive factors. Limited uses of force, such as border skirmishes, targeted attacks or self-defence actions, need not necessarily escalate into full-blown war if they remain proportionate and do not provoke wider hostilities. International law, in particular the judgments of the International Court of Justice (hereinafter: ICJ), distinguishes between minor use of force and armed attacks that justify war or collective defence. In Nicaragua v. United States,[58] the ICJ stated that the classification of an act as an "armed attack" depends on its scale and consequences, including loss of life, physical destruction and overall impact. If a cyber operation reaches a high threshold of severity, the victim State may invoke its inherent right of self-defence under Article 51 of the UN Charter,[59] which

55 Article 125 of the *Ustava Republike Slovenije* [Constitution of the Republic of Slovenia], Official Gazette of the Republic of Slovenia, no. 33/11.

56 Christopher Sanders, "The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an 'Act of War'?" *Utah Law Review* 2 (2018): 513.

57 Michael Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017), 328.

58 ICJ, Nicaragua v. United States of America, no. 1986 I.C.J. 14, of June 27, 1986.

59 Charter of the United Nations, of June 26, 1945, accessed May 13, 2025, https://www.un.org/en/about-us/un-charter.

may include military retaliation. Small-scale cyberattacks are unlawful but do not necessarily justify a military response. In this regard, the Tallinn Manual states: "a State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence. Whether a cyber operation constitutes an armed attack depends on its scale and scope".[60]

Whether a cyberattack justifies self-defence and consequently a declaration of war depends on the circumstances of the case, in particular the scale and impact of the attack. Some cyberattacks result in physical destruction, while others are disruptive but not destructive. An important example is the Stuxnet attack, which demonstrated that cyber operations could cause tangible, kinetic damage. Stuxnet was a sophisticated cyberweapon that targeted Iran's nuclear facility at Natanz, specifically the centrifuges used to enrich uranium. By manipulating their rotational speed, the malware caused the physical disruption and destruction of critical infrastructure, setting back Iran's nuclear program. Given its destructive impact, Stuxnet arguably approached the threshold of an armed attack, although Iran did not officially respond with military action. In contrast, the cyberattacks on Estonia in 2007, attributed to actors linked to Russia, were highly disruptive but not destructive. These attacks targeted government institutions, financial companies and media outlets through large-scale distributed denial of service (DDoS) attacks and paralyzed Estonia's digital infrastructure for weeks.[61] However, the attacks did not result in physical destruction or loss of life, making it difficult to classify them as an armed attack under international law.

A cyberattack that causes physical destruction, and direct damage is much more likely to justify self-defence and even a declaration of war, while a cyber disruption alone does probably not meet the required threshold. In summary, a cyberattack could serve as a basis for declaring a state of war if its scale and effects meet the thresholds established by international law for an armed conflict, such as causing significant destruction, loss of life, or severe disruption of critical infrastructure.

4.2 Cyberattacks that are not Acts of War

If a cyberattack does not reach the threshold that justifies the declaration of a state of war, States can still declare a state of emergency to take extraordinary legal measures to protect national security, public order or critical infrastructure. The historical use of states of emergency in Europe shows that they have been used in a variety of crises.

During the Covid pandemic, several EU member States, including the Czech Republic, Estonia, Finland, Luxembourg, Portugal, Romania, Slovakia and Spain declared a state of emergency to deal with the public health crisis. These measures

60 Schmitt, ed., *Tallinn Manual 2.0,* 339.

61 Stephen Herzog, "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses," *Journal of Strategic Security* 4, no. 2 (2011): 49-60; Samuli Haataja, "The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach," *Law, Innovation and Technology* 9, no. 2 (2017): 159-189.

facilitated lockdowns, travel bans and economic interventions.[62] Hungary adopted emergency measures under its own constitutionally foreseen "state of danger" at the beginning of the pandemic in March 2020. This was later changed to a "state of danger due to war" following Russia's invasion of Ukraine in 2022, which remains in effect to this day. Besides this, Hungary also declared a "state of migration emergency" during the migration crisis in 2015 and "state of medical emergency" during the Covid pandemic, both of which were introduced with ordinary laws and were not subject to the restrictions applying to constitutional states of emergency.[63] France has also made extensive use of emergency powers in recent decades, using them in response to civil unrest, terrorism and regional instability. The riots of 2005 prompted President Jacques Chirac to declare a state of emergency on November 8, 2005, which was later extended for three months by parliament with a UMP majority.[64] Following the Paris attacks in November 2015, a much longer state of emergency was declared, which was originally intended as a short-term measure but was extended several times until November 2017. The state of emergency remained in force during the French presidential elections in 2017 and was only lifted after new counter-terrorism laws were passed in October 2017 to replace it.[65] Most recently, President Emmanuel Macron declared a state of emergency in New Caledonia on May 16, 2024, in response to violent protests sparked by proposed changes to electoral law in the territory. The French government wanted to change the electoral rules to expand the electorate for the provincial elections. This measure was seen by the pro-independence indigenous Kanak as a threat to their political influence. The protests quickly escalated into unrest, resulting in deaths, injuries and considerable damage to property.[66] In addition to political instability and security threats, natural disasters have also led to declarations of emergency. In February 2025, Greece declared a state of emergency on the island of Santorini following a series of earthquakes that severely threatened infrastructure and public safety, requiring immediate state intervention.[67]

The above analysed use of states of emergency across Europe demonstrates that States declare them to respond to crises that seriously threaten public order, national security and critical infrastructure. While emergencies in the past were predominantly triggered by physical threats such as terrorist attacks, pandemics,

62 European Parliament Research Service, *States of Emergency in Response to the Coronavirus Crisis* (Brussels: European Parliament, 2020), 11-14.

63 For more see: Gabor Mészáros, "How Misuse of Emergency Powers Dismantled the Rule of Law in Hungary," *Israel Law Review* 57, no. 2 (2024): 288-307.

64 Evelyne Sire-Marin, "L'état d'urgence, rupture de l'État de droit ou continuité des procédures d'exception?" *Mouvements* 44 (2006): 78-82; Jeniffer Fredette, "The French State of Emergency," *Current History* 116 (2017): 101-106.

65 "France's Macron 'to End State of Emergency', but Keep Its Anti-Terror Powers," accessed March 13, 2023, https://www.france24.com/en/20170609-france-state-emergency-macron-police-powers-civil-liberties-terrorism.

66 "Four Dead in New Caledonia Riots, France Declares State of Emergency," accessed March 13, 2025, https://www.reuters.com/world/asia-pacific/new-caledonia-riots-rage-after-paris-approves-voting-change-2024-05-15/.

67 "State of Emergency Declared for Santorini After Quakes," accessed March 14, 2025, https://www.bbc.com/news/articles/ce8jlm6rm9qo.

civil unrest or natural disasters, the increasing reliance on digital infrastructure raises the question of whether cyberattacks could reach the same threshold. By its very nature, a cyberattack does not have the immediate physical destruction of traditional emergencies, but that does not mean it cannot have similarly severe consequences. If a cyberattack disables critical government functions, paralyzes essential services and causes widespread societal disruption, it could justify the invocation of emergency powers. The legal and policy challenge is to determine when a cyberattack moves from a cybersecurity governance problem to a national emergency requiring a declaration of a state of emergency.

In my opinion, the key factor in justifying the declaration of a state of emergency is the extent of the disruption. Minor cyber incidents such as data breaches, ransomware attacks on individual institutions or temporary service outages would not meet this threshold. However, a cyberattack that paralyses national infrastructure such as power grids, banking systems, emergency services or military communications could result in the State no longer being able to function effectively, requiring extraordinary measures. Consider the legal justification for the prolonged state of emergency in France following the 2015 Paris attacks: the government deemed emergency powers essential to prevent further attacks, secure public spaces and strengthen counter-terrorism capabilities. If a cyberattack were to trigger a similar or even greater level of disruption with mass casualties due to healthcare outages, widespread economic collapse due to the paralysis of the financial sector, or prolonged insecurity due to the closure of security agencies, the declaration of a state of emergency could be justified using the same logic. The fundamental principle at the core of the declaration of a state of emergency is necessity: when the normal legal framework proves inadequate to contain a crisis, extraordinary measures become legally and politically legitimate.

There are clear precedents indicating that States have often been reluctant to classify cyberattacks as emergencies requiring exceptional measures. An important example is Estonia in 2007, when the country faced a series of large-scale cyberattacks on government institutions, banks and the media. At the time, these were among the most sophisticated cyberattacks ever recorded. They disrupted vital services and had geopolitical implications. Nevertheless, Estonia did not declare a state of emergency. Instead, it relied on its well-developed cyber security infrastructure and international cooperation to limit the damage. This shows that cyber threats, provided they do not completely incapacitate the State, can often be dealt with through targeted security measures rather than emergency powers. However, the 2022 ransomware attack in Costa Rica shows a contrasting approach. Over the course of several weeks, almost 30 government institutions, including the Ministry of Finance, were severely disrupted. Newly sworn-in President Rodrigo Chaves Robles responded by declaring a national state of emergency, the first known instance of a country taking such a step due to a cyberattack.[68] In my opinion, the contrast between these two cases illustrates how the

68 "Costa Rica Declares Emergency in ongoing Cyberattack," accessed March 14, 2025, https://apnews.com/article/covid-technology-health-caribbean-costa-rica-949b141c5b5e288214f80d2cb6753bdb.

role of digital infrastructure has evolved. In 2007, cyber systems were critical, but not yet as deeply embedded in every aspect of government, business and daily life as they are today. Today, with the exponential growth of digitization, cyberattacks have the potential to cripple the economy, disrupt critical services and even compromise national security in ways that can justify emergency measures that once seemed excessive.

Moreover, the potential for abuse of emergency powers must be carefully considered. Hungary's successive and prolonged declarations of emergency first for the Covid pandemic, and later for the war in Ukraine, show how emergency regimes can become entrenched and blur the line between crisis management and governance by decree.[69] Cyber security threats, unlike wars or natural disasters, are not temporary; they are ongoing, evolving and often persistent. When States begin to declare emergencies in response to cyber threats without clear boundaries, they risk normalizing emergency regulations, undermining democratic governance, and limiting fundamental rights indefinitely. Turning cyber incidents into States of emergency risks normalising exceptional powers and weakening oversight mechanisms. Although a detailed treatment of these governance challenges is beyond the scope of this paper, I emphasise the importance of future research on institutional safeguards and proportionality requirements that may constrain emergency powers in the cyber domain.

Nevertheless, the argument that a cyberattack could justify a state of emergency remains convincing, provided the consequences are serious enough. Should a cyberattack have effects such as the systemic collapse of financial institutions, the prolonged failure of energy infrastructure, or mass casualties from failed healthcare systems it would be illogical to deny the state the same legal tools it has used in other national crises. The key is to ensure that declarations of states of emergency remain a last resort, reserved for cases where no other legal framework is sufficient to deal with the crisis.

5 CONCLUSION

This article examined whether the traditional concept of a state of emergency can be extended to cyberattacks and under what conditions such an extension would be legally justified. The analysis has shown that while cyberattacks do not inherently fit into the traditional framework of emergencies, their increasing severity and systemic consequences call for a rethinking of existing legal paradigms.

This paper first addressed the definitional challenges of cyberattacks, distinguishing cybercrime, cyberespionage, and cyberwarfare. The legal framework for emergency powers was then examined, tracing its development from ancient Rome to modern constitutional provisions and identifying the key criteria for declaring states of emergency. The study also analyzed how states of emergency have been used in various crises. An important distinction made in this paper is that between a state of war and a state of emergency. If a cyberattack meets the threshold of an

69 Mészáros, "How Misuse," 288-307.

armed attack, i.e. physical destruction, casualties or effects comparable to kinetic warfare, a State could declare a state of war (*Verteidigungsfall, état de siège, voena sostojba, vojno stanje*, etc.). Ahead, the paper identified that the EU lacks a central framework for emergencies. Instead, it relies on sector-specific measures. In past crises, such as the euro and migration crises, emergency powers have been extended through circumvention of rules and judicial deference. In response, the 2023 treaty reform proposal aims to formalize the EU's emergency powers.

Cyber security threats have historically been addressed through criminal law enforcement, intelligence operations and defensive cyber strategies rather than declarations of states of emergency. However, the evolving nature of cyberwarfare, particularly its ability to cause widespread societal and economic disruption, could be challenging this traditional approach. The growing interdependence between digital infrastructure and State functions means that a well-coordinated cyberattack could cripple critical services, destabilize financial markets and undermine national security without a single bullet being fired. Cyberattacks are therefore increasingly capable of having similar effects to conventional security crises that have warranted a declaration of a state of emergency in the past. The principle of necessity that underpins declarations of states of emergency suggests that such a declaration could be justified if a cyberattack were to render a State unable to function effectively, whether by disabling power grids, shutting down financial systems or paralyzing national security mechanisms. The French state of emergency following the 2015 Paris attacks shows that States resort to extraordinary legal measures when normal government structures prove inadequate to contain a crisis. If a cyberattack were to cause a similar or even greater level of disruption, the same legal justification could apply.

Historical precedents show that States have responded differently to cyberattacks. Some have opted for targeted cybersecurity measures, while others have seen them as grounds for the use of emergency powers. Estonia's response to the 2007 cyberattacks is an example of a cautious approach. Despite widespread disruption to government institutions, banks and the media, the Estonian government relied on its cyber security infrastructure and international cooperation rather than declaring a state of emergency. At the time, cyberattacks were not necessarily seen as sufficient justification for extraordinary legal measures. However, recent cases suggest that this view is shifting. The ransomware attack in Costa Rica in 2022 severely disrupted nearly 30 government institutions, including the Ministry of Finance, and significantly impacted public administration and economic stability. In contrast to Estonia's response, President Rodrigo Chaves Robles declared a national state of emergency. This was the first known case in which such a measure was taken solely due to a cyberattack. This case shows that some States now consider cyberattacks serious enough to justify emergency powers, especially when they pose a direct threat to governance and essential services. The legal and technological landscape has changed dramatically since the Estonian experience. Today, States are far more dependent on digital systems to maintain essential functions. The increasing digitalization of critical services, combined with the increasing sophistication of

cyber threats, suggests that future cyberattacks could cause much greater damage than previously anticipated.[70] I believe that it is now more likely than in the past that a large-scale cyberattack will lead to the declaration of a state of emergency.

At the same time, this paper has highlighted the risks associated with emergency cyber governance. The Hungarian case shows how emergency powers, once invoked, can become entrenched and potentially undermine democratic institutions. As cyber threats are not temporary but persistent, States must be careful when using emergency measures and ensure that such declarations are proportionate, time-limited and subject to democratic scrutiny. The risk of States overextending their emergency powers in response to cyber security threats highlights the importance of establishing clear legal thresholds and procedural safeguards. Without these safeguards, there is a risk that governments will use cyber threats as a justification for eroding fundamental rights, expanding surveillance powers, or consolidating executive power in ways that go beyond the immediate crisis.

Not every cyberattack justifies the triggering of emergency powers, and rightly so. But when the consequences of such attacks are serious enough to disrupt essential state functions, endanger human lives or seriously destabilize the economy, there are good constitutional grounds for declaring a state of emergency. Although cyberattacks are a relatively new type of threat, their intentional and man-made nature places them in a broader category of risks to which jurisdictions have long responded with emergency measures. The real challenge lies not so much in the legal provisions themselves, but in how they are applied. It is vital that responses to cyber incidents remain firmly anchored in the principles of legality, necessity and proportionality, and that emergency powers are never used as a shortcut to circumvent constitutional safeguards.

BIBLIOGRAPHY

Books and Articles:

1. Ackerman, Bruce. "The Emergency Constitution." *Yale Law Journal* 113, no. 5 (2004): 1029-1091.
2. Agamben, Giorgio. *State of Exception*. Chicago: The University of Chicago Press, 2004.
3. Atrews, Ridge. "Cyberwarfare: Threats, Security, Attacks, and Impact." *Journal of Information Warfare* 19, no. 4 (2020): 17-28.
4. Bellenghi, Guido. "The European Parliament's Proposal for an EU State of Emergency Clause: A Comparative and Constitutional Analysis." *Croatian Yearbook of European Law and Policy* 20 (2024): 1-30.
5. Bonner, Robert. "Emergency Government in Rome and Athens." *The Classical Journal* 18, no. 3 (1922): 144-152.
6. Brown, Gary. "Spying and Fighting in Cyberspace: What is Which." *Journal of National Security Law & Policy* 8 (2017): 621-635.
7. Butler, Graham. "In Search of the Political Question Doctrine in EU Law." *Legal Issues of Economic Integration* 45, no. 4 (2018): 329-354.

70 For example, see: "Threat of Cyber-Attacks on Whitehall 'is Severe and Advancing Quickly', NAO Says," accessed March 14, 2025, https://www.theguardian.com/technology/2025/jan/29/cyber-attack-threat-uk-government-departments-whitehall-nao.

8. Eliezer, Joseph. "Cyberwar: A Critical Analysis of Schmitt and the Tallinn Manual." *University of New South Wales Law Journal* 28 (2021): 1-21.
9. European Court of Human Rights. *Guide on Article 15 of the European Convention on Human Rights.* Strasbourg: Council of Europe, 2014.
10. European Parliament Research Service. *States of Emergency in Response to the Coronavirus Crisis*. Brussels: European Parliament, 2020.
11. Fredette, Jeniffer. "The French State of Emergency." *Current History* 116 (2017): 101-106.
12. Haataja, Samuli. "The 2007 Cyber Attacks Against Estonia and International Law on the Use of Force: An Informational Approach." *Law, Innovation and Technology* 9, no. 2 (2017): 159-189.
13. Hathaway, Oona, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, and Julia Spiegel. "The Law of Cyber-Attack." *California Law Review* 100, no. 4 (2012): 817-886.
14. Herlin-Karnell, Ester. "Republican Theory and the EU: Emergency Laws and Constitutional Challenges." *Jus Cogens* 3 (2021): 209-228.
15. Herzog, Stephen. "Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses." *Journal of Strategic Security* 4, no. 2 (2011): 49-60.
16. Joerges, Christian. "Three Transformations of Europe and the Search for a Way Out of Its Crisis." In *The European Crisis and the Transformation of Transnational Governance. Authoritarian Managerialism Versus Democratic Governance*, eds. Christian Joerges, and Carola Glinski, 25-46. London: Hart Publishing, 2014.
17. Kaiser, Anna-Bettina. "The State of Exception under German Law and the Current Pandemic: Comparative Models and Constitutional Rights." *e-Pública* 7, no. 3 (2020): 4-15.
18. Kelly, Duncan. "Carl Schmitt's Political Theory of Dictatorship." In *The Oxford Handbook of Carl Schmitt*, eds. Jens Meierhenrich, and Oliver Simons, 217-244. Oxford: Oxford University Press, 2013.
19. Kerttunen, Mika. "Cyber Warfare - from Science Fiction to Reality." *Security and Peace* 36, no. 1 (2018): 27-33.
20. Khakee, Anna. "Securing Democracy? A Comparative Analysis of Emergency Powers in Europe." *Geneva Centre for the Democratic Control of Armed Forces Policy Papers*, no. 30 (2009): 1-45.
21. Kreuder-Sonnen, Christian. "Does Europe Need an Emergency Constitution?" *Political Studies* 71, no. 1 (2021): 125-144.
22. Lachow, Irving. "The Stuxnet Enigma: Implications for the Future of Cybersecurity." *Georgetown Journal of International Affairs,* special edition "International Engagement on Cyber: Establishing International Norms and Improved Cybersecurity" (2011): 118-126.
23. Lokdam, Hjalte. "We Serve the People of Europe: Reimagining the ECB's Political Master in the Wake of Its Emergency Politics." *Journal of Common Market Studies* 58, no. 4 (2020): 978-998.
24. McGhee, James. "Hack, Attack or Whack; The Politics of Imprecision in Cyber Law." *Journal of Law & Cyber Warfare* 4, no. 1 (2014): 13-41.
25. Mészáros, Gabor. "How Misuse of Emergency Powers Dismantled the Rule of Law in Hungary." *Israel Law Review* 57, no. 2 (2024): 288-307.
26. Nicolosi, Salvatore. "Addressing a Crisis through Law: EU Emergency Legislation and its Limits in the Field of Asylum." *Utrecht Law Review* 17, no. 4 (2021): 19-29.
27. Rooney, Bryan. "Emergency Powers in Democracies and International Conflict." *The Journal of Conflict Resolution* 63, no. 3 (2019): 644-671.
28. Rositer, Clinton. *Constitutional Dictatorship*. Princeton: Princeton University Press, 1948.

29. Sanders, Christopher. "The Battlefield of Tomorrow, Today: Can a Cyberattack Ever Rise to an 'Act of War'?" *Utah Law Review* 2 (2018): 503-522.
30. Schmitt, Carl. *Die Diktatur: von den Anfängen des modernen Souveränitätsgedankens bis zum proletarischen Klassenkampf.* Berlin: Duncker & Humblot, 1928.
31. Schmitt, Michael, ed. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press, 2017.
32. Schweitzer, Carl Christoph. "Emergency Powers in the Federal Republic of Germany." *The Western Political Quarterly* 22, no. 1 (1969): 112-121.
33. Sire-Marin, Evelyne. "L'état d'urgence, rupture de l'État de droit ou continuité des procédures d'exception?" *Mouvements* 44 (2006): 78-82.
34. Tran, Delbert. "The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack." *Yale Journal of Law and Technology* 20 (2018): 377-441.
35. Vera Santos, José Manuel. "The Notion of Exception in the Spanish Constitution of 1978: Theory and Practice." In *Legal Implications of Territorial Secession in Spain*, ed. Carlos Fernández de Casadevante Romani, 403-437. Berlin: Springer Nature, 2022.
36. White, Jonathan. "Emergency Europe." *Political Studies* 63, no. 2 (2015): 302-303.

Legal Sources:

1. Charter of the United Nations, of June 26, 1945. Accessed May 13, 2025. https://www.un.org/en/about-us/un-charter.
2. Consolidated Version of the Treaty on the Functioning of the European Union, OJ C 326 of October 26, 2012.
3. *Constitución Española* [Spanish Constitution], Official Gazette of the Kingdom of Spain, no. 1978-31229, with latest amendment no. 2024-3099.
4. *Constitution de la Cinquième République* [Constitution of the Fifth Republic], Official Gazette of the French Republic, no. 0234/58, with latest amendment no. 2024/200.
5. Convention for the Protection of Human Rights and Fundamental Freedoms, European Treaty Series no. 5 of November 4, 1950.
6. European Parliament Resolution of 22 November 2023 on proposals of the European Parliament for the amendment of the Treaties, 2022/2051(INL) of November 22, 2023.
7. *Grundgesetz für die Bundesrepublik Deutschland* [Basic Law for the Federal Republic of Germany], Official Gazette of the Federal Republic of Germany, no. 1/49, with latest amendment no. 94/25.
8. *Infektionsschutzgesetz (Gesetz zur Verhütung und Bekämpfung von Infektionskrankheiten beim Menschen)* [Infection Protection Act], Official Gazette of the Federal Republic of Germany, no. 33/00, with latest amendment no. 359/23.
9. International Covenant on Civil and Political Rights, United Nations Treaty Series no. 14668, of December 16, 1966.
10. *Konstytucja Rzeczypospolitej Polskiej* [Constitution of the Republic of Poland], Official Gazette of the Republic of Poland, no. 78/97, item 483, with latest amendment no. 114/09, item 946.
11. *Magyarország Alaptörvénye* [Fundamental Law of Hungary], Official Gazette of the Republic of Hungary, no. 43/11, with latest amendment no. 46/25.
12. The Convention on Cybercrime (Budapest Convention) and Its Protocols, European Treaty Series no. 185, of November 23, 2001.
13. *Ustav Republike Hrvatske* [Constitution of the Republic of Croatia], Official Gazette of the Republic of Croatia, no. 56/90, 135/97, 08/98, 113/00, 124/00, 28/01, 41/01, 55/01, 76/10, 85/10, 05/14
14. *Ustava Republike Slovenije* [Constitution of the Republic of Slovenia], Official Gazette of the Republic of Slovenia, no. 33/91-I, 42/97 – UZS68, 66/00 – UZ80, 24/03 – UZ3a, 47, 68, 69/04 – UZ14, 69/04 – UZ43, 69/04 – UZ50, 68/06 – UZ121,140,143, 47/13 – UZ148, 47/13 – UZ90,97,99, 75/16 – UZ70a in 92/21 – UZ62a.

15. *Устав на Република Северна Македонија* [Constitution of the Republic of North Macedonia], Official Gazette of the Republic of North Macedonia, no. 52/91, with latest amendment no. 6/19.

Case Law:

1. ECtHR, Aksoy v. Turkey, App. no. 21987/93, Judgment of December 18, 1996.
2. ECtHR, Domenjoud v. France, App. nos. 34749/16 and 79607/17, Judgment of January 25, 2024.
3. ECtHR, Ireland v. the United Kingdom, App. no. 5310/71, Judgment of January 18, 1978.
4. ECtHR, Lawless v. Ireland (No. 3), App. no. 332/57, Judgment of July 1, 1961.
5. ECtHR, Mehmet Hasan Altan v. Turkey, App. no. 13237/17, Judgment of March 20, 2018.
6. European Commission of Human Rights, Denmark, Norway, Sweden and the Netherlands v. Greece, App. no. 3321/67, Judgment of October 5, 1969.
7. ICJ, Nicaragua v. United States of America, no. 1986 I.C.J. 14 of June 27, 1986.

Internet Sources:

1. "British Spies 'Hacked into Belgian Telecoms Firm on Ministers' Orders'." Accessed March 7, 2025. https://www.theguardian.com/uk-news/2018/sep/21/british-spies-hacked-into-belgacom-on-ministers-orders-claims-report.
2. "Costa Rica Declares Emergency in Ongoing Cyber Attack." Accessed March 14, 2025. https://apnews.com/article/covid-technology-health-caribbean-costa-rica-949b141c5b5e288214f80d2cb6753bdb.
3. "Cyber Warfare." Accessed March 6, 2025. https://www.oxfordbibliographies.com/display/document/obo-9780199796953/obo-9780199796953-0087.xml.
4. "Cyberespionage Explained." Accessed March 7, 2025. https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/cyber-espionage/.
5. "Emergency Powers." Accessed March 8, 2025. https://www.britannica.com/topic/constitutional-law.
6. "Four Dead in New Caledonia Riots, France Declares State of Emergency." Accessed March 13, 2025. https://www.reuters.com/world/asia-pacific/new-caledonia-riots-rage-after-paris-approves-voting-change-2024-05-15/.
7. "France's Macron 'to end State of Emergency', but Keep its Anti-Terror Powers." Accessed March 13, 2023. https://www.france24.com/en/20170609-france-state-emergency-macron-police-powers-civil-liberties-terrorism.
8. ""Projet Pegasus:" un téléphone portable d'Emmanuel Macron dans le viseur du Maroc." Accessed March 8, 2025. https://www.lemonde.fr/projet-pegasus/article/2021/07/20/projet-pegasus-un-telephone-portable-d-emmanuel-macron-dans-le-viseur-du-maroc_6088950_6088648.html.
9. "Russian Spies behind Cyberattack on Ukraine Power Grid in 2022." Accessed March 7, 2025. https://www.reuters.com/technology/cybersecurity/russian-spies-behind-cyberattack-ukrainian-power-grid-2022-researchers-2023-11-09/.
10. "State of Emergency Declared for Santorini after Quakes." Accessed March 14, 2025. https://www.bbc.com/news/articles/ce8jlm6rm9qo.
11. "Threat of Cyber-Attacks on Whitehall 'is Severe and Advancing Quickly', NAO Says." Accessed March 14, 2025. https://www.theguardian.com/technology/2025/jan/29/cyber-attack-threat-uk-government-departments-whitehall-nao.

Rok Dacar*

Sažetak

KIBERNETIČKI NAPADI KAO TEMELJ ZA PROGLAŠAVANJE IZVANREDNOG STANJA

Ovaj rad razmatra mogućnost da veliki kibernetički napadi predstavljaju legitiman razlog za proglašenje izvanrednog stanja. Središnja teza je da, iako kibernetički napadi ne pripadaju tradicionalnim kategorijama izvanrednih situacija, njihova sve veća sposobnost ozbiljnog ugrožavanja ključnih državnih funkcija zahtijeva preispitivanje pravnih kriterija za korištenje izvanrednih ovlasti. U radu se ističe da se izvanredno stanje može opravdano proglasiti ako kibernetički napad izazove sustavno narušavanje kritične infrastrukture, javnog reda ili nacionalne sigurnosti te dosegne razinu ozbiljnosti usporedivu s onom konvencionalnih izvanrednih situacija. Primjeri iz stvarnog života, poput kibernetičkih napada na Estoniju 2007. godine i *ransomware* krize u Kostariki 2022. godine, prikazuju različite odgovore država i evoluciju pravnog poimanja kibernetičkih prijetnji. Istodobno, u radu se upozorava na opasnost od normalizacije izvanrednih režima kao odgovora na stalne ili nejasne prijetnje u kibernetičkom prostoru. Postoji rizik da dugotrajno ili neopravdano korištenje izvanrednih mjera potkopa demokratsko upravljanje. Iako u određenim i iznimnim okolnostima kibernetički napadi mogu opravdati proglašenje izvanrednog stanja, takve odluke moraju ostati iznimka i biti temeljene na načelima nužnosti, proporcionalnosti i demokratskog nadzora.

Ključne riječi: *kibernetički napadi; izvanredno stanje; izvanredne ovlasti; pravo nacionalne sigurnosti; upravljanje ustavnim krizama.*

* Dr. sc. Rok Dacar, docent, Sveučilište u Mariboru, Pravni fakultet; rok.dacar@um.si. ORCID: https://orcid.org/0000-0001-8936-9311.